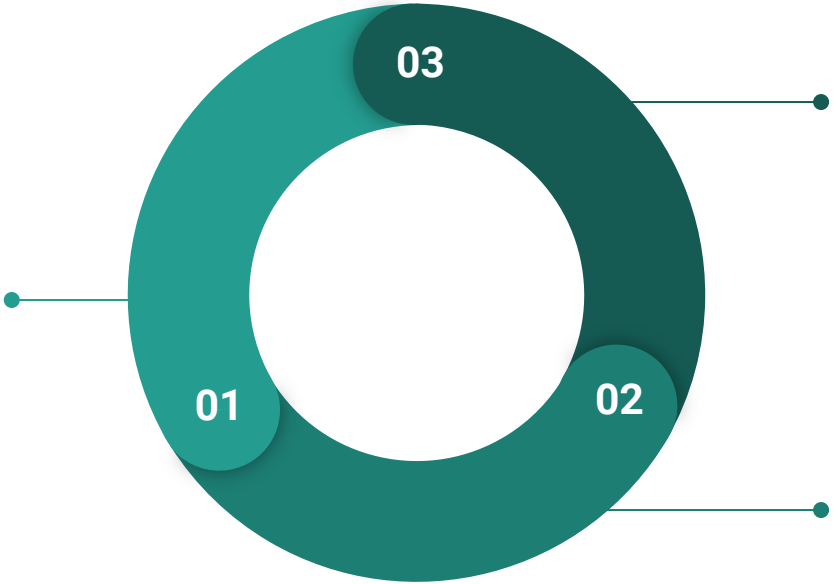
FNA

Resilience against cyber attacks

Components of Cyber Resilience

1. Preventing

Ensuring that cyber attacks don't access internal systems, red team testing, etc.



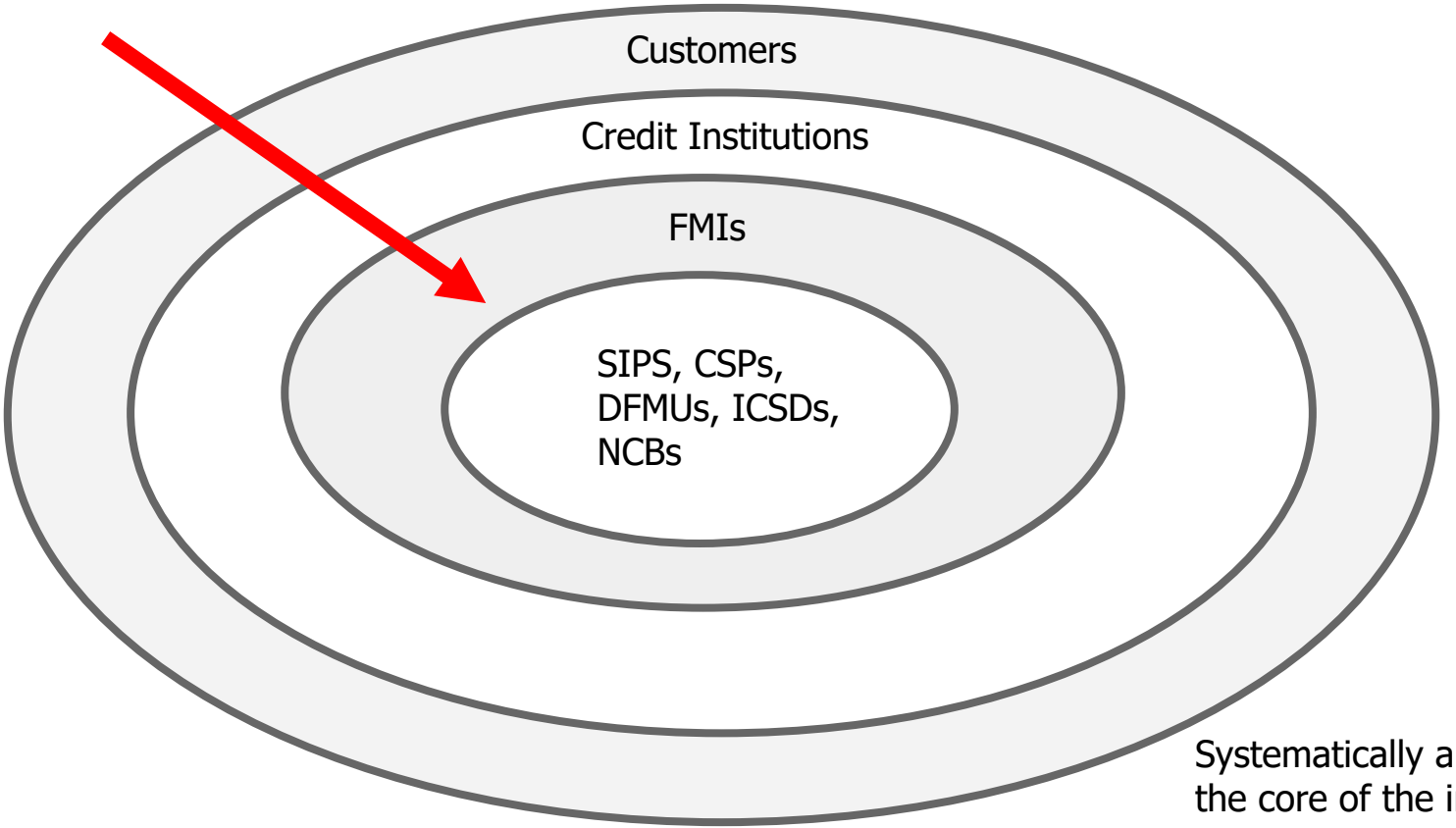
3. Recovering

Methods and processes to ensure recovery from successful attacks and improving resilience towards them,

2. Detecting

Monitoring and alerting about possible intrusions, and investigating incidents.

Cyber Attackers are Penetrating the Financial Sector Core



Systematically approaching the core of the industry

Credit: Wiebe Ruttenberg (ECB)

Increasing number of Cybersecurity Breaches

$81M "Bangladesh Bank Heist" at FRBNY, 2016

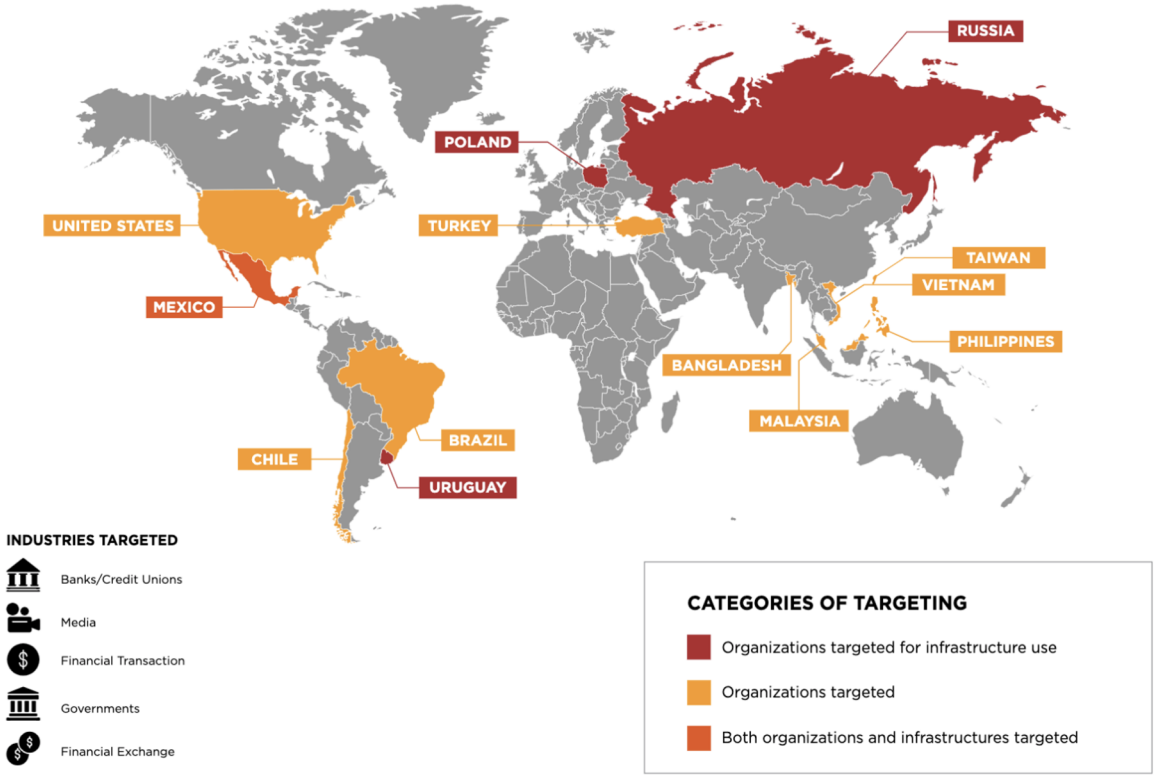
$6M Theft at Russian Central Bank, 2018

$15M Cyber incident in SPEI, Mexico, 2018

Bank Negara Malaysia detected unauthorised fund transfers, 2018

Cyber attacks are often state sponsored

Figure 1. APT38 global targeting.

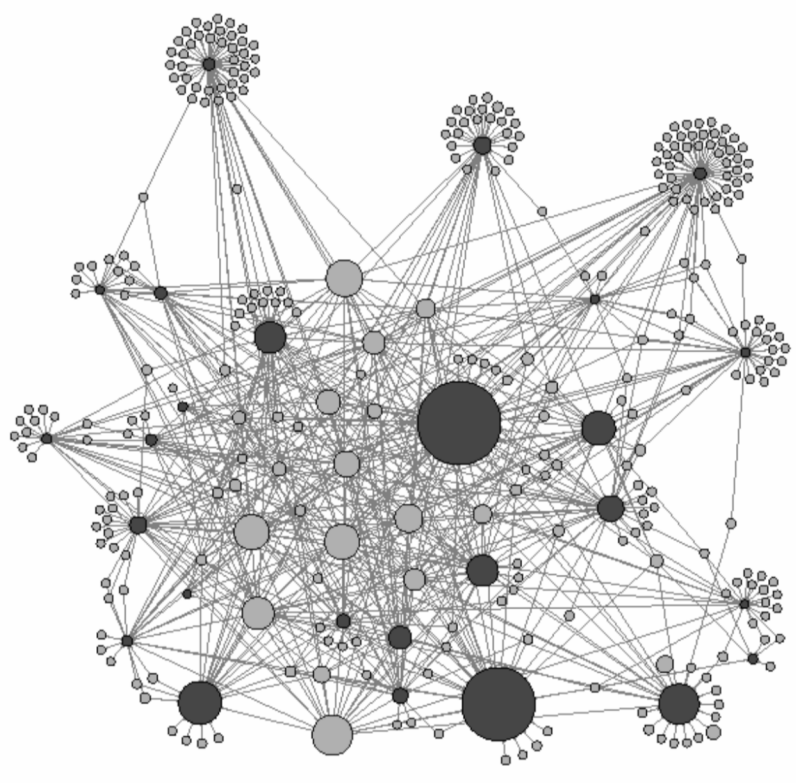


APT38
(Advanced Persistent Threat)

"APT38 is a financially motivated North Korean regime-backed group responsible for conducting destructive attacks against financial institutions, as well as some of the world's largest cyber heists"

- FireEye Report

CPMI-IOSCO - Driving Resilience in FMIs



"FMIs should **immediately** take necessary steps (....) to improve their cyber resilience, taking into account this Guidance."

"FMIs should also, **within 12 months** of the publication of this Guidance, have developed concrete plans to improve their capabilities in order to meet the two-hour RTO."

