Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

From Local Shocks to Global Cascades: An End-to-End Framework for Simulating Complex Contagion in Financial Networks

Hong Shen
Nanjing Audit University
Xinyu Ma
Nanjing Audit University
Yazhi Li
liyazhi@jit.edu.cn

Jinling Institute of Technology
Jiaqian Wu
Nanjing Audit University
Su Jin
Nanjing Audit University
Xiaodong Zhang
Nanjing Audit University

Research Article

Keywords: Complex Networks, Risk Propagation, Leiden Algorithm, Risk Coupling, Dynamic Contagion Simulation

Posted Date: October 5th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11103947/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

From Local Shocks to Global Cascades: An End-to-End Framework for Simulating Complex Contagion in Financial Networks

Abstract

The proliferation of artificial intelligence (AI) applications introduces emergent AI-associated risks as novel and potent vectors for systemic contagion in interconnected capital markets. Traditional complex network models, however, are often static and fail to capture the non-linear, multi-path coupling effects and the dynamic evolutionary trajectory of risk propagation. To address these gaps, this study develops a hybrid static-dynamic analytical framework. First, we conduct a static analysis to identify systemically important nodes by integrating multi-dimensional centrality metrics and employ the Leiden algorithm to partition the network into distinct risk communities. The core innovation lies in our dynamic analysis. We introduce a non-linear, multi-path risk coupling model to quantify the compounded influence intensity when risk propagates simultaneously through multiple channels. Building on this, we design a multi-stage, multi-level dynamic risk transmission algorithm that simulates the entire cascade, from initial infection and three-degree diffusion to the eventual stabilization of network-wide risk. Empirical analysis on a network of 2,052 Chinese listed companies demonstrates the framework's effectiveness. This research provides a novel, quantifiable methodology for tracing risk from local shocks to systemic cascades, offering valuable tools for financial regulators.

Keywords: Complex Networks, Risk Propagation, Leiden Algorithm, Risk Coupling, Dynamic Contagion Simulation

1 Introduction

The rapid integration of Artificial Intelligence (AI) into the financial sector represents a double-edged sword (Goldstein et al. 2019). While promising unprecedented gains in efficiency and decision-making accuracy (Kou et al. 2021), it simultaneously introduces novel and poorly understood vulnerabilities. A prominent driver of these vulnerabilities is the rise of emergent AI-associated risks—exemplified by phenomena such as "AI hallucinations," where the "black box" nature of complex models generates confident but factually incorrect outputs (Barredo Arrieta et al. 2020) —which serve as potent new vectors for systemic contagion. This concern is not merely theoretical. Leading

international bodies, including the International Monetary Fund (IMF) (International Monetary Fund 2024), the Bank for International Settlements (BIS) (Doerr et al. 2021), and the Financial Stability Board (FSB) (Financial Stability Board 2017), have issued explicit warnings that the contagion mechanism of systemic risks driven by AI applications often begins as a localized technological anomaly before rapidly transforming into a financial cascade. Meanwhile, researchers also have the consensus that the widespread adoption of homogenous AI models could become a new source and amplifier of financial crises. In response to these challenges, novel analytical methodologies have emerged to evaluate the specific impacts of AI-driven model risk and herding behavior on financial stability (Hansen and Lee 2025). Leading scholars now also argue that AI fundamentally alters risk dynamics, creating a "new era of systemic risk" characterized by unprecedented speed and correlation, potentially rendering traditional risk management tools obsolete (Daníelsson et al. 2022). However, the systemic threat of these AI-driven anomalies cannot be understood in isolation. Their capacity to trigger widespread crises is fundamentally governed by the structural topology of the financial system.

In this context, the modern capital market network is best understood as a densely interconnected complex system, a concept established by foundational work showing how linkages can propagate both liquidity and defaults (Acemoglu et al. 2015; Allen and Gale 2000). More importantly, network science (Borgatti and Everett 2006) provides an essential paradigm for mapping these interconnections. Influential frameworks have been developed to measure systemic risk and spillover effects using network econometrics (Billio et al. 2012; Diebold and Yilmaz 2009), with recent applications vividly capturing market connectedness during crises like the COVID-19 pandemic (So et al. 2021). Furthermore, analyses of corporate ownership have revealed "too-interconnected-to-fail" structures through network topology (Vitali et al. 2011), while advanced approaches explore multi-layer networks (Poledna et al. 2015). Regarding the dynamic transmission of risks, other research has applied epidemiological models like the Susceptible-Infected-Recovered (SIR) framework to model financial contagion dynamics (Elliott et al. 2014; Gai and Kapadia 2010). More recently, agent-based models, crucially serving as a bridge between AI-specific risks and network dynamics, have been proposed to simulate how AI-driven trading behaviors can amplify market shocks (Gualdi and Riccetti 2024), highlighting the need for dynamic simulation.

Despite these advances, existing research suffers from critical limitations. First, while recent work has begun to explore time-varying connectedness (Baruník and Křehlík 2018), the majority of these influential studies still rely on static analysis (Billio et al. 2012; Poledna et al. 2015; Vitali et al. 2011), providing a frozen snapshot that fails to capture the dynamic, multi-stage process of how risk actually propagates. Second, they often implicitly assume a 'simple contagion' model (Gai and Kapadia 2010), overlooking the non-linear, synergistic amplification that occurs when an entity is shocked by multiple sources simultaneously. This 'complex contagion' mechanism is a critical but under-quantified factor in systemic risk buildup (Centola and Macy 2007). Finally, there is a conspicuous absence of an end-to-end simulation framework that can trace the entire lifecycle of a risk event from a local shock triggered by these emergent AI anomalies to a potential network-wide crisis.

To address these critical gaps **and effectively model the complex contagion of emergent AI-associated risks**, this paper develops a comprehensive methodology for systemic risk analysis that makes four principal and interconnected contributions:

1) **An Integrated Closed-Loop Analytical Framework.** A novel framework is established that holistically combines "static identification with dynamic simulation." In the static stage, a topological "scan" of the network is performed, using centrality metrics to pinpoint systemically important entities, such as 'risk sinks' (high in-degree), 'risk spreaders' (high out-degree), and 'key bridges' (high betweenness). Concurrently, the advanced Leiden algorithm is employed to partition the network into 'risk communities', laying the groundwork for analyzing localized risk containment and cross-community contagion. This static structure then serves as the substrate for the dynamic simulation stage, which models the actual "flow" of risk. The resulting integrated approach forms a complete analytical cycle, from vulnerability assessment to process tracing **of emergent shocks**.
2) **A Novel Quantitative Model for Multi-Path Risk Coupling.** As a core theoretical contribution, a quantitative model for 'multi-path risk coupling influence' is proposed. Departing from simplistic linear aggregation models, our probabilistic formula scientifically captures the non-linear amplification effect that occurs when a node is simultaneously impacted by multiple distressed neighbors. This approach more realistically mirrors real-world risk superposition logic, **particularly the highly correlated and rapid contagion characteristic of AI-driven market anomalies**. To ensure both analytical depth and computational efficiency, the model's application is pragmatically bounded by a 'three-degree influence' principle.
3) **A Multi-Stage, Multi-Level Risk Propagation Algorithm (M2RPA).** As our core technical contribution, a sophisticated algorithm is designed and implemented for the dynamic simulation. The **M2RPA** decomposes the macro-level contagion phenomenon by actualizing the 'multi-path risk coupling' model into a tractable, micro-level computational process of "three-degree connected node lookup, influence calculation, and state update." It operates through several key mechanisms to **simulate how localized technological anomalies escalate into systemic cascades**: it simulates diffusion in discrete stages (Multi-Stage) until the system stabilizes; it calculates risk influence hierarchically within defined local neighborhoods (Multi-Level); and it incorporates a node immunity mechanism to prevent infinite re-infection loops, thereby enhancing model realism.
4) **Empirical Validation with a Real-World Application Paradigm.** Our research extends beyond pure theory by conducting an extensive empirical analysis on a dataset of 2,052 Chinese listed companies. This validation not only confirms the efficacy of our framework by successfully identifying specific, critical nodes (e.g., V16, V1145) but also demonstrates its utility as an actionable toolkit for regulatory bodies. A concrete example of how this methodology can be used is provided for proactive monitoring, targeted surveillance, and the development of precise risk mitigation strategies, significantly enhancing the practical impact of our research **in the era of AI-driven finance**.

2 Overall Framework: An Integrated Static-Dynamic Approach

Our methodology is designed as a closed-loop, two-stage process that combines static network analysis with dynamic risk simulation. This integrated approach allows for a comprehensive assessment of systemic risk, from identifying latent vulnerabilities to simulating the kinetic process of contagion. The main workflow is shown in Fig. 1 and is as follows:

1) Static Identification Stage: A complex network is first constructed from real-world corporate data. Using a suite of network topology metrics and community detection algorithms, a "static scan" is performed to identify systemically important nodes and cohesive "risk communities." This stage answers the question: "Where are the latent vulnerabilities in the system?"
2) Dynamic Simulation Stage: Leveraging the insights from the static analysis, the propagation of a risk shock—such as a localized disruption triggered by an emergent AI anomaly—is simulated originating from a specific node. A novel multi-path coupling model and a multi-stage simulation algorithm are developed to trace the "flow" of risk through the network over time. This stage answers the question: "How does risk actually spread, and what is its ultimate impact?"

