Contagion in Financial Networks

23.01.2020
Source (published March 2010):

Working Paper No. 383
Contagion in financial networks
Prasanna Gai\(^1\) and Sujit Kapadia\(^2\)

Abstract

This paper develops an analytical model of contagion in financial networks with arbitrary structure. We explore how the probability and potential impact of contagion is influenced by aggregate and idiosyncratic shocks, changes in network structure, and asset market liquidity. Our findings suggest that financial systems exhibit a robust-yet-fragile tendency: while the probability of contagion may be low, the effects can be extremely widespread when problems occur. And we suggest why the resilience of the system in withstanding fairly large shocks prior to 2007 should not have been taken as a reliable guide to its future robustness.

Key words: Contagion, network models, systemic risk, liquidity risk, financial crises.

JEL classification: D85, G01, G21.
The model

Network structure:

- Financial network with $n$ financial intermediaries (vertices, 'banks').
- Interbank exposures define edges (directed and weighted).
- In-degree: interbank assets (owed to the bank by a counterparty).
- Out-degree: interbank liabilities (owed to a counterparty by the bank).
- Assumption: Network is random in all aspects other than its degree distribution (configuration model).
Configuration model for directed networks

Specify a double degree sequence for each vertex:
- in-degree sequence $j_i$.
- out-degree sequence $k_i$.

Obvious condition:

$$\sum_i k_i = \sum_i j_i.$$ 

Create network by randomly connecting stubs (matching), and consider the ensemble of all possible matchings, with each matching appearing with equal probability.
Configuration model for directed networks

Joint degree distribution:

▶ $p_{jk}$ denotes the fraction of vertices having in-degree $j$ and out-degree $k$.

It follows:

▶ In-degree distribution:

$$p_{j}^{\text{in}} = \sum_{k=0}^{\infty} p_{jk}.$$ 

▶ Out-degree distribution:

$$p_{k}^{\text{out}} = \sum_{j=0}^{\infty} p_{jk}.$$
Configuration model for directed networks

Average degree:

\[ \langle j \rangle = \sum_j j p_j^{in} = \sum_k k p_k^{out} = \langle k \rangle \]

Excess degree distribution: Distribution of number of outgoing edges leaving a vertex reached by following a randomly chosen incoming edge (other definitions possible):

\[ r_{jk} = \frac{j \cdot p_{jk}}{\sum_{j,k} j \cdot p_{jk}} = \frac{j \cdot p_{jk}}{\langle k \rangle}. \]
Vulnerable banks

Balance sheet:

- Interbank assets $A_{i}^{IB}$.
- Illiquid external assets $A_{i}^{M}$.
- Interbank liabilities $L_{i}^{IB}$.
- Customer deposits $D_{i}$.

Assumption: Total interbank asset position of every bank is evenly distributed over each of its incoming edges.

Note: Interbank liabilities are endogenously determined by the interbank assets:

$$L_{i}^{IB} = \sum_{l \in \mathcal{N}_{i}^{\text{out}}} \frac{A_{l}^{IB}}{j_{l}}.$$
Vulnerable banks

Balance sheet:
- Interbank assets $A_{i}^{IB}$.
- Illiquid external assets $A_{i}^{M}$.
- Interbank liabilities $L_{i}^{IB}$.
- Customer deposits $D_{i}$.

Condition for bank $i$ to be solvent:

$$(1 - \phi)A_{i}^{IB} + qA_{i}^{M} - L_{i}^{IB} - D_{i} > 0.$$ 

Here $\phi$ denotes the fraction of defaulted banks with obligations to bank $i$, and $q$ is the resale price of the illiquid assets.
Vulnerable banks

Condition for bank $i$ to be solvent:

$$(1 - \phi) A_i^{IB} + q A_i^M - L_i^{IB} - D_i > 0.$$  

Here $\phi$ denotes the fraction of defaulted banks with obligations to bank $i$, and $q$ is the resale price of the illiquid assets.