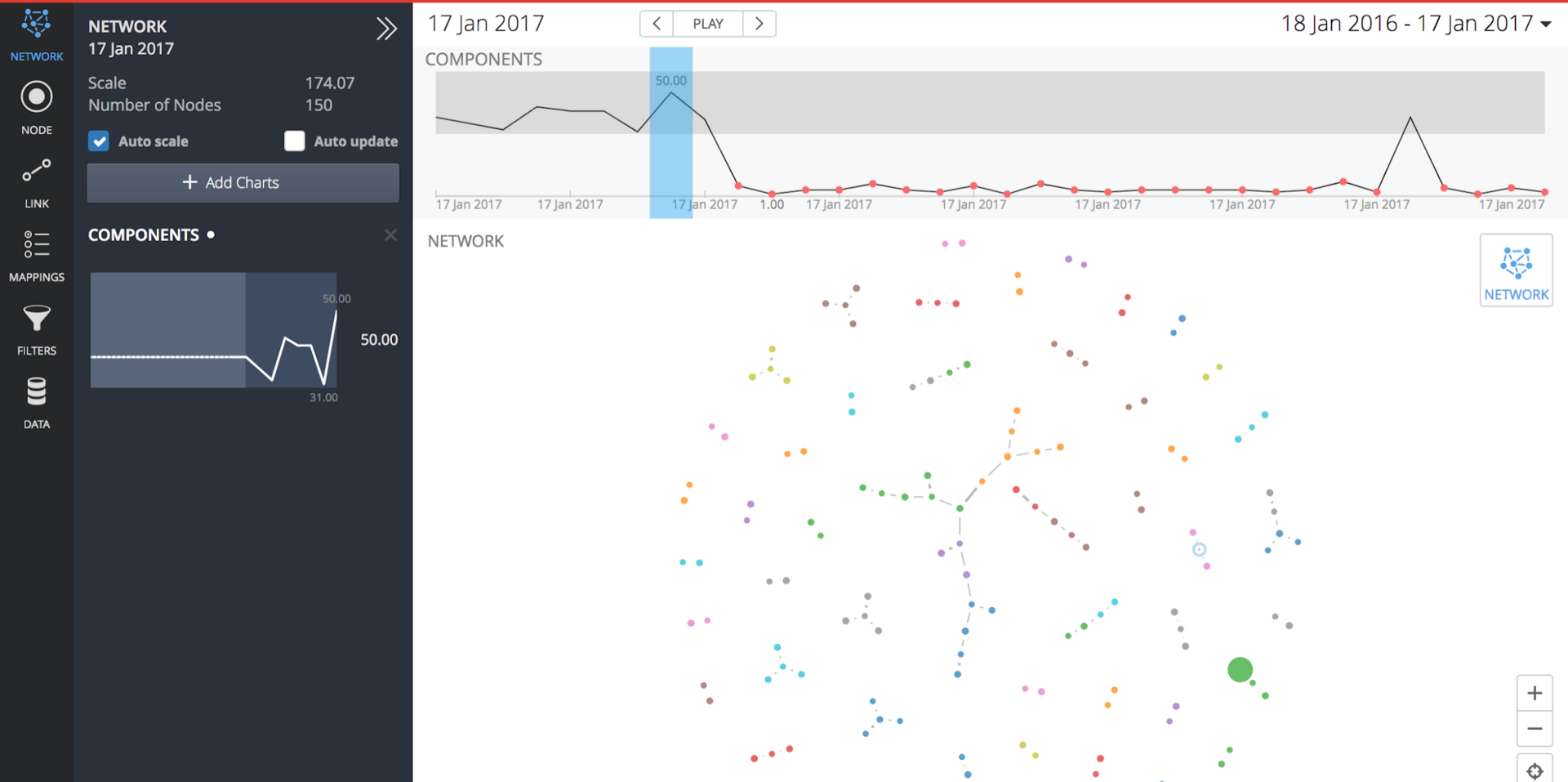
"**Testing** is an integral component of any cyber resilience framework."

CPMI-IOSCO Guidance on Cyber Resilience for FMIs (June 2016)

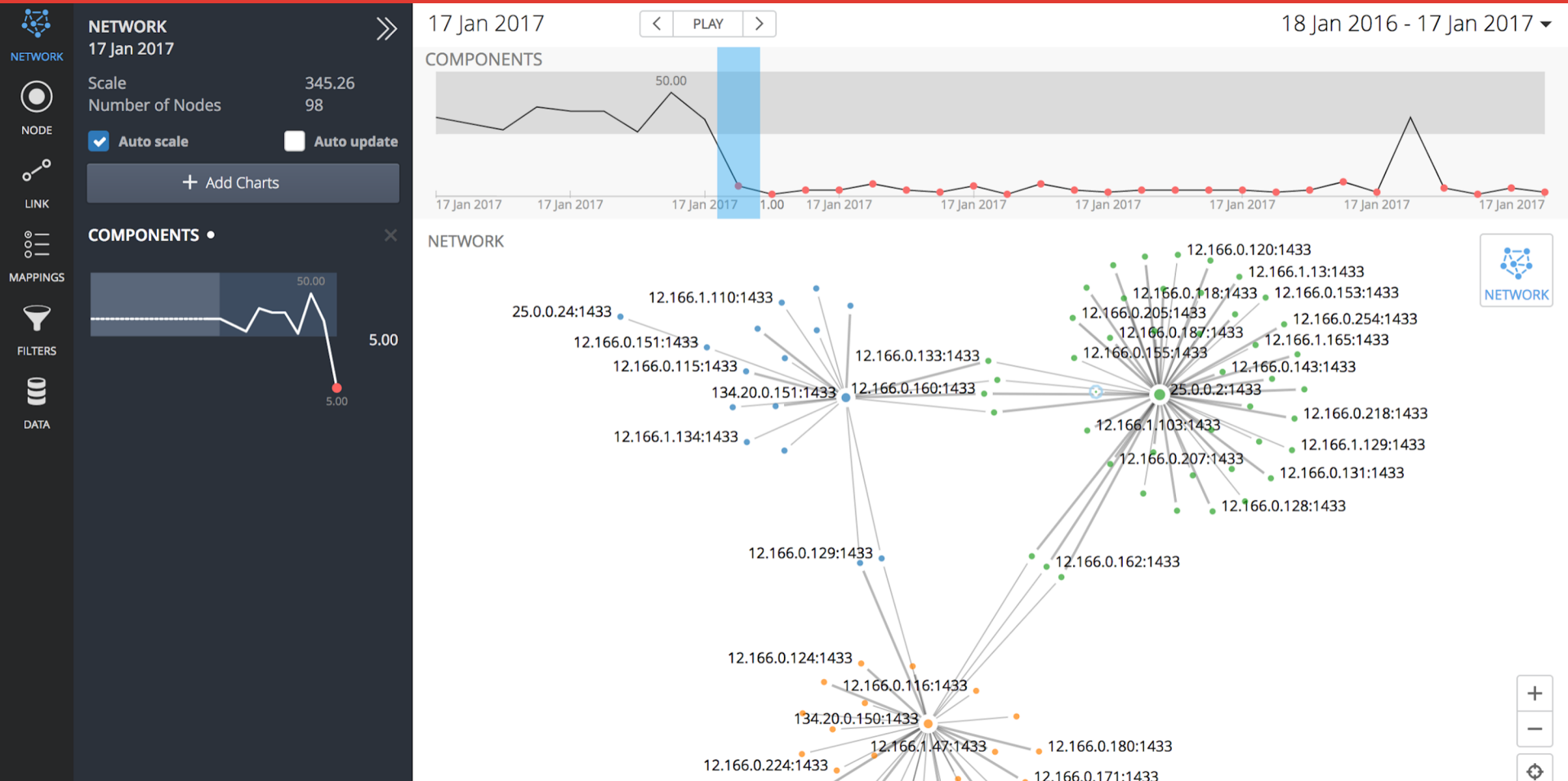
FNA

Monitoring DDoS attacks

Detect Anomalies in Cyber Networks in Real-time



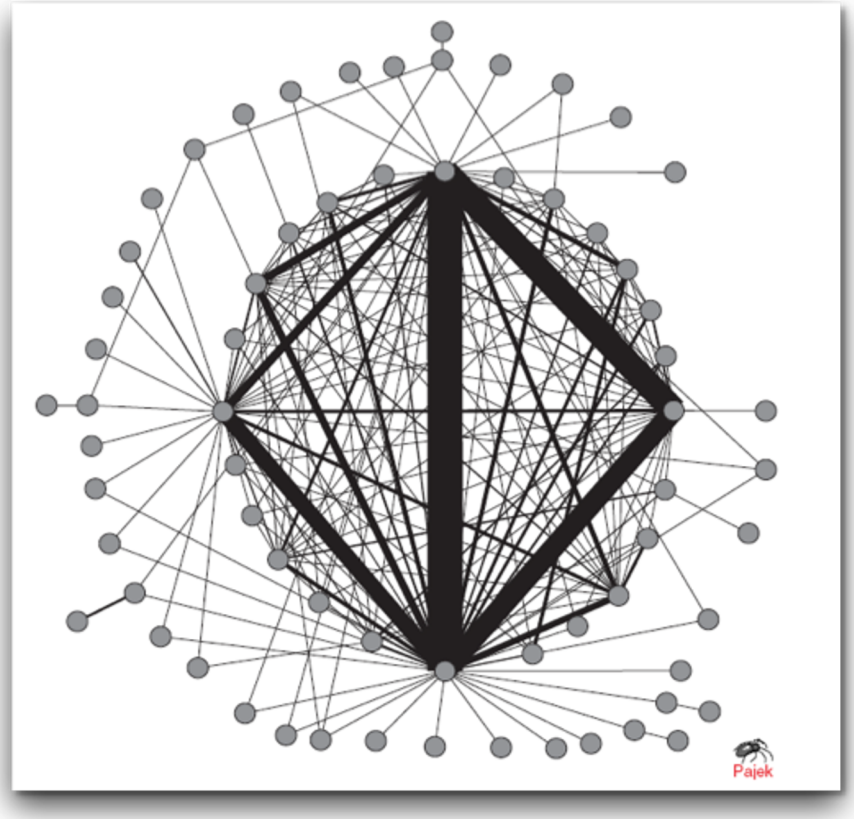
Identify Patterns of DDoS attacks



FNA

Mapping Financial Networks

First Financial Networks



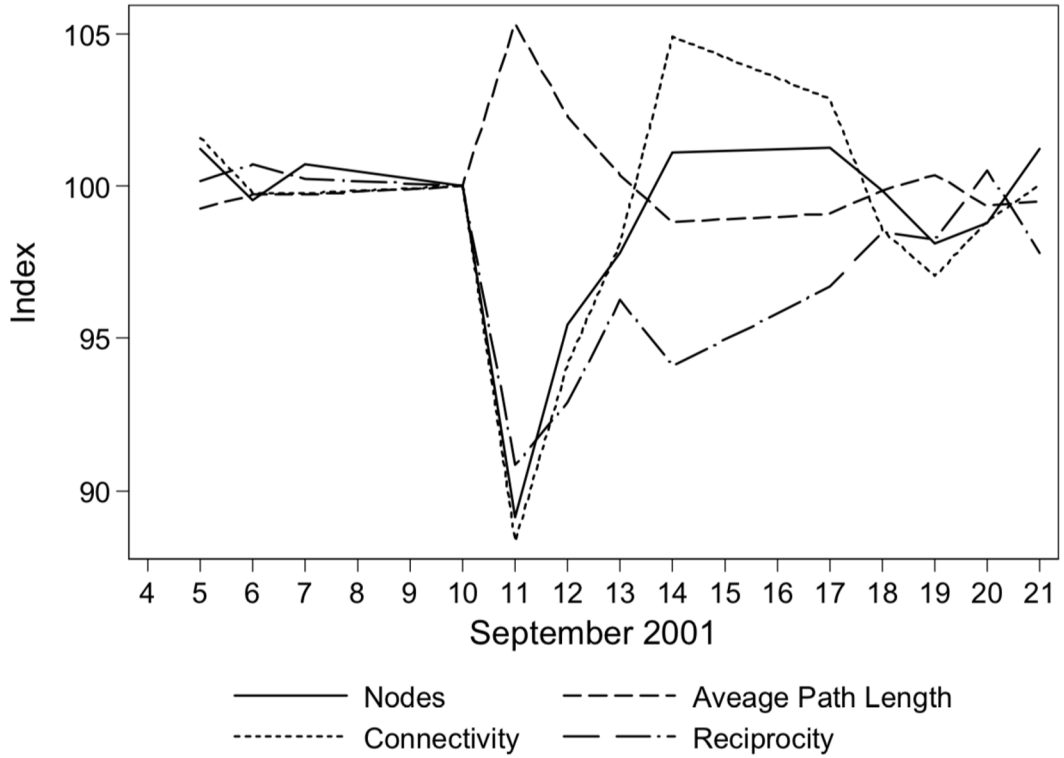
Fedwire Interbank Payment Network (Fall 2001) was one of the first network views into any financial system.