This two-stage design creates a powerful analytical cycle, enabling both proactive risk assessment and reactive crisis simulation in an increasingly interconnected financial ecosystem.

3 Static Network Analysis and Vulnerability Identification

This section investigates the static topological properties and structural vulnerabilities of the capital market network, establishing a foundational premise for subsequent dynamic risk propagation analysis. First, Section 3.1 details the network construction process based on entity relationships. Based on this structural baseline, Section 3.2 employs static centrality metrics to identify systemically important nodes that act as critical hubs during a risk outbreak. Finally, Section 3.3 introduces a risk community partition method to uncover modular clustering characteristics, revealing localized structures where risks are most likely to aggregate and amplify.

3.1 Network Construction

The modern capital market operates not as a collection of independent entities, but as a densely interconnected ecosystem. Within this system, capital flows, corporate control, and supply chain dependencies forge intricate risk transmission pathways. To untangle this complexity and formally model the underlying risk architecture, we employ a weighted directed network approach, and the capital market is represented as a graph, G = (V, E, W).

- Data Source and Node Definition (V)

  V (Vertices), V = {v_1, v_2, ..., v_N}, is the set of capital market entities (e.g., listed companies, financial institutions), each serving as a potential node for

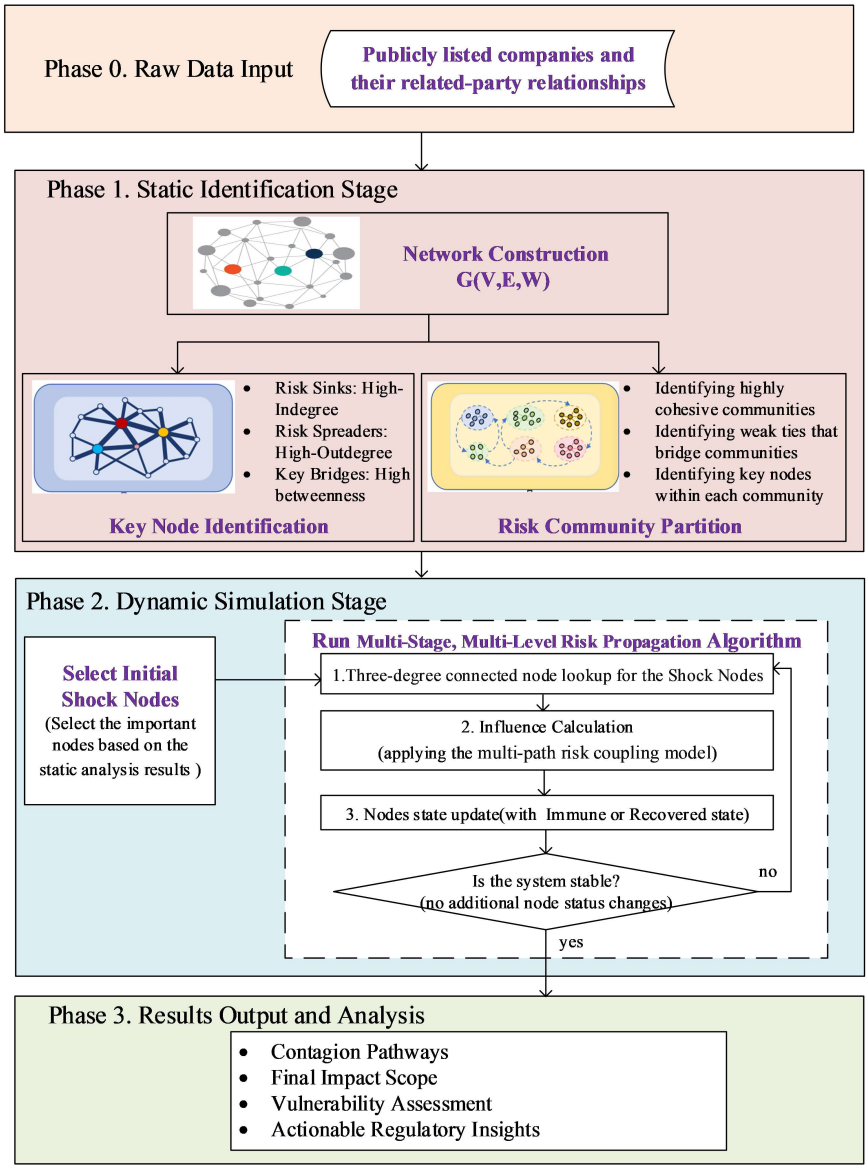


Fig. 1 Integrated Static-Dynamic Closed-Loop Analytical Framework

originating or receiving risk. Our analysis is based on a comprehensive database of China's A-share listed companies, which comprises N=2,052 distinct enterprises selected from this database.

- Edge Definition (E): A Multi-Relational Approach

E (Edges), is the set of directed relationships (i, j) that function as conduits for risk propagation. An edge from node i to j signifies that a shock originating at i

can directly impact j. To capture the multifaceted nature of corporate interdependencies of the above vertices, we identify ten distinct types of relationships that can serve as conduits for risk transmission, Including equity control relationships (e.g., parent company, subsidiary, grandparent company, grandchild company) and operational dependency relationships (e.g., suppliers, purchasers). Applying this multi-relational criterion to our dataset resulted in the generation of $|E|$=3,083 directed edges, forming the fundamental topology of our risk network.

- Weight Definition (W): LLM-Powered Semantic Scoring

  W (Weights), is a set of corresponding edge weights, $w_{ij} \in [0, 1]$, quantifying the transmission intensity or influence capacity of each edge. A higher w_{ij} indicates a greater potential impact of node i on node j. However, quantifying the risk transmission intensity across such diverse relationship types presents a significant challenge. A simple binary or uniform weighting scheme would fail to capture the nuances of control and dependency. For instance, the risk passed from a parent company to a subsidiary is intuitively stronger than that between a supplier and a purchaser. To address this, we introduce an innovative semantic scoring methodology powered by a Large Language Model (LLM, specifically DeepSeek). We leverage the LLM's advanced reasoning and knowledge capabilities to assign a risk influence intensity score to each of the ten relationship types. Based on their intrinsic logic of risk transmission, degree of control, and closeness, the LLM provides a score on a [1-10] scale, where a higher score indicates a stronger risk transmission capacity. The detailed scoring results are presented in Table 1. Finally, these integer scores are normalized to a continuous weight w_{ij} in the range [0, 1].

Table 1 LLM-Powered Semantic Scoring of Inter-Enterprise Risk Transmission Intensity

Relationship Type	**Category**	**Score (/10)**	**Rationale / Transmission Mechanism**
Subsidiary	Control & Ownership	**9.5**	**Direct & Total Control.** Risks are directly and swiftly transmitted through consolidated financials, integrated strategies, and unified capital management. High operational entanglement leads to immediate contagion.
Parent Company	Control & Ownership	**9.0**	**Top-Down Authority.** As the direct controlling shareholder, it dictates strategy and resource allocation. Risks cascade downward through formal governance channels.
Grand-subsidiary	Control & Ownership	**9.0**	**Tiered but Strong Control.** Despite an additional management layer, control from the ultimate parent remains stringent. Risk propagates through the intermediary subsidiary with minimal decay.

Table 1 (continued)

Relationship Type	Category	Score (/10)	Rationale / Transmission Mechanism
Grandparent Company	Control & Ownership	**8.5**	**Indirect Top-Down Authority.** Control is exercised through a multi-tiered structure. Risk transmission is slightly attenuated by intermediary governance, but remains potent.
Joint Venture	Significant Influence	**8.0**	**Shared Control & High Interdependence.** Major decisions require joint consent (typically ~50% equity). Risks are bi-directionally transmitted via contractual obligations and shared operational outcomes.
Associated Company	Significant Influence	**7.0**	**Significant but Non-Controlling Influence.** Equity holdings (typically 20-50%) allow participation in decision-making. Risk transmission is primarily through investment value impairment and dividend shocks.
Core Supplier	Supply Chain Dependency	**7.0**	**Upstream Operational Risk.** Disruption from a critical supplier directly threatens the firm's production and operational continuity. Assumes high dependency on the supplier.
Core Purchaser / Major Client	Supply Chain Dependency	**6.5**	**Downstream Revenue Risk.** Loss of or distress at a major client directly impacts revenue and cash flow. Assumes high client concentration.
Minority-held Investee	Financial Investment	**6.0**	**Limited Influence.** A general shareholding (typically <20%) primarily represents a financial investment. Risk transmission is delayed and mainly financial, lacking operational impact.
Other Affiliated Entity	Financial Investment	**5.0**	**Weak & Distant Link.** Non-core equity investment with low business relevance. Risk transmission is weak, indirect, and requires multiple triggers to manifest.