Equivalently for $A_i^{IB} \neq 0$:

$$\phi < \frac{K_i - (1 - q) A_i^M}{A_i^{IB}},$$

where $K_i = A_i^{IB} + A_i^M - L_i^{IB} - D_i$ is the bank’s capital buffer.
Vulnerable banks

Solvency condition:

\[ \phi < \frac{K_i - (1 - q)A_i^M}{A_i^{IB}} , \]

where \( K_i = A_i^{IB} + A_i^M - L_i^{IB} - D_i \) is the bank’s capital buffer.

If a single counterparty defaults, each connected bank \( i \) loses a fraction \( 1/j_i \) of their interbank assets. It follows that default can spread if there is a neighbouring bank for which

\[ \frac{K_i - (1 - q)A_i^M}{A_i^{IB}} < \frac{1}{j_i} \quad \text{or} \quad K_i - (1 - q)A_i^M < \frac{A_i^{IB}}{j_i} . \]

Such a bank is called vulnerable (vs. safe).
Vulnerable banks

Solvency condition:

\[ \phi < \frac{K_i - (1 - q)A_i^M}{A_i^{IB}} , \]

where \( K_i = A_i^{IB} + A_i^M - L_i^{IB} - D_i \) is the bank’s capital buffer.

If the capital buffer is taken to be taken a random variable, a bank with in-degree \( j > 0 \) is vulnerable with probability

\[ v_j = P \left[ \frac{K_i - (1 - q)A_i^M}{A_i^{IB}} < \frac{1}{j} \right] . \]

It holds \( v_j \leq v_{j'} \) for \( j > j' \).
Vulnerable cluster

Follow a randomly chosen edge to a vulnerable bank at its end, and then to every other vulnerable bank reachable from that end. This set of banks is defined as the (outgoing) vulnerable cluster at the end of a randomly chosen edge.

The corresponding generating function for the probability of reaching an outgoing vulnerable cluster of given size (in terms of the number of vulnerable banks) is denoted by

\[ h_1(z) = \sum_{s=0}^{\infty} \sigma_s z^s. \]
Vulnerable cluster

We need two generating functions:

- Probability distribution for randomly choosing a vulnerable bank with out-degree $k$:

  $$g_0(z) = \sum_{k=0}^{\infty} \left( \sum_{j=0}^{\infty} v_j p_{jk} \right) \cdot z^k =: \sum_{k=0}^{\infty} \tilde{p}_k^\text{out} z^k.$$

- Probability distribution for reaching a vulnerable bank with out-degree $k$, when following a randomly chosen incoming edge:

  $$g_1(z) = \sum_{k=0}^{\infty} \left( \sum_{j=0}^{\infty} v_j r_{jk} \right) \cdot z^k =: \sum_{k=0}^{\infty} \tilde{r}_k^\text{out} z^k.$$
Vulnerable cluster

It holds:

\[ h_1(z) = P[\text{reach safe bank}] + z \sum_{k=0}^{\infty} \tilde{r}_k^{\text{out}} [h_1(z)]^k \]

\[ = 1 - g_1(1) + zg_1(h_1(z)). \]

The size of the vulnerable cluster to which a randomly chosen bank belongs is generated by:

\[
h_0(z) = P[\text{bank safe}] + z \sum_{k=0}^{\infty} \tilde{\rho}^\text{out}_k [h_1(z)]^k
\]

\[
= 1 - g_0(1) + zg_0(h_1(z)).
\]

Vulnerable cluster

Using

\[ h'_1(1) = \frac{g_1(1)}{1 - g'_1(1)} , \]

the average size of a vulnerable cluster is calculated as

\[ h'_0(1) = \frac{d}{dz} \left[ 1 - g_0(1) + zg_0(h_1(z)) \right]_{z=1} \]
\[ = g_0(1) + g'_0(1)h'_1(1) \]
\[ = g_0(1) + \frac{g'_0(1)g_1(1)}{1 - g'_1(1)} . \]