Of a total of around 8000 banks, the 66 banks shown comprise 75% of total value. Of these, 25 banks completely connected

The research was subsequently used e.g. in congressional hearings to showcase the type of information that should be collected by financial institutions after the financial crisis.

Soramaki, K. M Bech, J. Arnold, R.J. Glass and W.E. Beyeler, The Topology of Interbank Payment Flows, Physica A, Vol. 379, pp 317-333, 2007.

Impact of 9/11 Terrorist Attacks on the Network



Note: 100 = September 10th, 2001.

Cyber Risks now more likely than Terrorism

"The next crisis might not come from a financial shock at all. The more likely culprit: a cyber attack that causes disruptions to financial services capabilities, especially payments systems, around the world."

- "How a Cyber Attack Could Cause the Next Financial Crisis" by Paul Mee & Til Schuermann, HBR 2018

FNA

Interconnectedness in the
Global System of CCPs

Motivation

The **New Systemic Risk**

Three CCP failures in the past (Paris, Kuala Lumpur and Hong Kong)

Interest by regulators, CCPs and members.

Especially with tie in to Cyber, IT and other operational risks.

"*They [CCPs] are not equipped, however, to test the impact of their failure on the financial system as a whole nor are they equipped to assess the potential contagion effect on other members of a given member's failure.*"

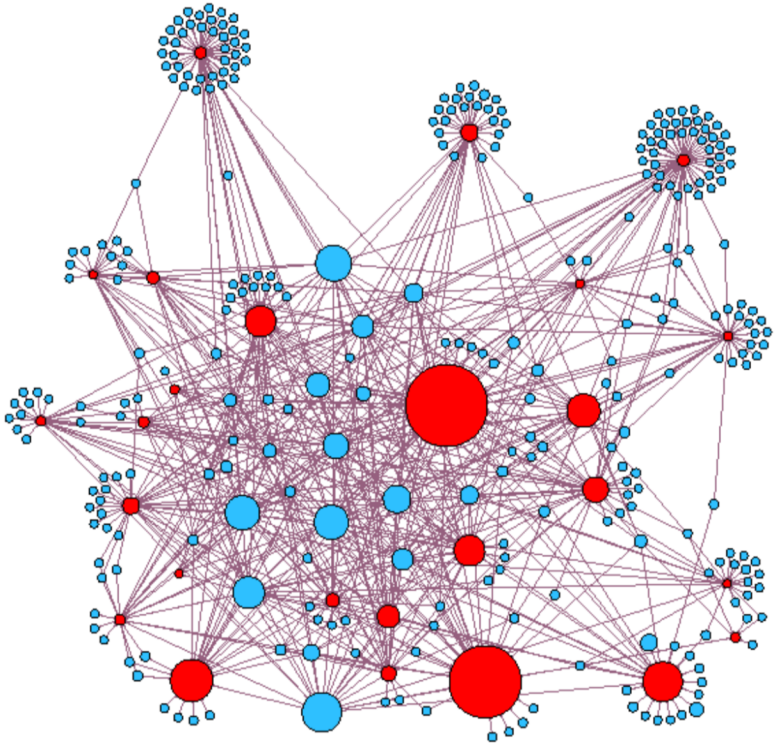
Cox & Steigerwald (2018)

Scope of Analysis

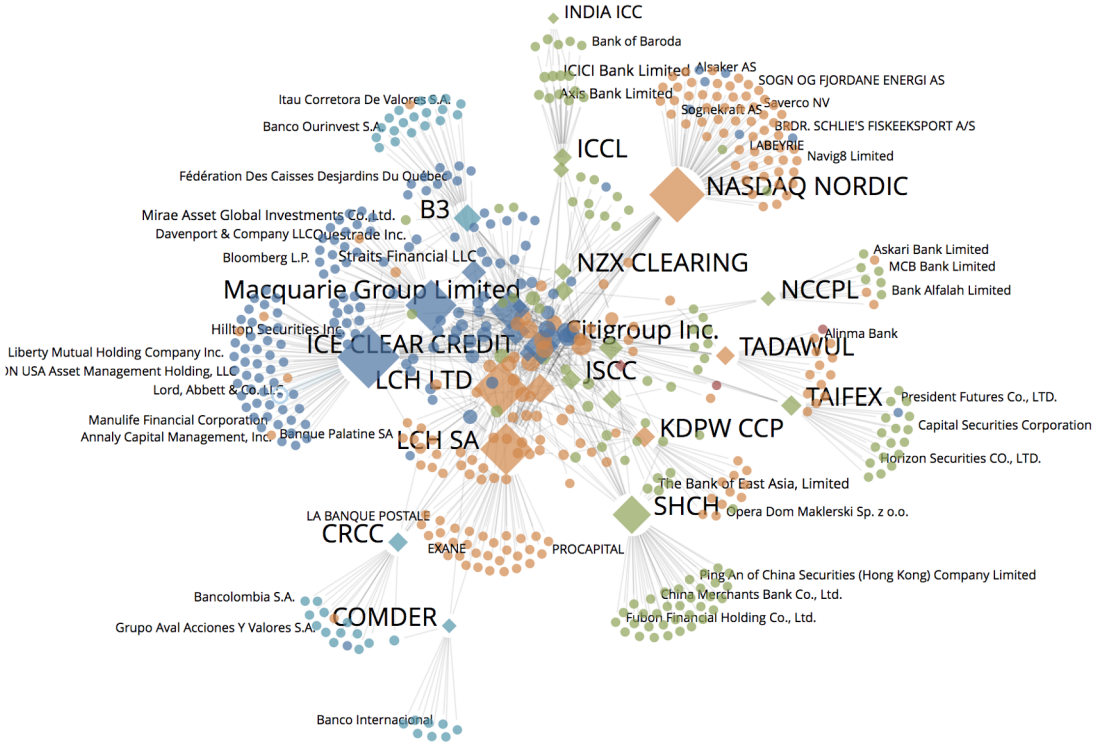
Comparison with BIS "Analysis of Central Clearing Interdependencies" (2018)

	BIS (2018)	**FNA (2018)**
CCPs	26	29
Clearing Members	n/a	813
Parent Organizations	306	495
Roles	7 (member, settlement, LOC, ...)	1 (member)

Private vs Public Data



BIS (2018)



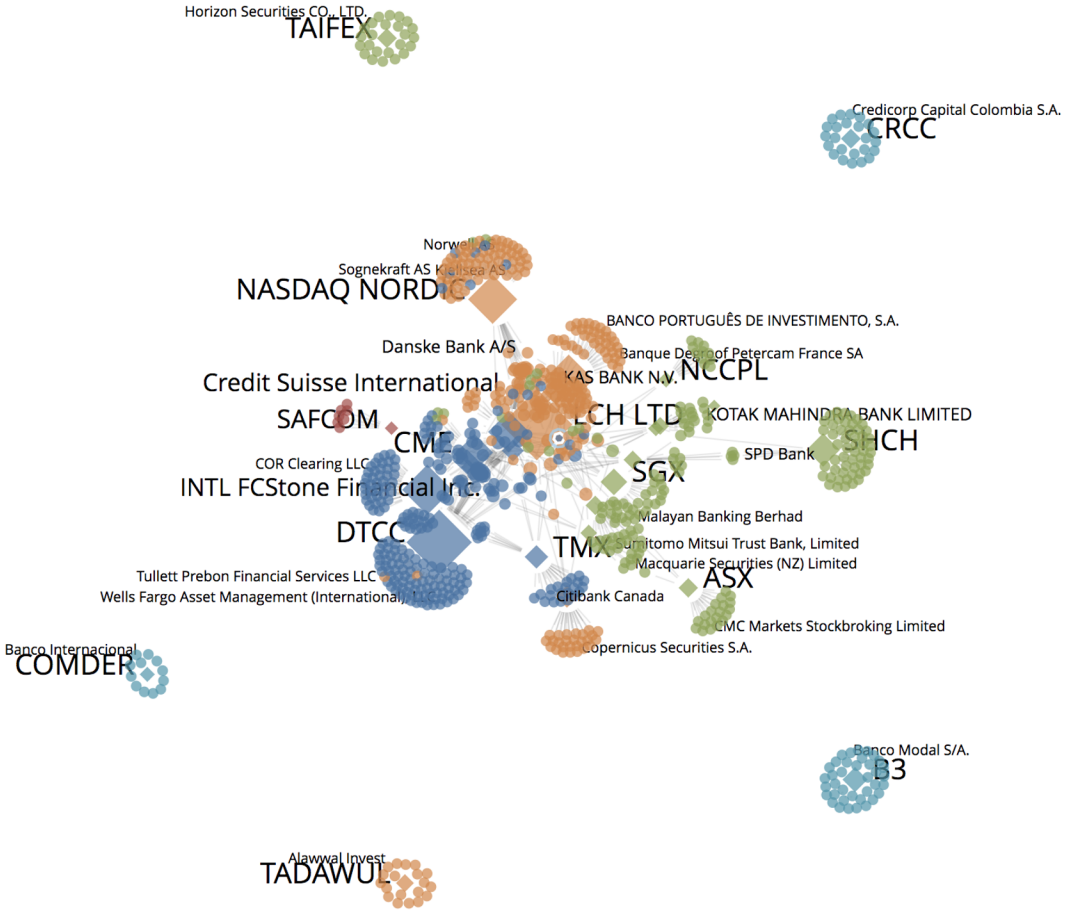
FNA (2018)

CCP Interconnectedness - Subsidiary Level

We see CCPs (diamonds) and their members (circles) from different regions:

- North America (blue)
- Europe and Middle East (orange)
- Asia and Pacific (green)
- Latin America (light blue)
- Africa (red)

On subsidiary level, we see a tight core with peripheral CCPs and a number of completely disconnected CCPs from Latin America and Middle East.