The entire network structure can be mathematically described as an N × N weighted adjacency matrix A, where $A_{ij}=w_{i,j}$ if a directed edge from i to j exists, and 0 otherwise. This matrix serves as the foundational data structure for our subsequent static and dynamic risk analyses.

$$A = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{pmatrix} \tag{1}$$

$$A_{ij} = \begin{cases} w_{i,j}, & \text{if } \langle i,j \rangle \in E, \\ 0, & \text{if } \langle i,j \rangle \notin E. \end{cases} \tag{2}$$

3.2 Identification of Systemically Important Nodes via static Centrality Analysis

To identify the nodes most critical to risk propagation, this paper employ centrality analysis, a cornerstone of network science. The node importance is evaluated from three distinct but complementary perspectives: connectivity (Degree), influence intensity (Strength), and structural brokerage (Betweenness). This multi-faceted approach allows us to pinpoint entities that act as risk aggregators, primary disseminators, and crucial conduits within the inter-enterprise network.

1) Connectivity-Based Importance: In-Degree and Out-Degree Centrality Degree centrality is the most direct measure of a node's connectivity. In a directed network, we distinguish between two types:

In-Degree quantifies the number of incoming risk channels. A high weighted in-degree signifies a "Risk Aggregator"—an entity highly exposed to shocks from its partners (e.g., a manufacturer reliant on many suppliers). These nodes are points of systemic vulnerability.

Out-Degree measures the number of outgoing risk channels. A high weighted out-degree identifies a "Risk Disseminator"—an entity whose distress can impact numerous others (e.g., a parent company to many subsidiaries). These nodes are primary sources of contagion. Nodes exhibiting both high in-degree and out-degree are classified as "Super-Spreaders," capable of both absorbing and amplifying shocks, thus posing the greatest systemic threat.

2) Intensity-Based Importance: Node Strength While degree counts connections, Node Strength measures their cumulative intensity. Defined as the sum of weights of all incident edges, strength reflects a node's total risk "energy"—a composite of its total exposure (in-strength) and influence (out-strength). High-strength nodes represent major economic hubs interconnected by "highways" for risk transmission. Analyzing strength allows us to move beyond the mere number of relationships to quantify the financial and operational magnitude of their interdependence, providing a more refined view of risk concentration.

3) Structural Importance: Betweenness Centrality Betweenness Centrality captures a node's importance as an intermediary or "gatekeeper" in the network. It measures how often a node lies on the shortest path between other pairs of nodes. The formula is given by:

$$C_B(v) = \sum_{s \neq v \neq t \in V} \frac{\sigma_{st}(v)}{\sigma_{st}} \sigma_{st} \sigma_{st}(v) \tag{3}$$

Where σ_{st} is the count of weighted shortest paths between nodes s and t, and $\sigma_{\mathrm{st}}(\mathrm{v})$ is the number of those paths that traverse node v.

Nodes with high betweenness centrality are critical conduits that bridge otherwise disconnected communities. Their failure can fragment the network, leading to cascading failures by isolating entire segments. Controlling these structurally vital nodes is a highly efficient strategy for containing risk within localized areas and preventing system-wide contagion.

Based on the capital market network constructed as per Section 3.1, we introduce the following Algorithm 1 to operationalize the static analysis in detail. This algorithm

processes is developed to compute the four key centrality metrics for each node: weighted in-degree, weighted out-degree, node strength, and betweenness centrality. The primary computational bottleneck within this algorithm is the calculation of betweenness centrality for a weighted directed graph, which results in an overall time complexity of $O(n^3)$, where n is the number of nodes. The outputs are four distinct arrays—inDegree, outDegree, strength, and betweenness—which respectively store the calculated values for all nodes. These outputs serve as the quantitative basis for identifying systemically important nodes, namely those exhibiting high values in one or more of these centrality dimensions, and provide the initial state for our subsequent dynamic risk propagation analysis.

Algorithm 1 Static Centrality Analysis for Important Nodes

```
Initialize inDegree[0..n-1] ← {0}
Initialize outDegree[0..n-1] ← {0}
Initialize strength[0..n-1] ← {0}
Initialize betweenness[0..n-1] ← {0}
// Calculate in-degree, out-degree, and node strength
For i = 0 to n-1
  For j = 0 to n-1
    If A[i][j] > 0 then
      outDegree[i] ← outDegree[i] + 1
      inDegree[j] ← inDegree[j] + 1
      strength[i] ← strength[i] + A[i][j]
    End if
  End for
End for
// Calculate betweenness centrality
For s = 0 to n-1
  Initialize dist[0..n-1] ← {∞}
  Initialize sigma[0..n-1] ← {0}
  Initialize pred[0..n-1] ← ∅
  dist[s] ← 0
  sigma[s] ← 1
  stack ← ∅
  queue ← ∅
  EnQueue(queue, s)
  // BFS for shortest path counting
  While queue ≠ ∅ do
    current ← DeQueue(queue)
    Push(stack, current)
    For j = 0 to n-1
      If A[current][j] > 0 then
        If dist[j] = ∞ then
          dist[j] ← dist[current] + 1
          EnQueue(queue, j)
        End if
        If dist[j] = dist[current] + 1 then
          sigma[j] ← sigma[j] + sigma[current]
```

Algorithm 1 Static Centrality Analysis for Important Nodes (continued)

```
            pred[j].append(current)
          End if
        End if
      End for
    End while
    Initialize delta[0..n-1] ← {0}
    // Accumulate betweenness scores
    While stack ≠ ∅ do
      w ← Pop(stack)
      For each v in pred[w]
        delta[v] ← delta[v] + (sigma[v] / sigma[w]) × (1 + delta[w])
      End for
      If w ≠ s then
        betweenness[w] ← betweenness[w] + delta[w]
      End if
    End while
  End for
  Return inDegree, outDegree, strength, betweenness
```

3.3 Risk community partition method

In the capital market network, the strength of connections between entities is fundamentally driven by the underlying relational semantics among participants. Subsets of highly interconnected nodes naturally aggregate to form risk communities, within which systemic shocks are easily amplified due to significant mutual exposure. Structurally, these communities exhibit high modularity-characterized by dense, high-impact internal ties and relatively sparse external linkages. By partitioning the network based on these topological patterns, we can map the entire market into distinct risk modules, occasionally identifying isolated clusters resulting from weak systemic integration. Delineating these risk communities is critical for understanding macro-level contagion dynamics. It provides a strategic blueprint for regulatory intervention: when a localized shock erupts, early warning systems can be activated, and preventive "firewalls" can be established by temporarily isolating the key bridging nodes that connect the affected community to the broader network, thereby effectively containing the contagion and mitigating systemic spillover.

This study employs the Leiden (Traag et al. 2019) algorithm for risk community partition. As an optimized community discovery algorithm based on the Louvain algorithm, it specifically addresses community partitioning in weighted directed graphs. The core methodology achieves community optimization through modular degree optimization and local community redistribution. The modular degree of directed graphs is defined as:

$$Q = \frac{1}{m} \sum_{i,j} \left(A_{ij} - \frac{k_i^{\text{out}} k_j^{\text{in}}}{m} \right) \delta(c_i, c_j) \tag{4}$$

Here, A_{ij} indicates whether there exists an association between the capital market entities i and j, and the strength of that association. k_i^{out} and k_j^{in} represent the out-degree and in-degree of node i respectively. m shows the total weight of all edges in the graph. $\delta(c_i,c_j)$ is an indicator function. It returns 1, if i and j belong to the same community, otherwise 0.

The larger the Q-value (typically between 0 and 1), the higher the quality of community partition. High-quality community partition is achieved by maximizing the modular degree of the directed graphs. The modular degree gain ΔQ is defined as follows.

$$\begin{aligned}\Delta Q = & \left[\frac{\Sigma_{in} + k_i^{in,in}}{2m} - \left(\frac{\Sigma_{tot} + k_i^{tot}}{2m}\right)^2\right] \\ & - \left[\frac{\Sigma_{in}}{2m} - \left(\frac{\Sigma_{tot}}{2m}\right)^2 - \left(\frac{k_i^{tot}}{2m}\right)^2\right].\end{aligned} \tag{5}$$

Here, Σ_{in} represents the total edge weight sum within the community, Σ_{tot} denotes the total edge weight sum of the community, and k_i^{tot} indicates the total degree of node i.

Based on the concept of community partitioning in the Leiden algorithm, and considering the various categories of relationships in the network structure model of capital market entities, the risk community partition method is described in detail in Algorithm 2. The time complexity of the algorithm is O(N+E), where N is the total number of the nodes, and E is the total number of the edges in the capital market network.