Phase transition:

\[ g'_1(1) = 1 . \]
Giant vulnerable cluster

Phase transition:

\[ g_1'(1) = 1. \]

Recall that \( g_1'(1) \) is the average out-degree of a vulnerable first neighbour:

\[
g_1'(1) = \sum_{k=0}^{\infty} k \tilde{r}_k^{\text{out}} \\
= \sum_{k=0}^{\infty} k \cdot \left( \sum_{j=0}^{\infty} v_j \cdot \frac{j \cdot p_{jk}}{\langle k \rangle} \right) \\
= \frac{1}{\langle k \rangle} \left( \sum_{j,k=0}^{\infty} k \cdot j \cdot v_j \cdot p_{jk} \right). \]
Giant vulnerable cluster

Giant vulnerable component appears for

\[ g'_1(1) > 1 , \]

or equivalently

\[ \sum_{j,k=0}^{\infty} k \cdot j \cdot v_j \cdot p_{jk} > \langle k \rangle , \]

or

\[ \sum_{j,k} (2 \cdot j \cdot k \cdot v_j - j - k) \cdot p_{jk} > 0 . \]

This contains the condition for the appearance of a giant component in both directed and undirected networks.
Giant vulnerable cluster

Giant vulnerable component appears for

$$\sum_{j,k} (2 \cdot j \cdot k \cdot v_j - j - k) \cdot p_{jk} > 0.$$ 

Recall:

$$v_j = P \left[ \frac{K_i - (1 - q)A_i^M}{A_i^{IB}} < \frac{1}{j} \right].$$

Probability of contagion (existence of a giant vulnerable cluster) is non-monotonic in $\langle k \rangle$:

- Initially, higher connectivity increases the size of the vulnerable cluster ('risk-spreading').
- Eventually, for high enough connectivity the number of vulnerable banks is sufficiently reduced ('risk-sharing').
Probability and spread of contagion

- Occurrence of a *contagion window*, that is a lower and an upper phase transition.
- Size of the vulnerable cluster is either curtailed by limited connectivity or by the presence of a high fraction of safe banks.
- 'Safe banks' can default if more than one of their neighbours fail.
- Near the lower phase transition: Nearly all banks are likely to be vulnerable and the size of the giant vulnerable cluster corresponds closely to the size of the connected component of the network.
- Near the upper phase transition: Robust-yet-fragile tendency, with episodes of contagion occurring rarely, but spreading very widely when they do take place.
Numerical simulations

- Uniform (Poisson) random graphs.
- \( n = 1000 \) banks.
- Identical asset positions and capital buffers.
- 1000 realisations of the network for each value of \( \langle k \rangle \).
- Shock one bank at random, which defaults on all of its interbank liabilities. Consequently, neighbouring banks may default if their capital buffer is insufficient to cover their losses. These failed banks then also default on all of their interbank liabilities (iterative process).
- Count only episodes in which over 5% of the system defaults.
Numerical simulations

Here 'Extent of contagion' is *conditional* on contagion over the 5% threshold.

Numerical simulations

Here 'Extent of contagion' is *conditional* on contagion over the 5% threshold.

Numerical simulations

Here 'Extent of contagion' is *conditional* on contagion over the 5% threshold.

Liquidity risk

Second potential source of contagion:
▶ If a bank defaults, all its external assets are sold onto the market.
▶ Price of the illiquid assets falls.
▶ External assets of all banks are marked to market to reflect the new asset price.
▶ Bank’s capital buffers are reduced, possibly making some banks vulnerable.

The incorporation of liquidity risk magnifies the extent of contagion when it breaks out, also widening the contagion window.
Contagion in financial networks – conclusion

- Model based on random graphs.
- Analytical approach using generating functions.
- Occurrence of a *contagion window* with respect to the connectivity of the network.
- *Robust-yet-fragile* property for higher connectivity in the contagion window.