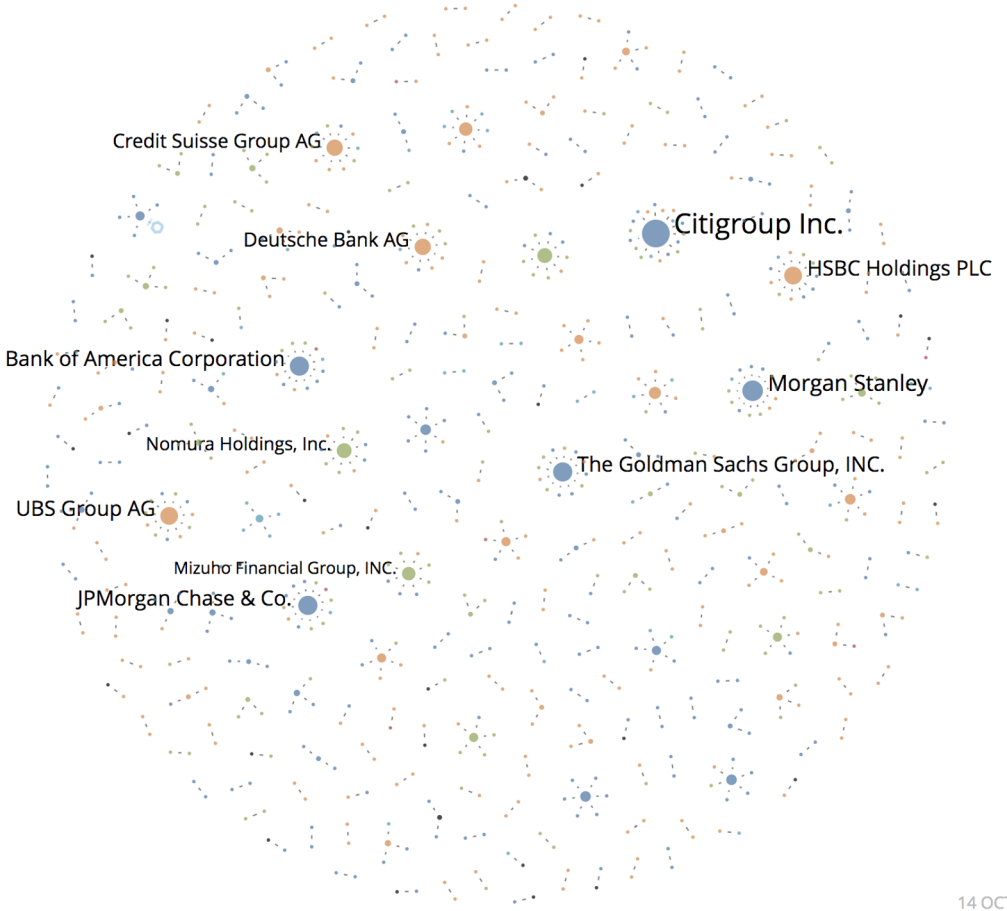


Banking Groups

210 Banking Groups

Largest (# of entities):

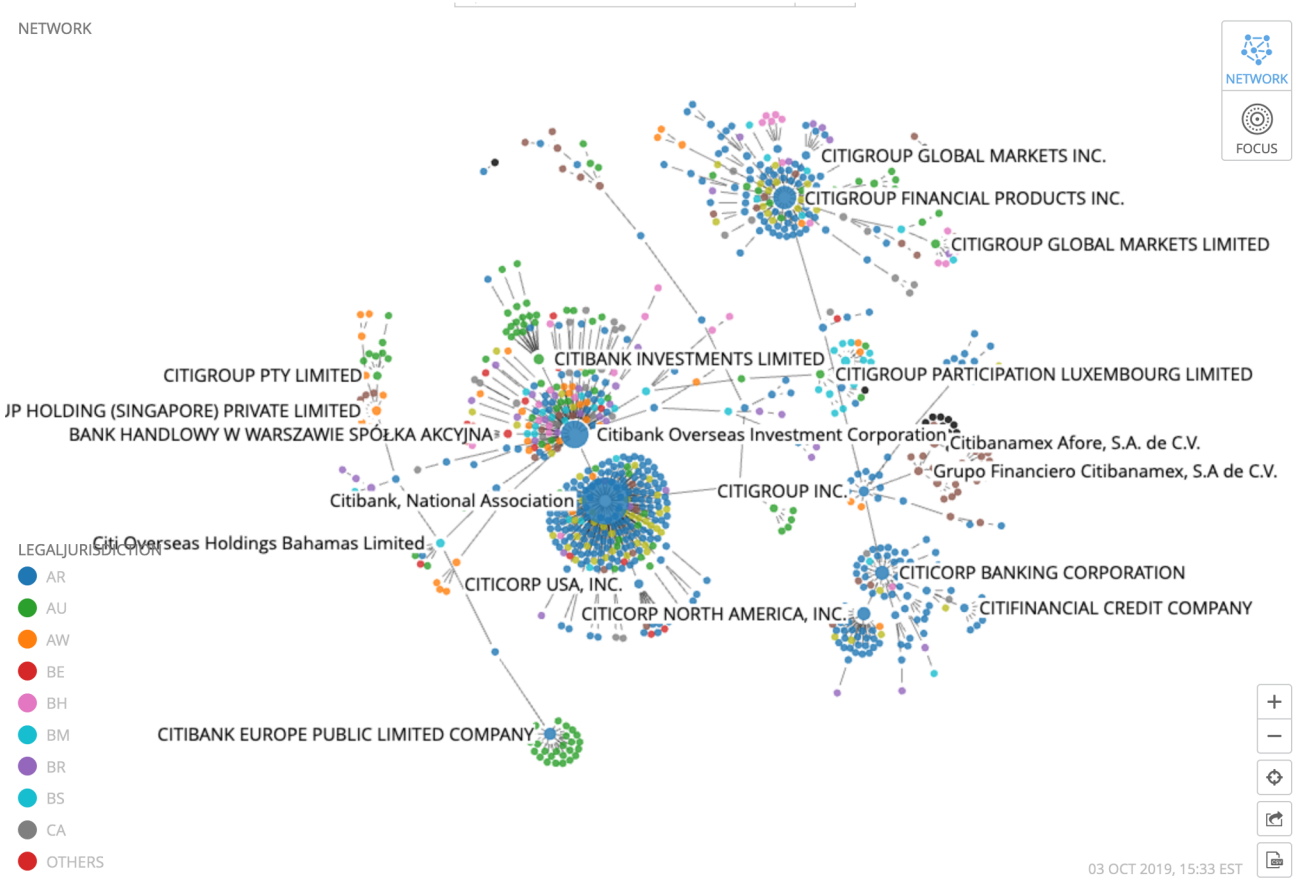
1. Citigroup (18)
2. Morgan Stanley (13)
3. Goldman Sachs (12)
4. JPMorgan Chase (12)
5. Bank of America (12)
6. HSBC (11)
7. UBS (11)
8. Deutsche Bank (10)
9. Credit Suisse (10)
10. Nomura Holdings (9)



LEI level 2 data

Automatic generation of complex bank structures / beneficial ownership structures.

Exploration through "Knowledge graphs"

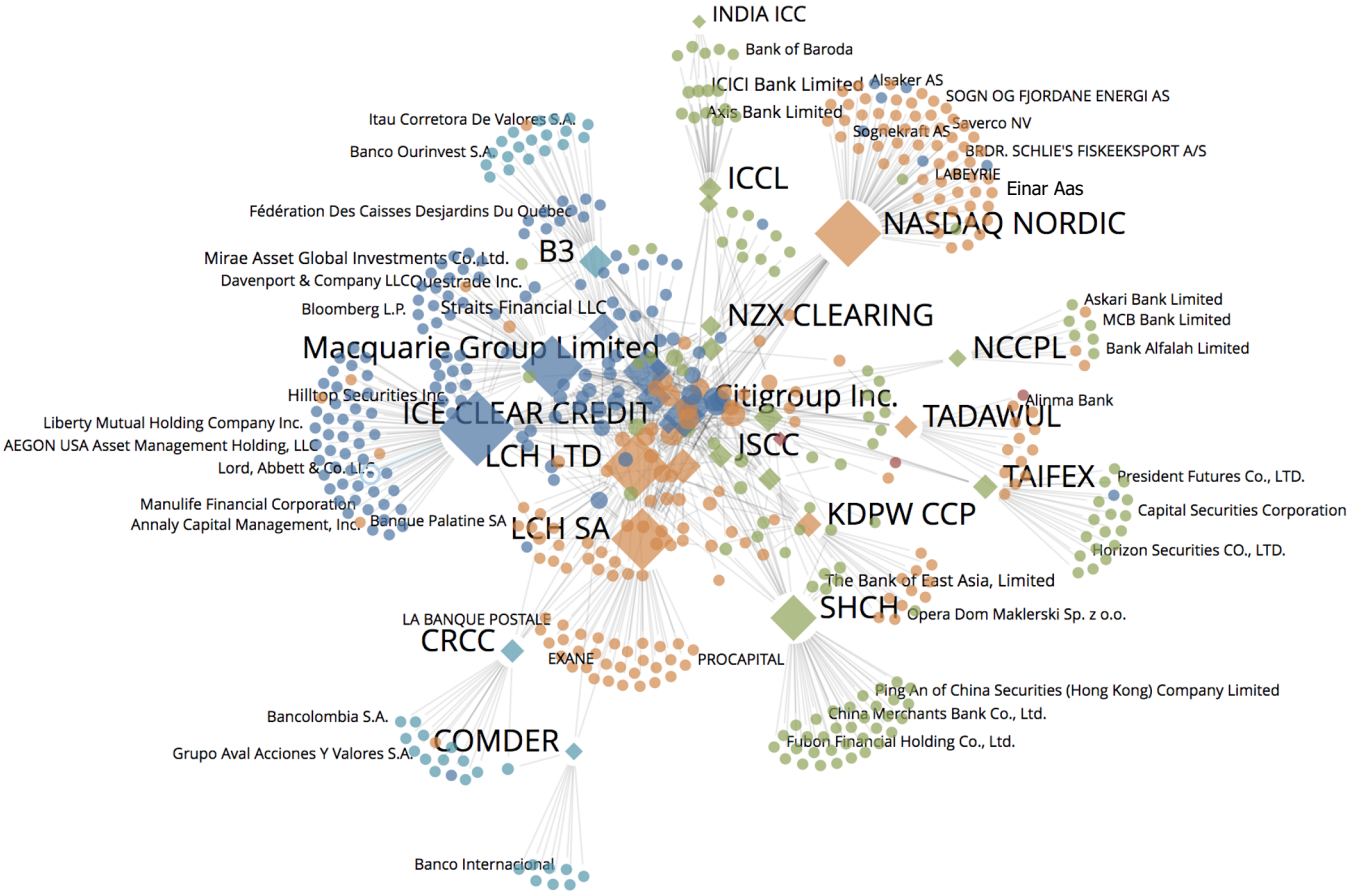


CCP Interconnectedness on Parent Level

We see CCPs (diamonds) and their members (circles) from different regions:

- North America (blue)
- Europe and Middle East (orange)
- Asia and Pacific (green)
- Latin America (light blue)
- Africa (red)

On parent level we see a completely connected network dominated by a core consisting of CCPs from North America and Europe and global banks.