Algorithm 2 The Risk Community Partition Method

```
// Initialization
For each node i ∈ V do
  c[i] ← i // Each node starts in its own community
End for
improved ← true
While improved do
  improved ← false
  // Phase 1: Local Move - maximize modularity gain ΔQ
  For each node i ∈ V in random order do
    oldCommunity ← c[i]
    Remove i from oldCommunity
    bestCommunity ← oldCommunity
    maxDeltaQ ← 0
    // Try moving i to each neighboring community
    For each neighbor j of i where A[i][j] > 0 do
      targetCommunity ← c[j]
      If targetCommunity = oldCommunity then continue
      // Compute modularity gain ΔQ using the formula
      // ΔQ = (new modularity) - (old modularity)
      sumInTarget ← sum of weights of edges inside targetCommunity
```

Algorithm 2 The Risk Community Partition Method (continued)

```
        sumTotTarget ← sum of all edge weights connected to targetCommunity
        k_i_tot ← k_iˆout + k_iˆin
        k_i_inIn ← sum of weights of edges from i to nodes in targetCommunity
        newModTerm ← (sumInTarget + k_i_inIn) / (2*m) - ((sumTotTarget + k_i_tot)
/ (2*m))ˆ2
        oldModTerm ← sumInTarget / (2*m) - (sumTotTarget / (2*m))ˆ2 - (k_i_tot /
(2*m))ˆ2
        deltaQ ← newModTerm - oldModTerm
        If deltaQ > maxDeltaQ then
          maxDeltaQ ← deltaQ
          bestCommunity ← targetCommunity
        End if
      End for
      // Move i to the best community if gain is positive
      If bestCommunity ≠ oldCommunity then
        c[i] ← bestCommunity
        improved ← true
      Else
        // Put back to old community
        c[i] ← oldCommunity
      End if
    End for
    // Phase 2: Refinement (ensure well-connected communities)
    For each community C in current partition do
      If C is not well-connected then
        Split C into well-connected sub-communities
        Update community assignment c accordingly
      End if
    End for
    // Phase 3: Aggregation (form new "super nodes")
    Aggregate communities into super nodes, build new adjacency matrix A'
    Set A ← A', m ← total edge weight of A'
    Renumber nodes according to new communities
  End while
  // Compute final modularity Q
  Q ← 0
  For i = 0 to n-1 do
    For j = 0 to n-1 do
      If c[i] = c[j] then
        Q ← Q + (A[i][j] - (k_iˆout * k_jˆin) / m)
      End if
    End for
  End for
  Q ← Q / m
  Return c, Q
```

4 Dynamic Risk Contagion Analysis via Multi-Path Coupling

4.1 Quantifying the Intensity of Multi-Risk Coupling

As previously established, capital market networks exhibit highly complex topologies. When localized risks accumulate and exceed inherent systemic defense thresholds, they can trigger cascading spillovers, leading to multi-path and multi-risk coupled interactions. If positive coupling effects emerge during this propagation, they significantly amplify the contagion volume and may even spawn more complex systemic threats.

Following the third-degree influence principle (Christakis and Fowler 2009), a risk originating at source node i exerts a measurable impact on associated nodes within a three-hop radius. The single-path transmission pattern from node i to any target node j within this boundary operates via direct (i→j) or indirect (i→s1→j, or i→s1→s2→j) edges. The single-path influence intensity, $\rho_{\mathrm{i,j}}$, is formally defined as:

$$\rho_{i,j} = \begin{cases} \rho_{i,i} w_{i,s_1}, & \text{for path } i \to j, \\ \rho_{i,i} w_{i,s_1} w_{s_1,j}, & \text{for path } i \to s_1 \to j, \\ \rho_{i,i} w_{i,s_1} w_{s_1,s_2} w_{s_2,j}, & \text{for path } i \to s_1 \to s_2 \to j, \end{cases} \tag{6}$$

$$0 < \rho_{i,j} \leq 1.$$

where $\rho i,i$ denotes the baseline risk intensity at the source (with $\rho i,i$=1).

Financial anomalies induced by AI hallucinations predominantly exhibit positive network coupling, wherein convergent risks mutually reinforce each other, inflating total risk exposure and destabilizing market equilibrium. As illustrated in Fig. 2, a shock at node 1 propagates initially to its first-degree neighbors {2,3,4,6,8,10}, and subsequently reaches second-degree nodes {5,7,9}. Notably, target nodes such as 5 and 9 are subjected to multi-path risk coupling. During propagation, overlapping transmission channels (e.g., via nodes 7, 8, and 10) generate mutually intensified risk vectors, amplifying the compounded impact on terminal node 9.

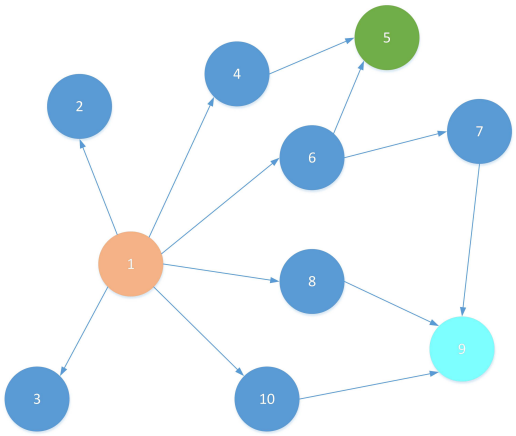


Fig. 2 An example of risk transmission across multiple levels and pathways

To formally quantify this multi-pathway coupling mechanism, we first model a dual-factor scenario (Fig. 3). Referring to Fig. 2, the source node 1 impacts intermediate nodes 4 and 6 with intensities $\rho_{1,4}$=a, $\rho_{1,6}$=b, computed via Equation (6). These intermediate nodes subsequently converge on node 5 (Fig. 4). Assuming independent probabilistic propagation across edges, the coupled influence intensity integrating these dual pathways is given by the union probability:$\rho_{1,5}=\{\rho_{4,5},\rho_{6,5}\}=1-(1-a)\times(1-b)$.

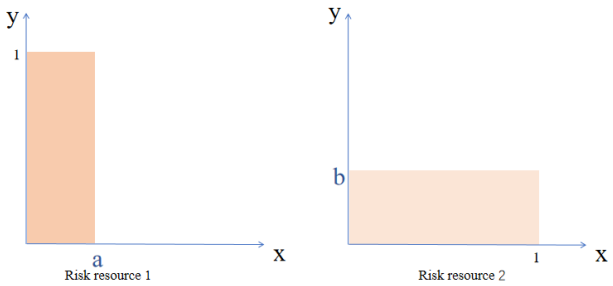


Fig. 3 Multi-path risk resources

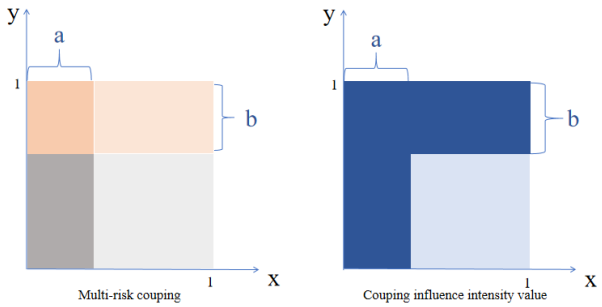


Fig. 4 Risk coupling influence intensity value

This dual-factor logic naturally extends to generalized n-ary multi-path risk coupling. When an initial shock at node i propagates through arbitrary converging pathways to reach node j, the aggregate multi-path coupled influence intensity on j is formalized as:

$$\rho_{i,j} = 1 - \prod_{\langle \mathrm{pre},j\rangle \in E} (1 - \rho_{i,\mathrm{pre}} w_{\mathrm{pre},j}) \tag{7}$$

where <pre,j> denotes the set of all active incoming edges to node j from proximate precursor nodes pre, and $w_{\mathrm{pre,j}}$ represents the respective edge weights. The term $\rho_{\mathrm{i,pre}}$, determined by Equation (6), captures the accumulated influence intensity reaching the precursor nodes.

This model transcends strictly linear node-to-node impact assessments by integrating localized direct shocks with complex, third-degree converging indirect effects.

By mathematically framing multi-path risk coupling as a product of complementary probabilities, this framework aligns rigorously with empirical systemic risk contagion behaviors and serves as the quantitative foundation for subsequent dynamic contagion simulations.

4.2 Heuristic-driven Dynamic Risk Contagion Model

When a local shock originates at a specific node within the capital market network, it propagates outward across interconnected topological layers. If the cumulative risk influence intensity on a target node surpasses its inherent tolerance threshold, its defense mechanism is breached. Consequently, this node transitions into an infected state and acts as a secondary source, triggering further outward contagion. Macroscopically, this cascade manifests as a multi-stage, multi-level oscillatory diffusion pattern across the entire market network. Furthermore, it is critical to note that compromised nodes possess self-recovery capabilities. Through institutional resilience and self-repair mechanisms, these nodes can acquire risk immunity, thereby precluding reinfection during subsequent oscillatory shocks.

To formally formalize this heuristic-driven multi-stage transmission process, we define a discrete-time state transition framework. At any given transmission stage t, each entity node j in the capital market network exists in one of three mutually exclusive states: S, I, or R.

- Susceptible State (S): Nodes that are operating normally but are exposed to potential upstream risks. Their cumulative received risk intensity $\rho_{i,j}$ has not yet exceeded their inherent defensive threshold θ_j.
- Infected State (I): Nodes whose defensive thresholds have been breached by accumulated risk spillovers ($\rho_{i,j}>\theta_j$). These nodes suffer operational or financial impairment and act as secondary risk sources, propagating shocks to their downstream connected nodes in the next stage.
- Recovered/Immune State (R): Nodes that have triggered self-repair mechanisms or institutional interventions following an infection. Once entering this state, they acquire risk immunity and will not be reinfected or transmit risks during subsequent oscillatory cycles.

Heuristic State Transition Rules: The dynamic evolution of the network at stage $t \rightarrow t+1$ is governed by the following heuristic rules:

- Infection Rule ($S \rightarrow I$): If node $j \in S(t)$, and the aggregated multi-path risk influence intensity $\rho_{i,j}(t)$ computed via Equation (7) exceeds its tolerance threshold θ_j, the node transitions to the infected state: $j \in I(t+1)$.
- Recovery Rule ($I \rightarrow R$): After an infected node $j \in I(t)$ has fully transmitted its risk exposure to its neighboring nodes within a designated stage window, it activates its self-repair capability and transitions to the immune state: $j \in R(t+1)$.

  By iterating these state transitions across topological layers, the model systematically captures the complete life cycle of risk accumulation, cascading outbreaks, and eventual network stabilization.

In order to analyze dynamic risk propagation in the capital market entity networks, this study proposes a multi-stage, multi-level risk dynamic transmission method based on heuristic rules, comprising four algorithms. Standard search and intensity calculations are handled by Algorithms 4-1 through 4-3, establishing the baseline

network topology and risk coupling parameters. Specifically, Algorithm 3 (CNS_BFS) applies a breadth-first search to extract a three-degree connected subgraph Δ, invoking Algorithm 4 (ROR_DFS) to eliminate cyclic risk loops. Algorithm 5 (CRTI_FB) calculates the multi-path risk influence intensity (ρ) using forward-backward tracing strategies (Equations (6) and (7)).

Based on the breadth-first search rule, Algorithm 3 CNS_BFS starts from a specified risk node and, and identifies all connected nodes within a three-degree of that node, then aggregates these nodes into a set Δ. By invoking Algorithm 4, it can effectively resolve loop issues and successfully eliminate loops formed during risk impact propagation, ensuring stable system operation and effective risk management.

Algorithm 3 Connected Node Search (CNS_BFS)

```
1  //Given the the network relationships matrix A, and the current risk node i
2  //Using breadth−first search to find the set Δ of connected nodes within three degrees
3  Initialize the set Δ as ∅,  X0←{i}, X1←∅, X2←∅, X3←∅
4  Initialize the number of risk transfer layers n←1
5  Repeat
6    For each node cnode in X(n−1)
7      If (cnode has successor nodes) then
8        For each successor node adj of cnode
9          If ROR_DFS(A, adj, cnode) //find risk loops
10           Delete the edge connecting node adj to cnode //eliminate risk loops
11         Endif
12         Add the node adj to the set, Xn ← Xn ∪ {adj}
13       Endfor
14     Endif
15   Endfor
16   n ← n+1
17 Until n>3
18  Δ ← X1 ∪ X2 ∪ X3
19 Returns the set of connected nodes Δ within three degrees
```

Algorithm 4 ROR_DFS is designed to find risk loops. Its main idea employs depth-first search (DFS) to determine whether a path exists from node adj to node cnode in the adjacency matrix A. The algorithm utilizes a stack for non-recursive implementation, starting with adj to traverse all reachable nodes. If cnode is encountered during traversal, the algorithm returns true. Otherwise, it returns false.

Algorithm 4 Resolution of Rings (ROR_DFS)

```
1 //Given the network relationships matrix A, and current node adj and cnode
2 //Using depth-first search (DFS) to determine whether there exists a path from adj to
  cnode
3 //If exist, inform Algorithm 3 to eliminate risk loops
4 Initialize visited[0..n-1] ← {false}
5 Initialize the stack and Push(stack, adj)
6 While the stack is not empty
```

Algorithm 4 Resolution of Rings (ROR_DFS) (continued)

```
    current ← Pop(stack)
    If current == cnode
      return true
    Endif
    visited[current] ← true
    For j from 0 to n-1
      If A[current][j] == 1 and visited[j] == false
        Push(stack, j)
      Endif
    Endfor
  Endwhile
  Return false
```

Time complexity analysis of Algorithm 4: Using a stack for DFS, it accesses all N nodes and E edges at most. In the worst case, the entire graph must be traversed, resulting in a time complexity of O(N+E).

Time complexity analysis of Algorithm 3: Let the capital market entity network consist of N nodes, with each node having a maximum out-degree of d. Breadth-First Search (BFS) traverses a three-degree range, with a maximum node access count of $1+d+d^2+d^3$. In dense networks, this can be approximated as $O(d^3)$, while in sparse networks it scales with N. During BFS execution, the ROR_DFS subroutine is invoked for each edge (*cnode*, *adj*) to detect reverse paths and determine edge deletion. Although ROR_DFS has a worst-case time complexity of O(N + E), its repeated invocations during BFS operations combined with network constraints result in overall complexity of $O(N \cdot d^3)$ or more precisely $O(N \cdot (d + d^2 + d^3))$. Consequently, Algorithm 3 achieves time complexity $O(N \cdot d^3)$, which can be approximated as $O(N^2)$ in dense networks and approaches O(N) in sparse networks.

Algorithm 5 CRTI_FB employs recursive methods and forward-backward tracing strategies to calculate risk influence intensity value. The recursive approach computes risk influence intensity value of all predecessor nodes for the current node, while The forward-backtracking strategy analyzes each node in the set Δ to identify either a single path predecessor node or multiple predecessor nodes for the current node. For single-path transmission scenarios, the risk influence intensity value of the current node is calculated using Formula (6). For the multi-path transmission scenarios, the multi-path coupling influence intensity value is computed via Formula (7).

Algorithm 5 Calculation of Risk Transmission Influence Intensity (CRTI_FB)

```
//Calculation of Risk Transmission Influence Intensity Based on Recursion Method and
Forward-Backward Strategy
//Given the network relationships matrix A, the set of three-degree connected nodes Δ
//Forward Backtracking Strategy
For each node i in the node set Δ
  If (the impact degree of node i has been calculated)
    continue
  Endif
```

Algorithm 5 Calculation of Risk Transmission Influence Intensity (CRTI_FB) (continued)

```
    //Recursive method for calculating node influence degree
    For each predecessor node pre of node i // A(pre,i)==1
      Call CRTI_FB() to calculate the influence intensity value of the predecessor pre on node i.
    Endfor
    If (inDegree[i] == 1 ) //The in-degree of node i is 1
      Calculate the Influence Intensity on node i by Formula (6)
    Else
      Calculate the Influence Intensity on node i by Formula (7)
    Endif
  Endfor
  Return
```

Time complexity analysis of Algorithm 5: Let the number of nodes in three-degree $|\Delta|$=m, each node is computed at most once during recursion (using a "computed" flag to avoid repetition). For every node, all its predecessor nodes must be traversed, with average in-degree denoted as d_{in}. Thus, the overall time complexity is $O(m \cdot d_{in})$. In dense networks, this can be approximated as $O(m \cdot N)$, while in sparse networks it approaches O(m).

The core state transitions are governed by Algorithm 6 (M2RPA), which utilizes the predefined Susceptible (S), Infected (I), and Recovered/Immune (R) state space to conduct multi-stage risk diffusion analysis. Initially, all nodes except the initial risk source exist in the Susceptible set S. During propagation, the algorithm utilizes CNS_BFS for local topology extraction and CRTI_FB for intensity computation. If the cumulative intensity ρ on a node in S exceeds the threshold Θ, it transitions to the Infected set Inew for the subsequent stage. Crucially, nodes in the current infected set I that have completed their outward transmission immediately transition into the Recovered set R, acquiring risk immunity to prevent infinite oscillations. The diffusion terminates when the active infected set becomes empty.