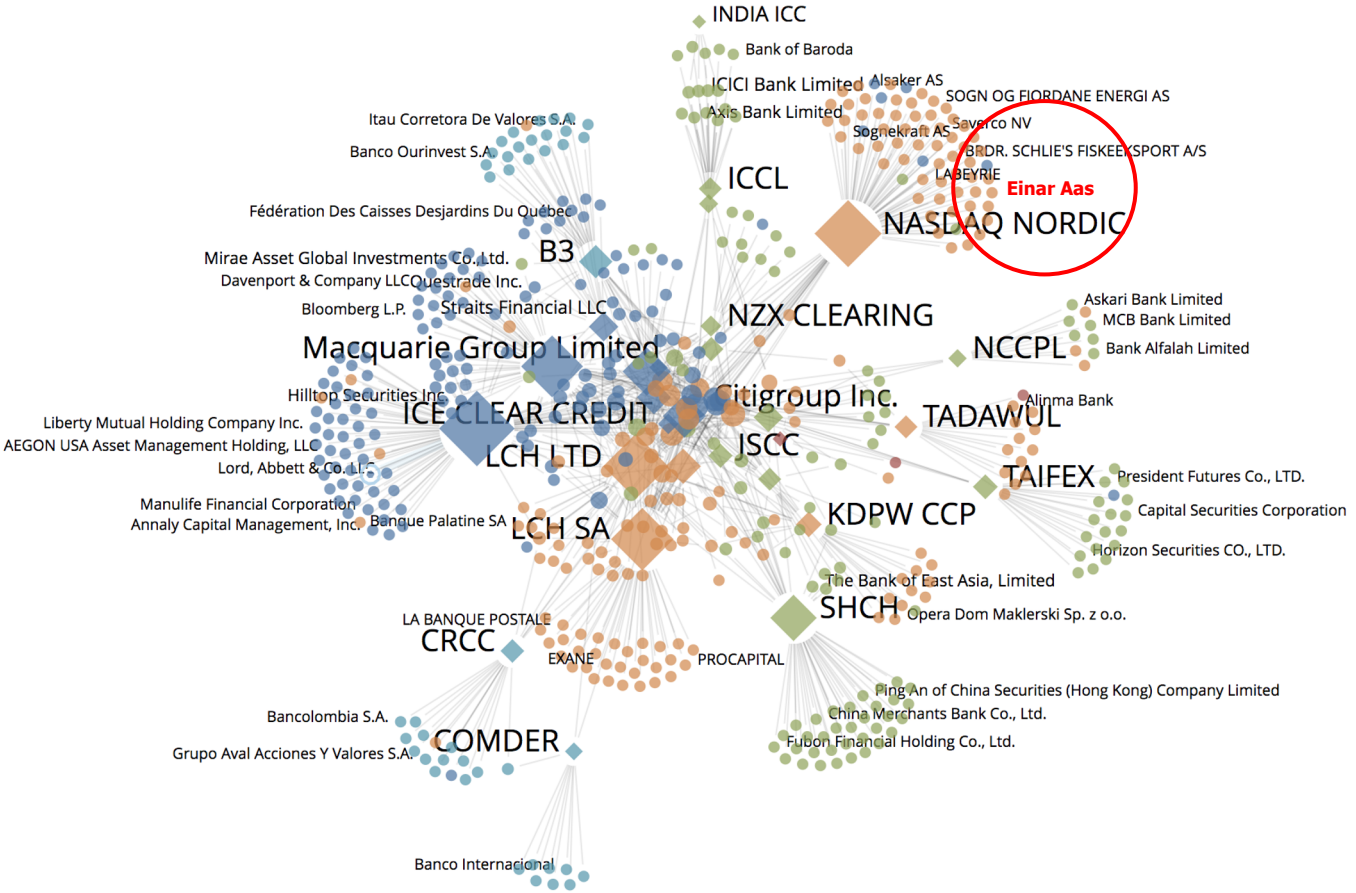


CCP Interconnectedness on Parent Level

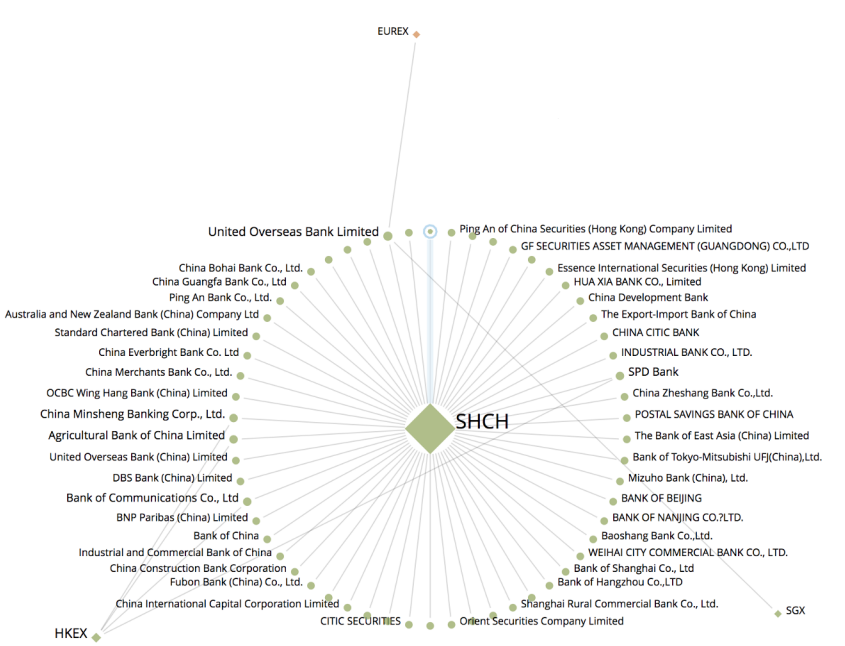
We see CCPs (diamonds) and their members (circles) from different regions:

- North America (blue)
- Europe and Middle East (orange)
- Asia and Pacific (green)
- Latin America (light blue)
- Africa (red)

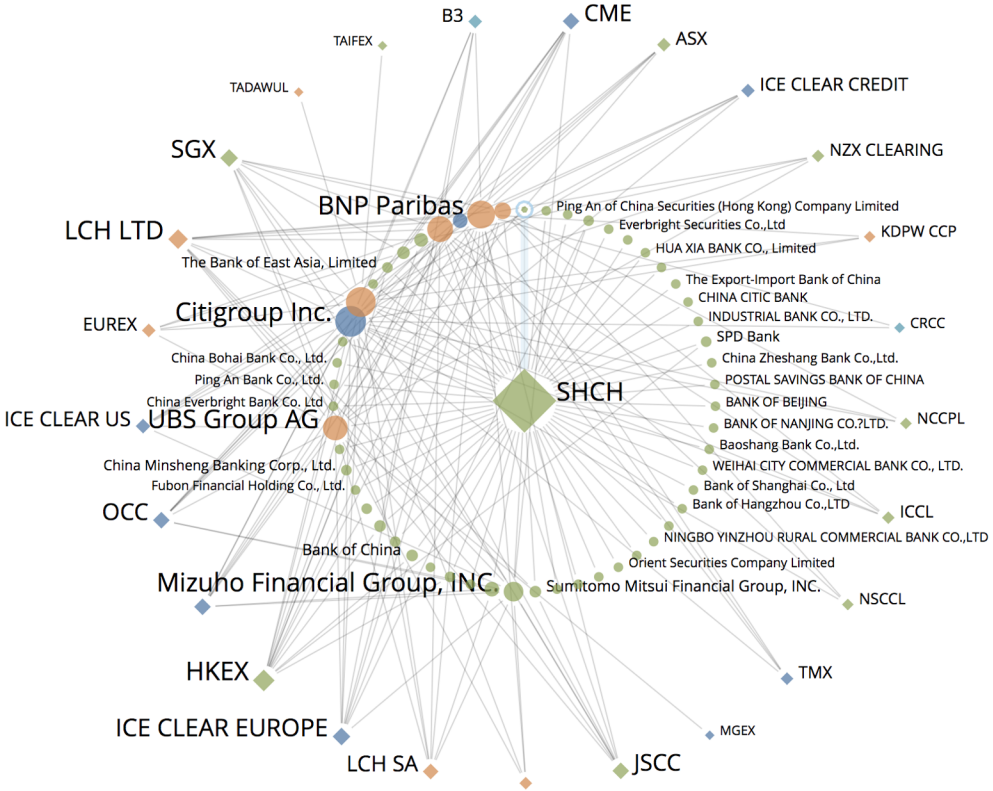
On parent level we see a completely connected network dominated by a core consisting of CCPs from North America and Europe and global banks.



CCP Interconnectedness on Subsidiary vs Parent Level - Example



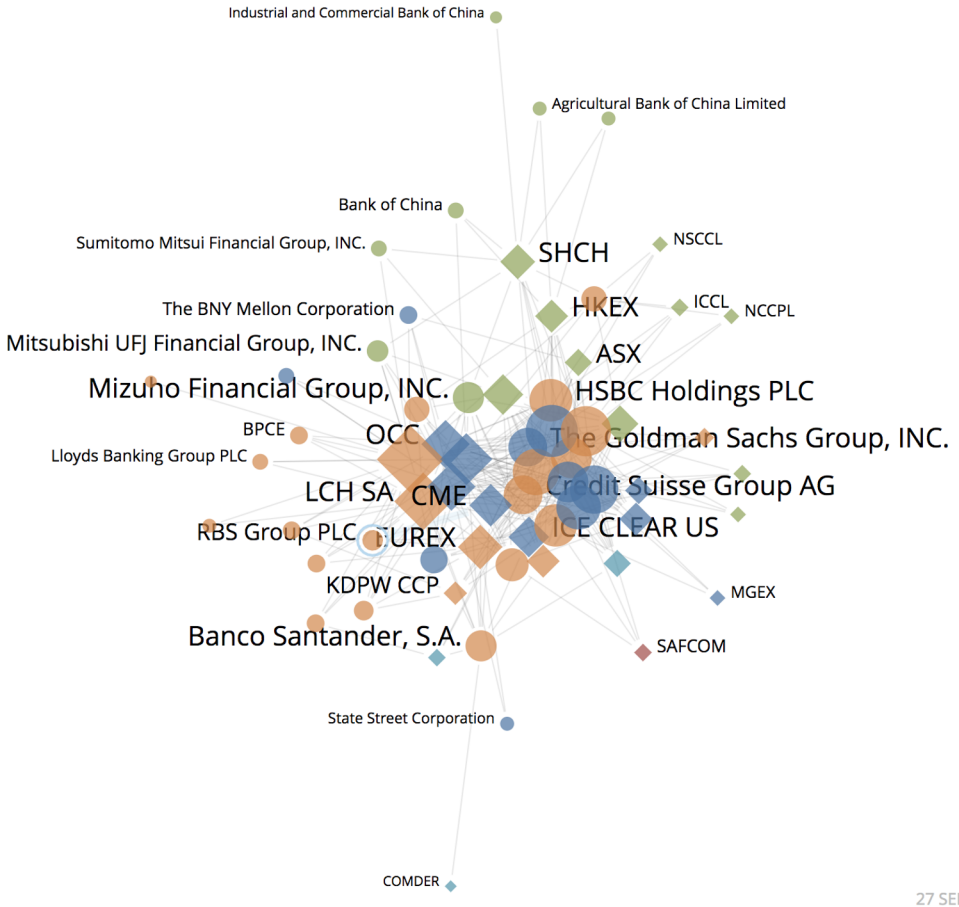
Subsidiary Level
(Connected to 3 CCPs)



Parent Level
(Connected to 25 CCPs)

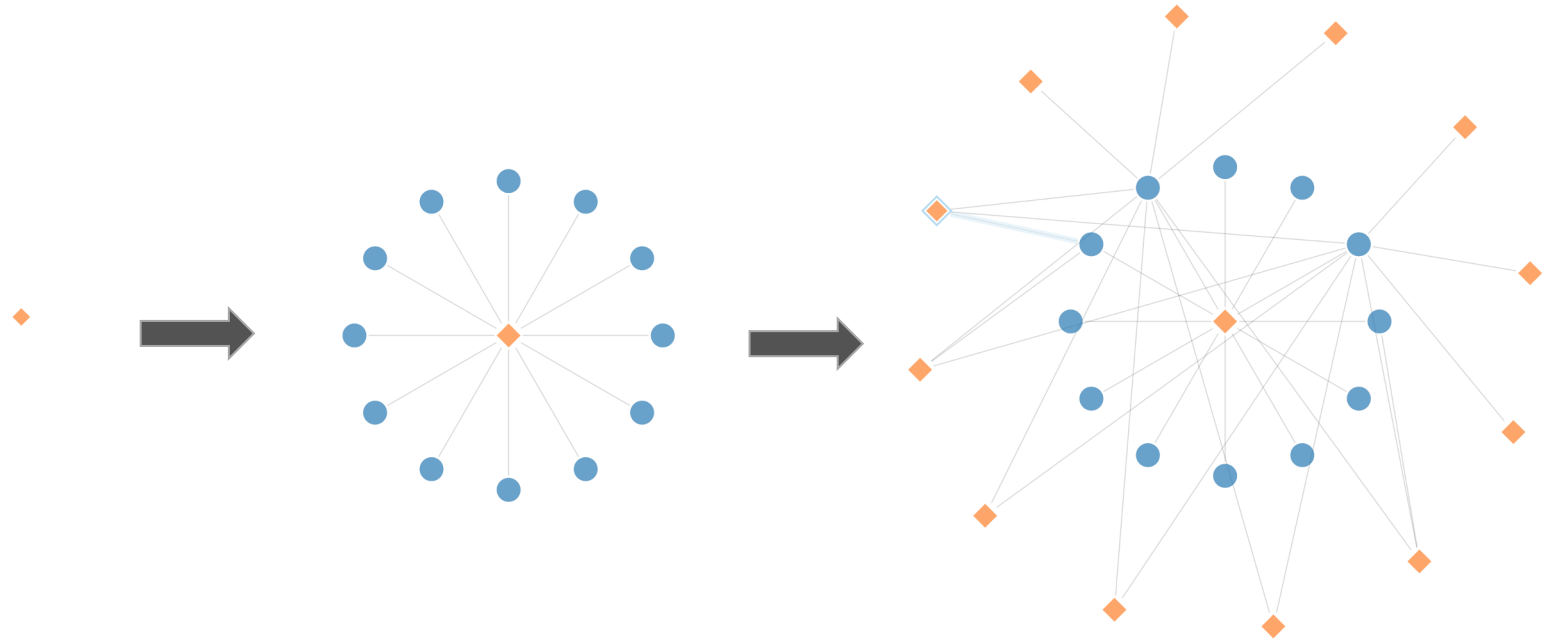
CCP Interconnectedness on GSIB Level

Bank (Parent)	# of CCPs
Citigroup	22
Deutsche Bank	21
JPMorgan Chase & Co.	20
BNP Paribas	19
Bank of America	18
HSBC	17
Societe Generale	17
UBS	16
Morgan Stanley	16
Credit Suisse	15



Contagion - CCP Disruption

A disruption in a CCP would affect all of that CCP's clearing members, thereby affecting the other CCP's to which the affected CCP's members belong, possibly creating a cascading cycle as disruption is propagated across members and CCPs



CCP disruption

Propagates to all members

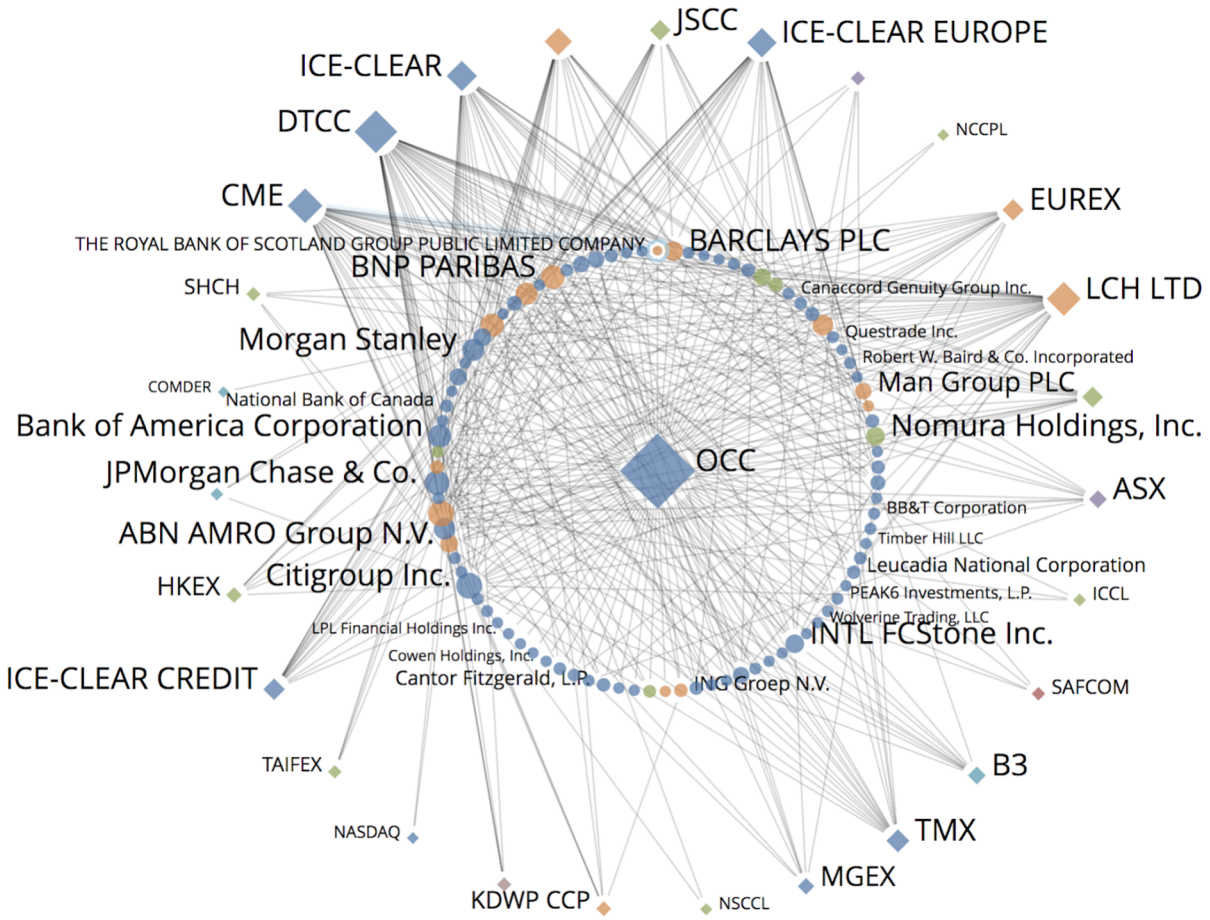
Propagates to other CCPs

Footprint of CCPs - OCC

OCC's 79 members are connected to 27 other CCPs

The membership is mostly US with a significant EU base.

The most connected CCP's are DTCC and CME.