Algorithm 6 Multi-Stage Multi-Level Method for Risk Propagation Analysis (M2RPA)

```
// Given the network relationships matrix A and the initial risk nodes {r}
// Initialize the standard state sets (S, I, R)
I ← {r} // Initial infected nodes
R ← ∅ // Initial immune/recovered set is empty
S ← All Network Nodes - {r} // Remaining nodes are susceptible
Repeat
  I_new ← ∅ // Temporary set for newly infected nodes in stage t+1
  For each active risk node i ∈ I do
    Call CNS_BFS() to find the set Δ of connected nodes within three-degree of i
    Call CRTI_FB() to calculate the influence intensity value ρ(i,k) of each node in Δ
  Endfor
  For each node k ∈ Δ
```

Algorithm 6 Multi-Stage Multi-Level Method for Risk Propagation Analysis (M2RPA) (continued)

```
    If k ∈ S and ρ(i,k) > Θ then // Heuristic Infection Rule (S -> I)
      I_new ← I_new ∪ {k}
      S ← S - {k} // Remove from susceptible
    Endif
  Endfor
  R ← R ∪ I // Heuristic Recovery Rule (I -> R): old sources become immune
  I ← I_new // Next stage is driven only by newly infected nodes
Until I is ∅ // Stop when no new infections occur
Return the cumulative risk infection set R
```

Time complexity analysis of Algorithm 6: Let the total number of eventually infected nodes be $|R|=k$. During each multi-stage iteration, CNS_BFS is invoked for each active node in I, yielding a local complexity of $O(N \cdot d^3)$. Algorithm CRTI_FB calculates intensities for the localized set Δ with complexity $O(m \cdot din)$, where $m \leq N$. Because nodes definitively transition into the R state post-transmission (preventing redundant cycles), each infected node acts as an active source exactly once. The worst-case time complexity aggregates to $O(k \cdot (N \cdot d^3 + N \cdot din))$. In extreme cascading scenarios ($k \approx N$), this evaluates to $O(N^2 \cdot (d^3 + din))$. This simplifies to $O(N^3)$ in dense networks and approaches $O(N^2)$ in sparse networks, ensuring computational efficiency despite topological scale.

5 Experiments and Analysis

5.1 Data Summary and General Environment

As detailed in Section 3.1, the empirical experiments are conducted on a weighted directed network representing China's A-share market. The static topology comprises N=2,052 listed companies (nodes) and |E|=3,083 multi-relational dependencies (edges). The risk transmission capacity (weights) for each edge is intrinsically initialized using the normalized LLM-powered semantic scores. This defined network serves as the structural baseline for the subsequent experiments. All network visualizations and analytical algorithms in this section are implemented in Python and executed on an Intel Core i7 processor with 16 GB of RAM.

5.2 Static Network Characteristics Analysis

5.2.1 Key Node Identification results

Based on the established capital market network, we utilize Algorithm 1 to compute the in-degree, out-degree, nodal strength, and betweenness centrality for each entity. The top 10 nodes with the highest metric values are presented in Tables 2, 3, and 4.

By analyzing these static topological features, we can categorize the critical nodes and derive targeted risk management strategies:

- Risk Aggregation Hubs (High In-degree): As shown in Table 2, Node V16 exhibits an exceptionally high in-degree. Nodes within the high in-degree set, such as {V16,

V18, V10, V239, V2}, function as risk sinks. Due to the multi-path coupling of risk transmission, they are highly susceptible to converging shocks. During risk prevention, these nodes require rigorous vulnerability monitoring.

- Active Super-spreaders (High Out-degree): Nodes such as V1145 and V16 demonstrate prominent out-degree characteristics, acting as active risk disseminators. Once a local shock occurs, they can rapidly amplify and propagate the risk to a broader range of downstream nodes. Consequently, if risks are detected in the predecessor nodes of the set {V1145, V633, V16, V239, V52}, targeted isolation measures should be prioritized immediately to prevent widespread contagion.
- Systemically Important Nodes (High Centrality): Nodes in the set {V1145, V16, V633, V239, V52} rank highest in overall centrality (the sum of in-degree and out-degree), exerting a profound influence on the overarching network architecture. Node V16, in particular, acts as both a primary sink and a super-spreader. Regulators should establish strict risk thresholds and implement early warning mechanisms for these entities to preempt systemic crises.
- High-Intensity Propagators (High Node Strength): Node strength reflects the intrinsic "energy" of risk propagation, where high-weight edges serve as the "highways" for risk transmission. As illustrated in Table 3, the node strength rankings exhibit a high degree of consistency with Table 2. Nodes such as {V1145, V16, V633, V239, V52, V638} demonstrate significant risk propagation influence. For these high-intensity nodes, it is essential to trace their specific transmission pathways and accurately calculate their impact scope, providing quantitative evidence for precision risk control.
- Transmission Bridges (High Betweenness Centrality): Table 4 presents the top 10 nodes ranked by betweenness centrality. These nodes act as critical "transmission bottlenecks," typically located at community boundaries connecting different market clusters. Failures in these intermediary nodes are highly likely to trigger cascading chain reactions. When risks emerge, implementing targeted controls on these nodes can effectively divide the overarching network into isolated sub-networks, thereby confining the risk propagation to a localized area.

Table 2 Top 10 key nodes considering in-degree, out-degree, and centrality

Node ID	**In-degree**	**Node ID**	**Out-degree**	**Node ID**	**Centrality**
V16	247	V1145	758	V1145	759
V18	33	V633	321	V16	527
V10	26	V16	280	V633	323
V239	11	V239	149	V239	160
V2	10	V52	138	V52	140
V2029	9	V638	93	V638	94
V11	7	V735	73	V735	75
V8	5	V53	72	V53	74
V19	4	V535	69	V535	70
V17	2	V18	32	V18	65

Table 3 Top 10 key nodes considering weighted input intensity, weighted output intensity and strength

Node ID	Weighted input intensity	Node ID	Weighted output intensity	Node ID	Strength
V16	283.3	V1145	922.6	V1145	923.55
V10	33.15	V16	340.65	V16	623.95
V18	31.75	V633	301	V633	302.85
V239	11.6	V239	186.4	V239	198
V2	9.95	V52	154.6	V52	157.65
V2029	8.1	V638	103.7	V638	105.35
V11	5.9	V735	75.4	V735	77
V8	4.8	V53	74.7	V53	76.55
V19	3.2	V535	73.55	V535	74.25
V52	3.05	V10	35.9	V10	69.05

Table 4 Top 10 key nodes considering betweenness centrality

Node ID	Betweenness centrality	Ranking
V16	0.13543352	1
V1145	0.05113223	2
V53	0.0240449	3
V633	0.02154713	4
V52	0.02058746	5
V10	0.01380386	6
V2	0.01167093	7
V239	0.00971733	8
V334	0.00899311	9
V638	0.00601158	10

5.2.2 Results and Analysis of Risk Community Partition

To classify network nodes into distinct communities, we employ the Leiden algorithm designed for directed weighted networks as described in Section 3.3. This method optimizes modularity to achieve high-quality community detection, thereby facilitating modular supervision to contain risks within localized perimeters. The algorithm yields a highly optimized modularity score of 0.8034, resulting in the formation of 13 distinct communities.

Table 5 provides a detailed statistical summary of the identified communities. By analyzing network density and inter-community edges, we observe varying risk propagation characteristics across different clusters:

- Isolated Giant Component (Community No. 0): This is a super-large community comprising 758 nodes and 1,024 internal connections, exhibiting dense internal interconnectivity. Despite its massive scale, it maintains extremely sparse external linkages, with only 2 cross-community relationships, indicating a highly independent sub-system. Strengthening internal supervision here is highly effective for risk control. If localized shocks occur, immediately isolating these two external edges can effectively prevent any cross-community contagion.
- High-Spillover Hub (Community No. 2): Comprising 269 nodes and 671 internal connections, this community demonstrates strong internal cohesion alongside high external connectivity, evidenced by its 44 cross-community relationships. Once a risk materializes within this group, there is a severe probability of rapid spillover, leading to cascading infections in adjacent communities. Consequently, rigorous regulatory oversight for this specific community is exceptionally critical to prevent overarching systemic crises.

To further operationalize targeted and efficient risk supervision, Table 6 highlights the top 5 pivotal nodes within each community, ranked by centrality, providing focal points for intra-community monitoring.

Furthermore, Table 7 explicitly maps the cross-community transmission channels, detailing the source node and community, the target node and community, and the specific relationship type. Relying on this precise mapping, regulators can execute targeted interventions—selectively severing high-risk inter-community edges to surgically interrupt the systemic spread of financial contagion.

Table 5 Statistical information of each community (a) Community size and relationships

Community ID	**Number of nodes**	**Internal relationships**	**Total internal edge weights**	**Cross-community relationships**
0	758	1024	921.7	2
1	320	334	299.15	4
2	269	671	595	44
3	148	213	193.7	24
4	137	171	152.75	6
5	90	115	100.7	6
6	73	91	75.15	6
7	71	87	71.65	6
8	70	79	73.55	1
9	48	73	60.95	8
10	34	81	72.4	1
11	27	75	67.6	3
12	7	13	11.8	1
Global Statistics	2052	3027	2696.1	56

Table 5 Statistical information of each community (b) Topological metrics (continued)

Community ID	Subgraph density	Average outdegree	Mean total degree	Maximum total degree	Mean clustering coefficient
0	0.0013	1	2	759	0
1	0.0031	1	2.01	323	0
2	0.0069	1.94	3.86	527	0.0074
3	0.0072	1.14	2.27	160	0.0676
4	0.0073	1.01	2.01	140	0
5	0.0111	1.03	2.03	94	0
6	0.0139	1.01	2.08	75	0.0137
7	0.0141	1.01	2.03	74	0
8	0.0143	0.99	1.99	70	0
9	0.0288	1.44	2.83	31	0.0227
10	0.0651	2.15	4.32	65	0
11	0.0712	1.89	3.81	52	0
12	0.2857	1.71	3.57	13	0
Global Statistics	0.0006	1.18	2.36	759	0.0069

Table 6 Information of community key nodes

Community ID	No.1	No.2	No.3	No.4	No.5
0	V1145	V1146	V1147	V1148	V1149
1	V633	V743	V744	V745	V746
2	V16	V632	V225	V233	V328
3	V239	V250	V264	V276	V337
4	V52	V54	V55	V56	V57
5	V638	V639	V640	V641	V642
6	V735	V734	V646	V647	V648
7	V53	V1068	V1069	V1070	V1071
8	V535	V536	V537	V538	V539
9	V2	V33	V42	V8	V25
10	V18	V2029	V2028	V2031	V2039
11	V10	V207	V191	V192	V193
12	V11	V216	V217	V218	V219

Table 7 Cross-community relationship analysis (comm. denotes community)

Relation ID	Relation type	Source node ID	Source comm.	Target node ID	Target comm.	Comm. link
LR1710	Parent company	V1145	0	V16	2	0->2
LR1238	Parent company	V633	1	V16	2	1->2
LR1557	subsidiary	V633	1	V632	2	1->2
LR70	Parent company	V10	11	V52	4	11->4
LR1709	subsidiary	V16	2	V1145	0	2->0
LR1057	Parent company	V632	2	V633	1	2->1
LR1237	subsidiary	V16	2	V633	1	2->1
LR357	Subsidiary company	V16	2	V239	3	2->3
LR574	Subsidiary company	V16	2	V264	3	2->3
LR577	Subsidiary company	V16	2	V250	3	2->3
LR1059	affiliated company	V16	2	V334	3	2->3
LR1195	subsidiary	V16	2	V358	3	2->3
LR1198	subsidiary	V16	2	V239	3	2->3
LR1201	subsidiary	V16	2	V352	3	2->3
LR1206	subsidiary	V16	2	V347	3	2->3
LR1209	subsidiary	V16	2	V343	3	2->3
LR1215	subsidiary	V16	2	V276	3	2->3
LR1219	subsidiary	V16	2	V337	3	2->3
LR1227	subsidiary	V16	2	V362	3	2->3
LR1068	affiliated company	V16	2	V638	5	2->5
LR2861	subsidiary	V16	2	V638	5	2->5
LR1191	affiliated company	V16	2	V734	6	2->6
LR2894	subsidiary	V16	2	V735	6	2->6
LR1590	subsidiary	V16	2	V53	7	2->7
LR934	affiliated company	V16	2	V535	8	2->8
LR757	Subsidiary company	V16	2	V2	9	2->9
LR1050	affiliated company	V16	2	V17	9	2->9
LR2801	subsidiary	V16	2	V2	9	2->9
LR358	Parent company	V239	3	V16	2	3->2
LR359	Parent company	V239	3	V16	2	3->2

Table 7 (continued)

Relation ID	Relation type	Source node ID	Source comm.	Target node ID	Target comm.	Comm. link
LR449	affiliated company	V239	3	V328	2	3->2
LR575	Parent company	V264	3	V16	2	3->2
LR579	Parent company	V250	3	V16	2	3->2
LR1197	Parent company	V358	3	V16	2	3->2
LR1203	Parent company	V352	3	V16	2	3->2
LR1208	Parent company	V347	3	V16	2	3->2
LR1211	Parent company	V343	3	V16	2	3->2
LR1218	Parent company	V276	3	V16	2	3->2
LR1221	Parent company	V337	3	V16	2	3->2
LR1229	Parent company	V362	3	V16	2	3->2
LR167	subsidiary	V52	4	V10	11	4->11
LR71	Parent company	V52	4	V53	7	4->7
LR1069	Parent company	V638	5	V16	2	5->2
LR1077	supplier	V638	5	V646	6	5->6
LR1078	supplier	V638	5	V647	6	5->6
LR1079	supplier	V638	5	V648	6	5->6
LR2898	Parent company	V735	6	V16	2	6->2
LR1591	Parent company	V53	7	V16	2	7->2
LR1611	Other participating companies	V53	7	V52	4	7->4
LR1622	affiliated company	V53	7	V52	4	7->4
LR1663	subsidiary	V53	7	V52	4	7->4
LR19	Other participating companies	V2	9	V18	10	9->10
LR10	Other participating companies	V2	9	V10	11	9->11
LR11	Other participating companies	V2	9	V11	12	9->12
LR16	Parent company	V2	9	V16	2	9->2
LR17	Parent company	V2	9	V16	2	9->2

5.3 Dynamic Risk Propagation Analysis of M2RPA

To dynamically simulate the risk propagation process under the proposed M2RPA framework, we establish the following initial parameters. First, regarding the initial shock, we select node V53 as the risk source to trigger the contagion. Second, the risk propagation threshold Θ is set to 0.9 to mathematically determine whether an affected node transitions into an infected state.

Based on these initial settings, we employ the multi-stage, multi-level dynamic risk transmission method described in Section 4.2, integrated with our multi-path, multi-risk coupled transmission influence degree model, to analyze the dynamic risk impacts within the capital market entity network. **Table 8** presents the multi-path, multi-risk coupling influence intensities and the resulting cascade for the first three degrees of connections originating from V53.

The simulation results clearly delineate the scale of affected and infected nodes at different propagation stages. Initially, within the first-degree connections, 71 nodes are affected by the direct shock, among which 36 exceed the threshold and become infected. Subsequently, the contagion reaches its peak in the second-degree connections, rapidly expanding to 137 affected nodes and 90 infected nodes. However, as the propagation advances to the third-degree connections, the contagion momentum wanes; although 25 nodes are affected, none breach the risk threshold to become infected. Consequently, as the risk transmission chain extends, the dynamic impact of the risk exhibits a distinct trajectory: an initial severe amplification followed by a gradual attenuation.

Table 8 The calculation results of the multi-level, multi-path risk coupling risk influence intensity values for node V53

Transfer level	**The number of the affected nodes**	**The top 5 affected nodes**	**Influence intensity value**	**Infected or not**	**The number of the infected nodes**
1	71	52	0.9500	yes	36
		1068	0.7000	no	
		1072	0.9000	yes	
		1081	0.9500	no	
		1082	0.9000	yes	
		...	...	...	
2	137	10	0.9025	yes	90
		54	0.7600	no	
		55	0.6650	no	
		60	0.8550	no	
		74	0.9025	yes	
		...	...	...	
3	25	190	0.6317	no	0
		191	0.8574	no	

Table 8 (continued)

Transfer level	The number of the affected nodes	The top 5 affected nodes	Influence intensity value	Infected or not	The number of the infected nodes
		200	0.3791	no	
		205	0.8123	no	
		215	0.8123	no	
		...	...	...	

Table 9 presents the statistical results of the multi-stage, multi-level risk transmission within the capital market entity network triggered by the initial infection of node V53. In the first propagation stage, the risk affects 233 nodes, with 126 becoming infected (as detailed in Table 8). Subsequently, in the second stage, 72 nodes are affected and 12 are infected, whereas the third stage sees no further infections.

Overall, the initial shock at V53 impacts a total of 305 nodes (233 + 72) across the network, culminating in 138 infected nodes (126 + 12). This translates to a notable risk infection rate of 45.25% (138/305).

These findings provide a critical theoretical insight: although conventional static analysis does not classify V53 as a typical risk super-spreader, dynamic simulation reveals its substantial influence weights on nodes up to three degrees of separation, significantly amplifying the initial infection scale. Furthermore, because these newly infected nodes also possess strong influence over their respective connections, a cascading multi-stage risk transmission is effectively sustained. Consequently, node V53 can be definitively identified as a hidden but potent "multi-stage risk disseminator" within the network.

Table 9 Multi-stage risk transmission statistics for node V53

Risk transmission stage	The number of the affected nodes	The number of the infected nodes	The top 5 nodes by influence intensity value
0	/	1	V53
1	233	126	V52,V1081,V1085,V1086,V1092
2	72	12	V191,V193,V195,V201,V205
3	0	/	/

Based on the static network structure analysis, node V16 exhibits high out-degree and in-degree, suggesting it is highly likely to act as both a super-vulnerable node and a primary transmission hub. Given its high betweenness centrality, this node theoretically possesses the topological potential to trigger cascading reactions across multiple communities.

Table 10 presents the statistical data on the multi-stage, multi-level risk propagation triggered by an initial risk outbreak at node V16, V18, V1145.

Considering the node V16, the dynamic analysis results partially confirm its role as a super-spreader: in the first propagation stage alone, the shock widely affects a massive 2,015 nodes, among which 266 become infected. This yields a relatively low risk infection rate of 13.2% (266/2,015).