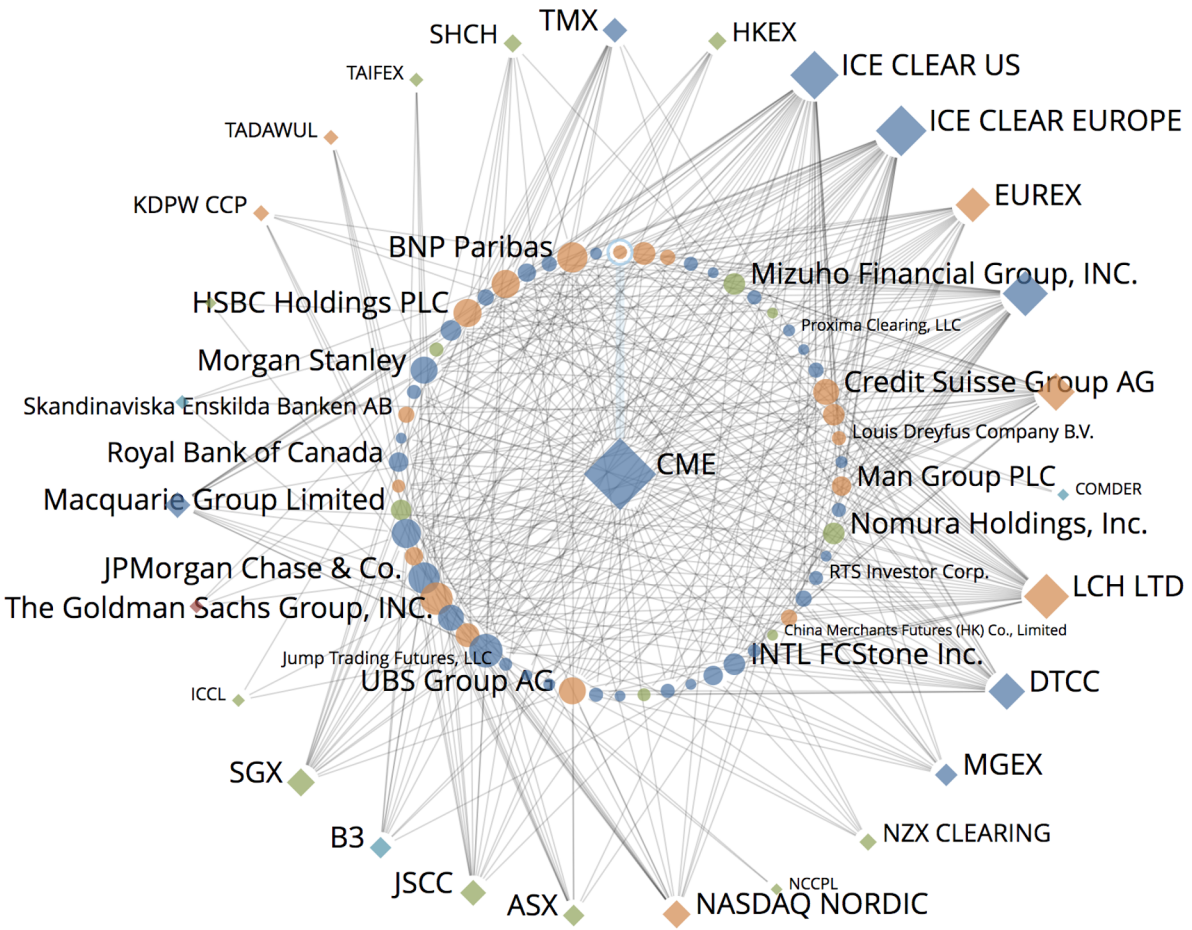


Footprint of CCPs - CME

CME's 58 members are connected to 27 other CCPs

The membership is mostly US with few entries from Europe and Asia

The most connected CCP are ICE US, ICE Europe, LCH Ltd. and OCC

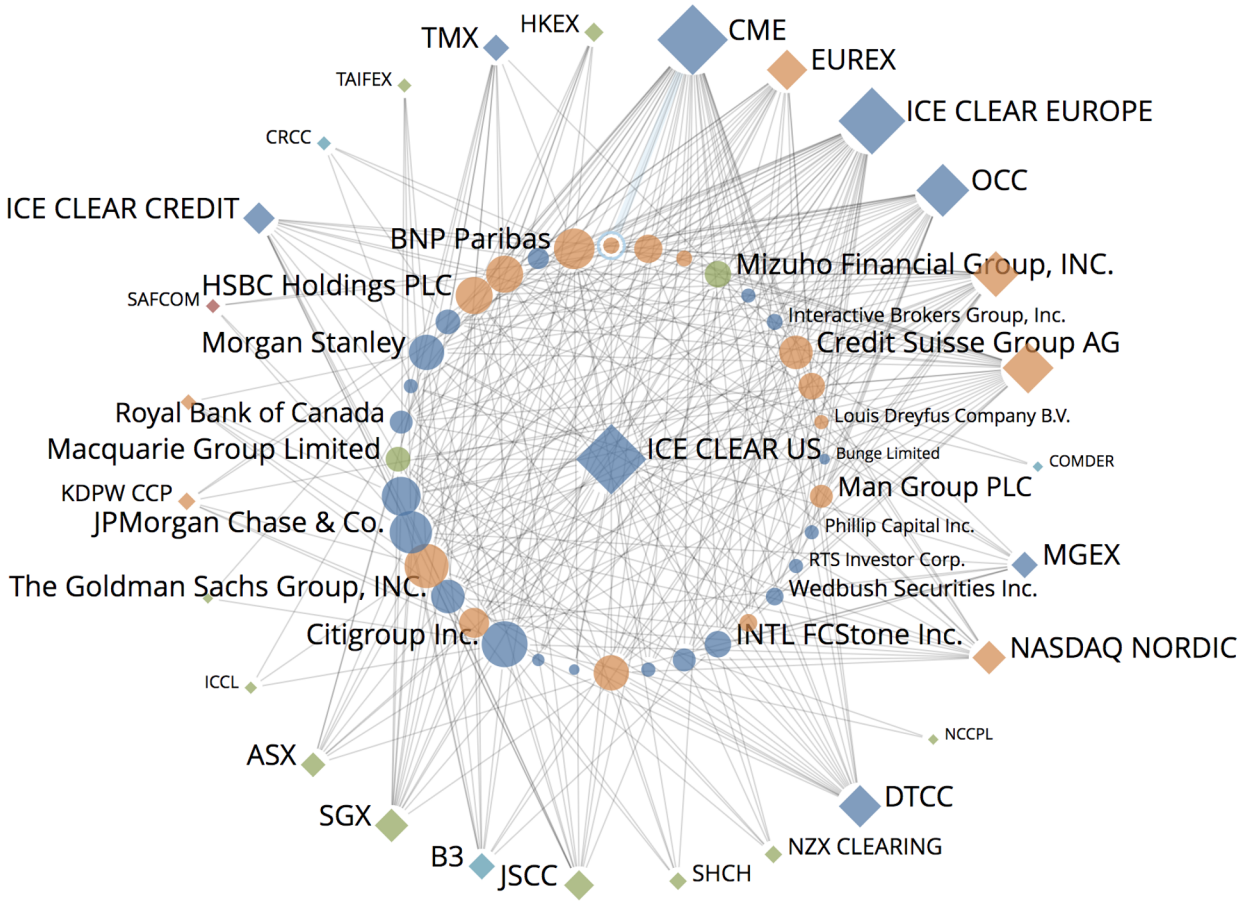


Footprint of CCPs - ICE

ICE's 36 members are connected to 27 other CCPs

The membership is mostly US with a significant European base.

The most connected CCPs are CME, ICE EUROPE and OCC



Contagion – Member Disruption

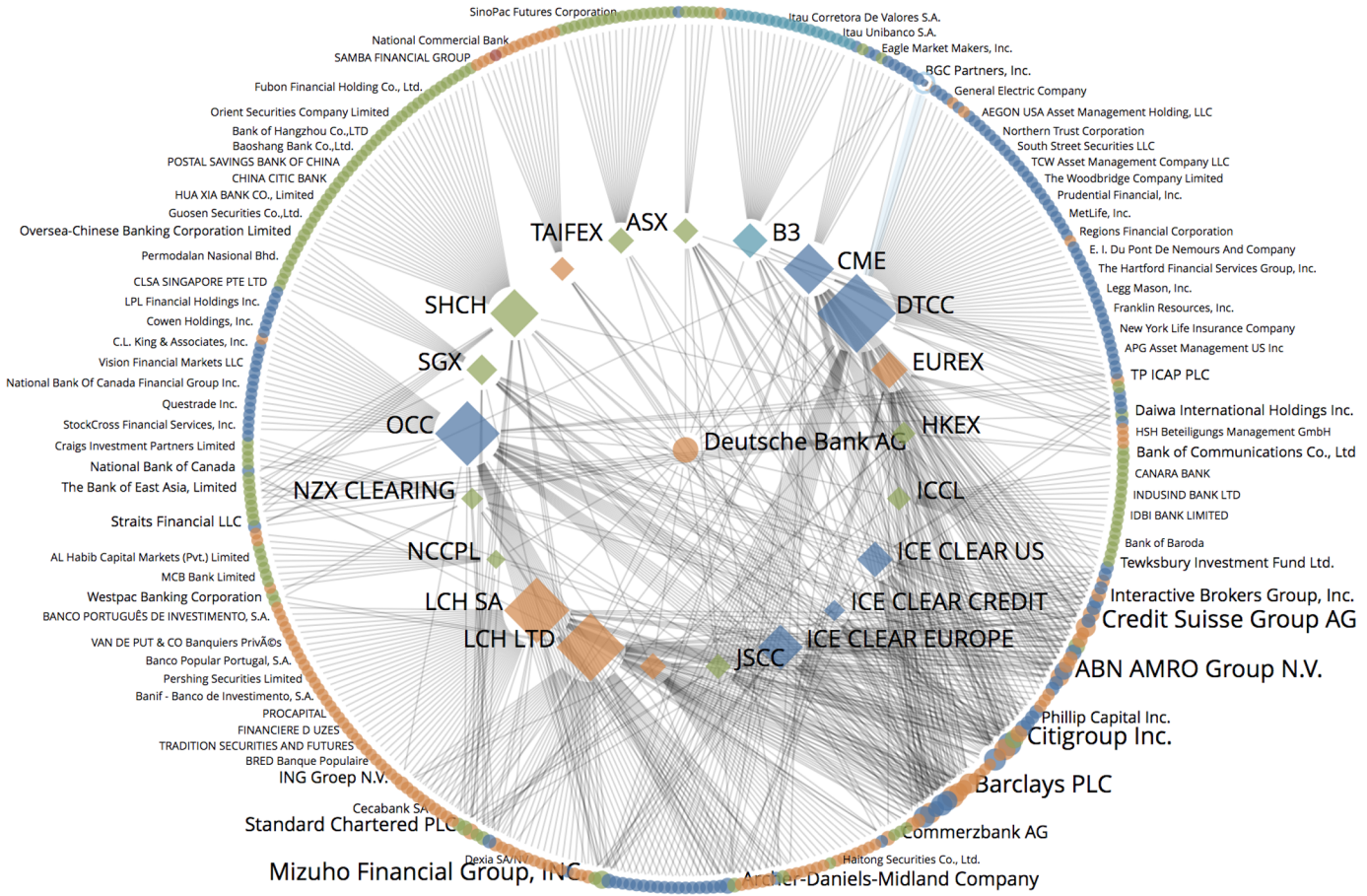
A member disruption could be felt by up to **448** banking groups or banks (of total of 495, or 90%) that are members of the same CCP as the stricken group.

Banking Group	# banking groups connected via a CCP
Citigroup	448
BNP Paribas	426
JPMorgan Chase	396
Deutsche Bank	392
Bank of America	391
Morgan Stanley	378
Credit Suisse	357
Société Générale	351
Goldman Sachs	349
HSBC Holdings	339

Contagion – Member Disruption

Deutsche Bank Group participates in 21 CCPs (of 29 mapped).

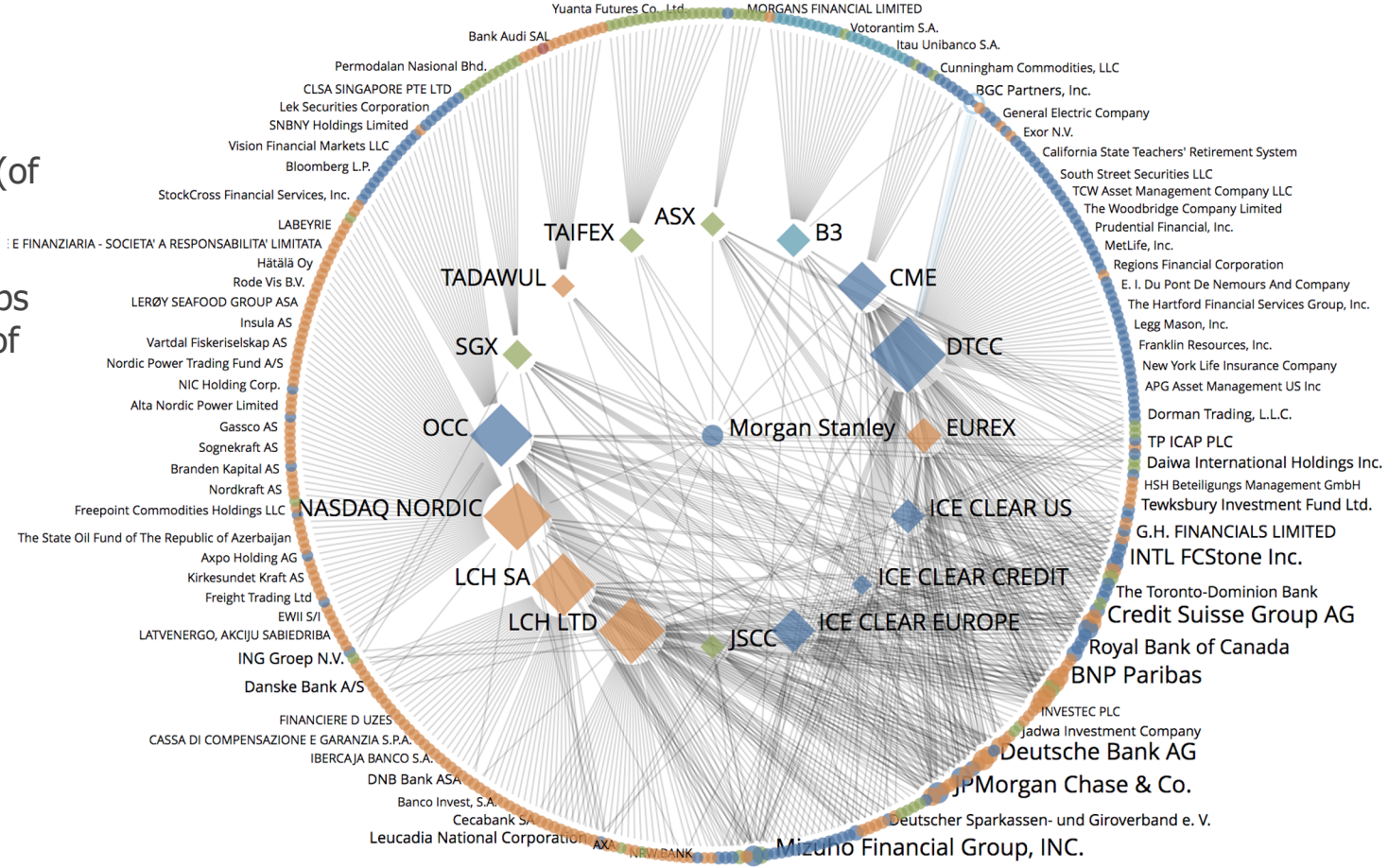
392 other banking groups or banks are members of these CCPs.



Contagion – Member Disruption

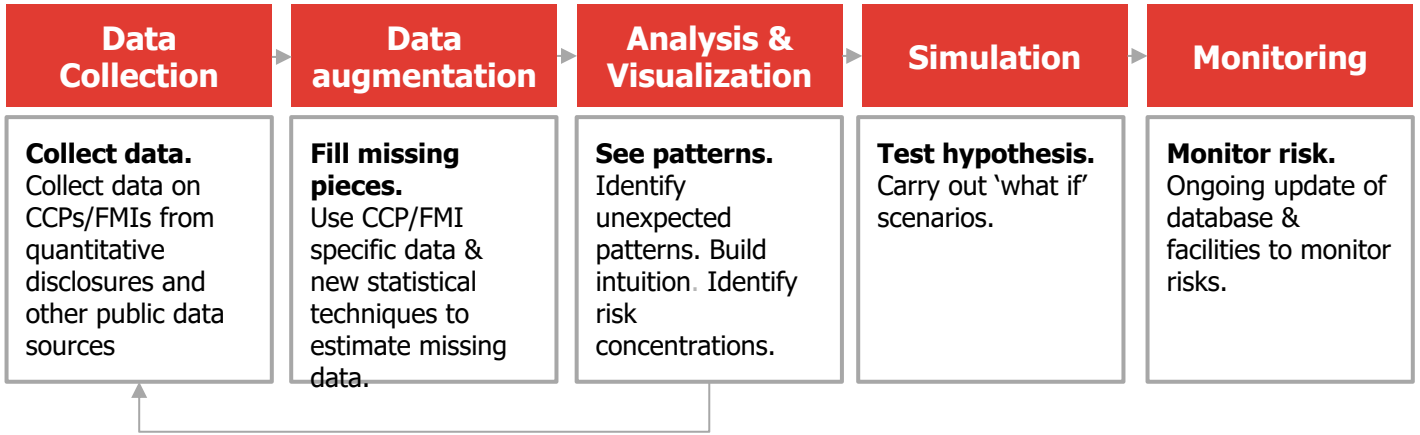
Morgan Stanley participates in 16 CCPs (of 29 mapped).