However, unlike the sustained propagation observed previously, the contagion initiated by V16 dissipates rapidly, ceasing entirely after just two stages. This limited depth occurs because V16 primarily transmits risk through single-path connections to the majority of its within-three-degree neighbors, resulting in a relatively weak cumulative impact intensity. Furthermore, the newly infected nodes exhibit limited secondary transmission capability; they possess only 158 within-three-degree connected nodes in total, and their associated impact weights remain low. Consequently, despite its broad initial reach, the outbreak at V16 lacks the momentum to trigger a sustained, multi-stage risk propagation.

Table 10 Multi-stage risk transmission statistics for node V16,V18,V1145

NodeID	**Risk transmission stage**	**The number of the affected nodes**	**The number of the infected nodes**	**The top 5 nodes by influence intensity value**
V16	0	/	1	V16
	1	2015	266	V1,V224,V225,V227,V233
	2	158	0	/
V18	0	/	1	V18
	1	32	4	V2021,V2022,V2024,V2025, V2044
	2	0	/	/
V1145	0	/	1	V1145
	1	758	376	V1159,V1160,V1163,V1164, V1178
	2	0	/	/

Considering the node V18, during the first stage of propagation, only 32 nodes are affected, resulting in a mere 4 infections. In the subsequent second stage, no further nodes are affected. Consequently, the risk contagion ceases rapidly, and the network restores its normal state after just two stages of transmission and recovery. This dynamic behavior clearly indicates that node V18 functions neither as a highly susceptible entity nor as a significant risk transmitter; its overall cumulative impact on its within-three-degree connected nodes is strictly marginal, posing minimal systemic threat to the network.

Considering the node V1145, it exhibits an exceptionally high out-degree of 758, ranking first across the entire network. Corresponding to this structural prominence,

an initial risk outbreak at V1145 directly infects a substantial 376 nodes. However, within the specific capital market entity network constructed in this study, these newly infected nodes lack subsequent outgoing connections. Consequently, they exert no secondary impact on the broader network, effectively confining the risk fallout of V1145 solely to its localized sub-community.

Nevertheless, the latent systemic threat posed by node V1145 should not be underestimated. In larger networks characterized by higher density and tighter interconnections, a node with such massive direct outreach could easily act as a super-spreader and trigger catastrophic systemic contagion. Therefore, nodes exhibiting such topological characteristics warrant high-priority attention in practical risk prevention and control strategies.

In summary, the comprehensive analysis of these representative nodes (V53, V16, V18, and V1145) reveals a significant divergence between a node's static topological prominence and its actual dynamic risk contagion capability. Traditional network metrics tend to misjudge systemic threats: highly centralized nodes like V16 and V1145, despite their massive initial reach, may fail to trigger prolonged systemic crises due to constrained secondary outward pathways or sub-community isolation. Conversely, structurally unobtrusive nodes like V53 can act as hidden, deep multi-stage spreaders, driving severe cascading failures that evade static detection, while nodes like V18 remain truly marginal. These distinct propagation mechanisms underscore a critical conclusion: Relying solely on static network topology is insufficient and may lead to regulatory blind spots. The dynamic multi-stage, multi-level risk propagation framework proposed in this study is indispensable, as it provides a structurally nuanced and dynamically accurate evaluation of systemic risk, thus offering more precise guidance for proactive market regulation and targeted risk intervention.

6 Conclusions

This study investigates the AI-driven systemic risks posed to capital markets, proposing a novel multidimensional analytical framework based on complex network theory. Given the vast number of market participants and their intricate interrelationships, we constructed a capital market entity network model. By leveraging the DeepSeek large language model, our approach successfully quantified and scored the risk impact intensity of various associations—based on transmission patterns, structural closeness, and causal logic—translating complex qualitative relationships into a robust two-dimensional adjacency matrix.

Based on this constructed network, we systematically evaluated market risks from both static topological and dynamic propagation perspectives:

- Static and Community Analysis: We utilized multidimensional static metrics (including out-degree, in-degree, degree centrality, betweenness centrality, and node strength) to identify key nodes that structurally influence network vulnerability. Furthermore, applying the Leiden community detection algorithm allowed us to partition the network into distinct sub-risk communities. This revealed inter-community transmission patterns and provided a topological basis for localized risk containment.

- Dynamic Multi-Stage Propagation: To overcome the limitations of static assessment, we introduced a three-degree diffusion model to calculate multi-path risk coupling effects. Building upon this, a multi-stage risk transmission algorithm based on multiple heuristic rules was developed. This dynamic approach explicitly identifies affected nodes, assesses localized impacts, and models multi-phase contagion trajectories over time.

Experimental results on a large-scale entity association network validate the effectiveness of the proposed multidimensional framework. The analysis demonstrates a critical divergence between a node's static topological prominence and its actual dynamic contagion capability; relying solely on static metrics can lead to severe regulatory blind spots.

Ultimately, this methodology provides a comprehensive quantitative tool for dynamic risk monitoring, structural visualization, and proactive market regulation. By accurately tracking how localized risks cascade through complex market networks, this study offers actionable evidence for global risk control strategies. Future research may focus on integrating real-time temporal dynamics and high-frequency trading data to further enhance the timeliness of AI-driven risk prediction in capital markets.

References

Acemoglu D, Ozdaglar A, Tahbaz-Salehi A (2015) Systemic risk and stability in financial networks. American Economic Review 105(2):564–608. https://doi.org/10.1257/aer.20130456

Allen F, Gale D (2000) Financial contagion. Journal of Political Economy 108(1):1–33. https://doi.org/10.1086/262109

Barredo Arrieta A, Díaz-Rodríguez N, Del Ser J, et al (2020) Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion 58:82–115

Baruník J, Křehlík T (2018) Measuring the frequency dynamics of financial connectedness and systemic risk. Journal of Financial Econometrics 16(2):271–296

Billio M, Getmansky M, Lo AW, et al (2012) Econometric measures of connectedness and systemic risk in the finance and insurance sectors. Journal of Financial Economics 104(3):535–559

Borgatti SP, Everett MG (2006) A graph-theoretic perspective on centrality. Social Networks 28(4):466–484. https://doi.org/10.1016/j.socnet.2005.11.005

Centola D, Macy M (2007) Complex contagions and the weakness of long ties. American Journal of Sociology 113(3):702–734

Christakis NA, Fowler JH (2009) Connected: The Surprising Power of Our Social Networks and How They Shape Our Lives. Little, Brown and Company, New York

Daníelsson J, Macrae R, Uthemann A (2022) Artificial intelligence and systemic risk. Journal of Banking & Finance 140:106290

Diebold FX, Yilmaz K (2009) Measuring financial asset return and volatility spillovers, with application to global equity markets. The Economic Journal 119(534):158–171

Doerr S, Gambacorta L, Serena Garralda JM (2021) Big data and machine learning in central banking. BIS Working Papers 930, Bank for International Settlements, Basel

Elliott M, Golub B, Jackson MO (2014) Financial networks and contagion. American Economic Review 104(10):3115–3153. https://doi.org/10.1257/aer.104.10.3115

Financial Stability Board (2017) Artificial intelligence and machine learning in financial services. Tech. rep., Financial Stability Board

Gai P, Kapadia S (2010) Contagion in financial networks. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences 466(2120):2401–2423. https://doi.org/10.1098/rspa.2009.0410

Goldstein I, Jiang W, Karolyi GA (2019) To FinTech and beyond. Review of Financial Studies 32(5):1647–1661

Gualdi S, Riccetti L (2024) Herding, minority game and market crashes in a multi-agent model with AI-driven trend followers. Journal of Economic Dynamics and Control 159:104789. https://doi.org/10.1016/j.jedc.2023.104789

Hansen AL, Lee SJ (2025) Financial stability implications of generative AI: Taming the animal spirits. Finance and economics discussion series, Board of Governors of the Federal Reserve System, Washington, DC

International Monetary Fund (2024) Global financial stability report, steadying the course: Uncertainty, artificial intelligence, and financial stability. Tech. rep., International Monetary Fund, Washington, DC

Kou G, Akbani Z, Xiao F (2021) Fintech and big data analytics in the financial sector: a systematic literature review. Technological Forecasting and Social Change 166:120612. https://doi.org/10.1016/j.techfore.2021.120612

Poledna S, Molina-Borboa JL, Martínez-Jaramillo S, et al (2015) The multi-layer network nature of systemic risk and its implications for the costs of financial crises. Journal of Financial Stability 20:70–81

So MKP, Chu AMY, Chan TWC (2021) Impacts of the COVID-19 pandemic on financial market connectedness. Finance Research Letters 38:101864

Traag VA, Waltman L, van Eck NJ (2019) From Louvain to Leiden: guaranteeing well-connected communities. Scientific Reports 9(1):5233

Vitali S, Glattfelder JB, Battiston S (2011) The network of global corporate control. PLoS ONE 6(10):e25995. https://doi.org/10.1371/journal.pone.0025995