378 other banking groups or banks are members of these CCPs.



Objective & Roadmap

Objective: Develop a global database and the methods to measure risk concentrations and simulate failures and stress scenarios of interconnected FMIs and markets. This will allow regulators, FMIs and members develop risk mitigation strategies to address this new and global systemic risk.



FNA

Simulating Failures

Short History of Payment System Simulations

1997 : Bank of Finland

Evaluate liquidity needs of banks when Finland's RTGS system was joining TARGET

First general purpose payment systems simulator

2000 : Bank of Japan and FRBNY

Test liquidity saving mechanisms (LSM) for BoJ-Net & Fedwire

2001 - : CLS approval process and ongoing oversight

Test CLS risk management

Evaluate settlement' members capacity for pay-ins

Understand how the system works

Since then: Bank of Canada, Banque de France, Nederlandsche Bank, Norges Bank, TARGET2, and many others

2018 : Exact replicas of LVTS, CHAPS and 4 other FMIs in FNA

Three main use cases:

- Liquidity optimization
- Liquidity stress testing
- What-if Analysis

Concept: Operational Failure of a Settlement Member

Mapping
This network shows settlement relationships between the:

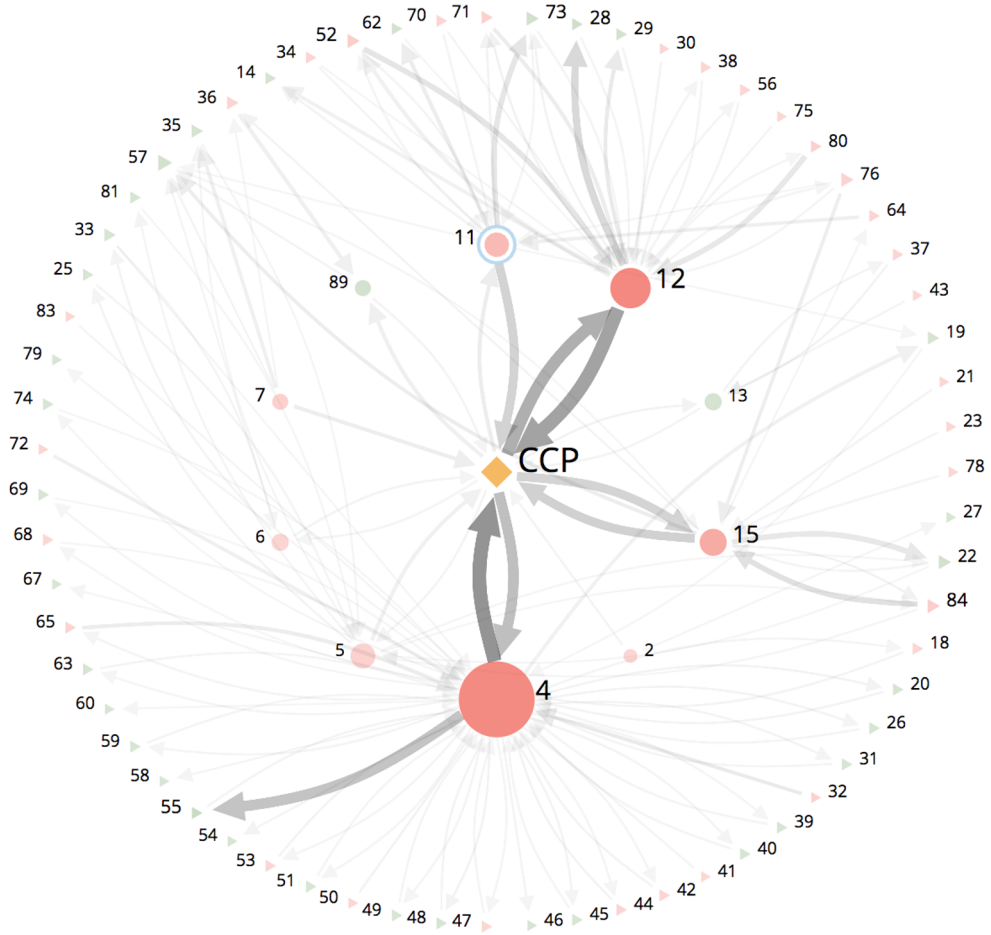
- CCP (center)
- Settlement members (inner circle) and
- Clearing members (outer circle)

Note: Data is representative, not real

Size of node shows value of multilateral position

Width of lines shows value of bilateral positions

Question
What would happen if member 4 had an operational failure?



Backup Relationships

Map

Shows Clearing Members on the left, and Settlement Members on the right.

The lines denote which settlement member the clearing member can use for settlement (ie its main and its backups)

Concept: Operational Failure of a Settlement Member

Mapping
This network shows settlement relationships between the:

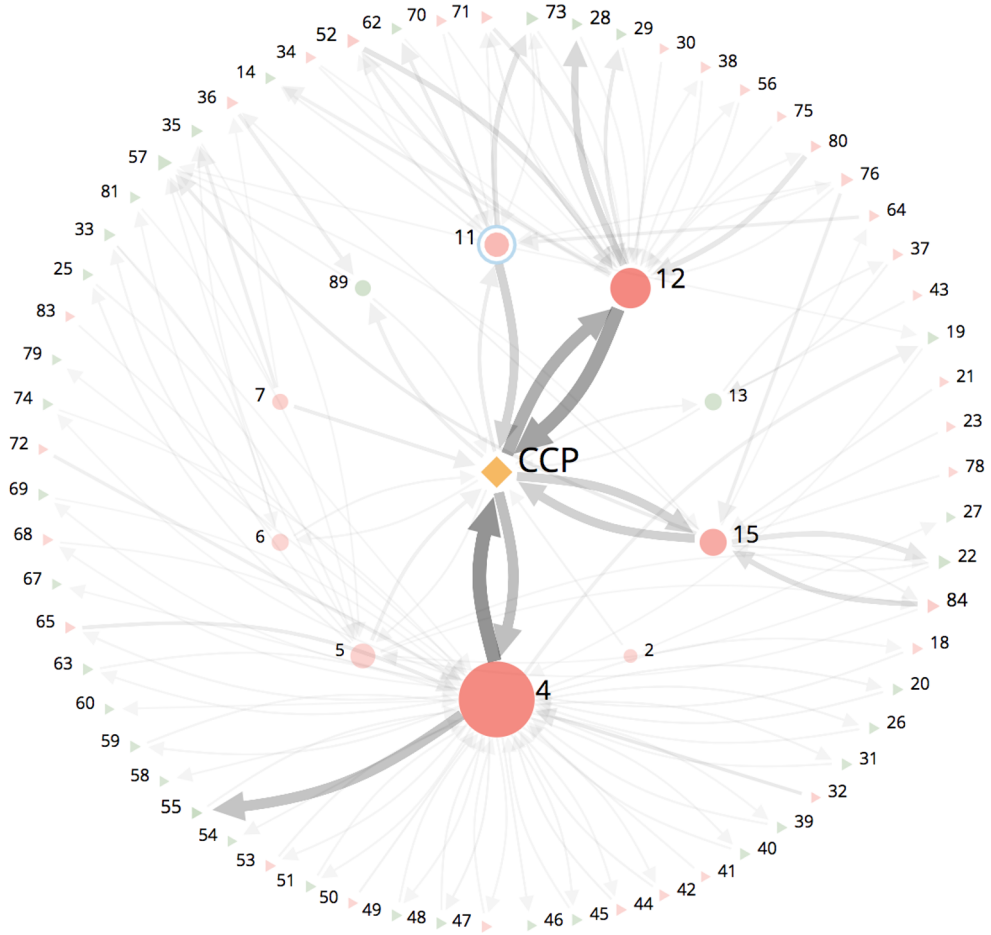
- CCP (center)
- Settlement members (inner circle) and
- Clearing members (outer circle)

Note: Data is representative, not real

Size of node shows value of multilateral position

Width of lines shows value of bilateral positions

Question
What would happen if member 4 had an operational failure?

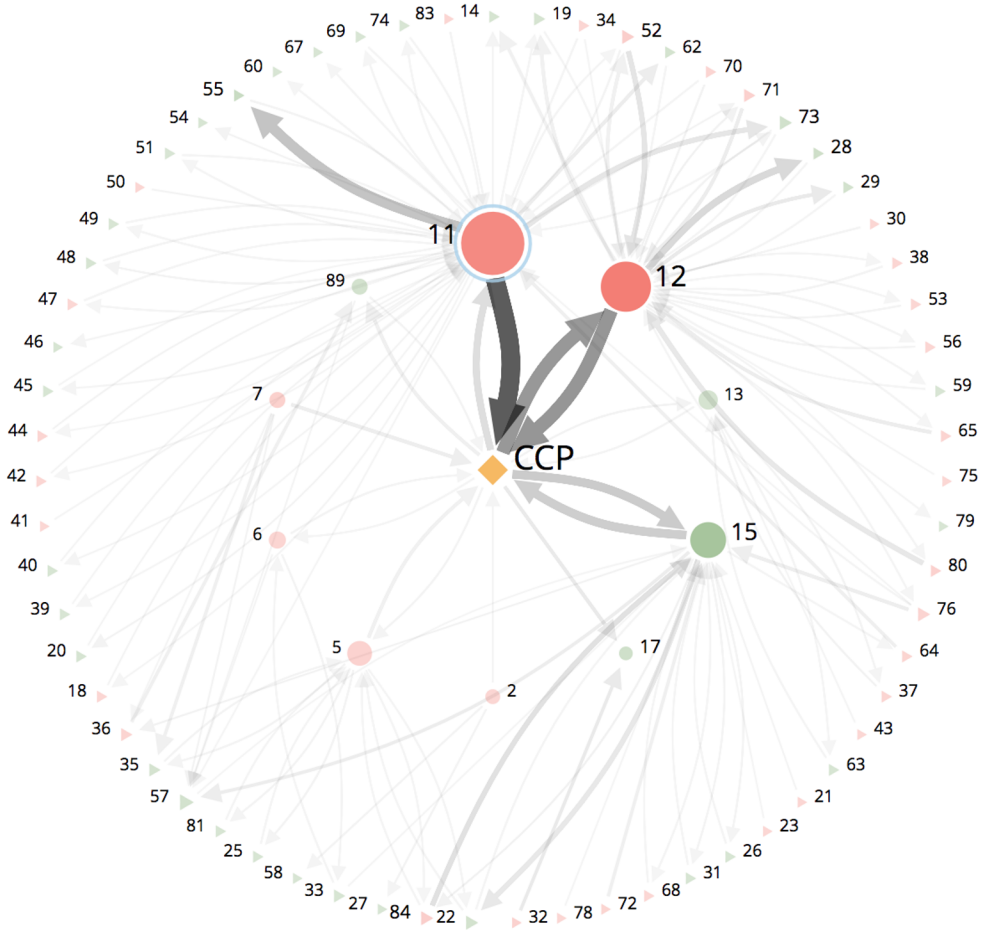


Rewiring for Maximum Concentration

Each clearing member using Bank 4 must now effect settlement through one of its backup relationships.

Findings
Simulation shows that settlement flows could be concentrated on a few participants, e.g.
causing operational challenges for Bank 11.

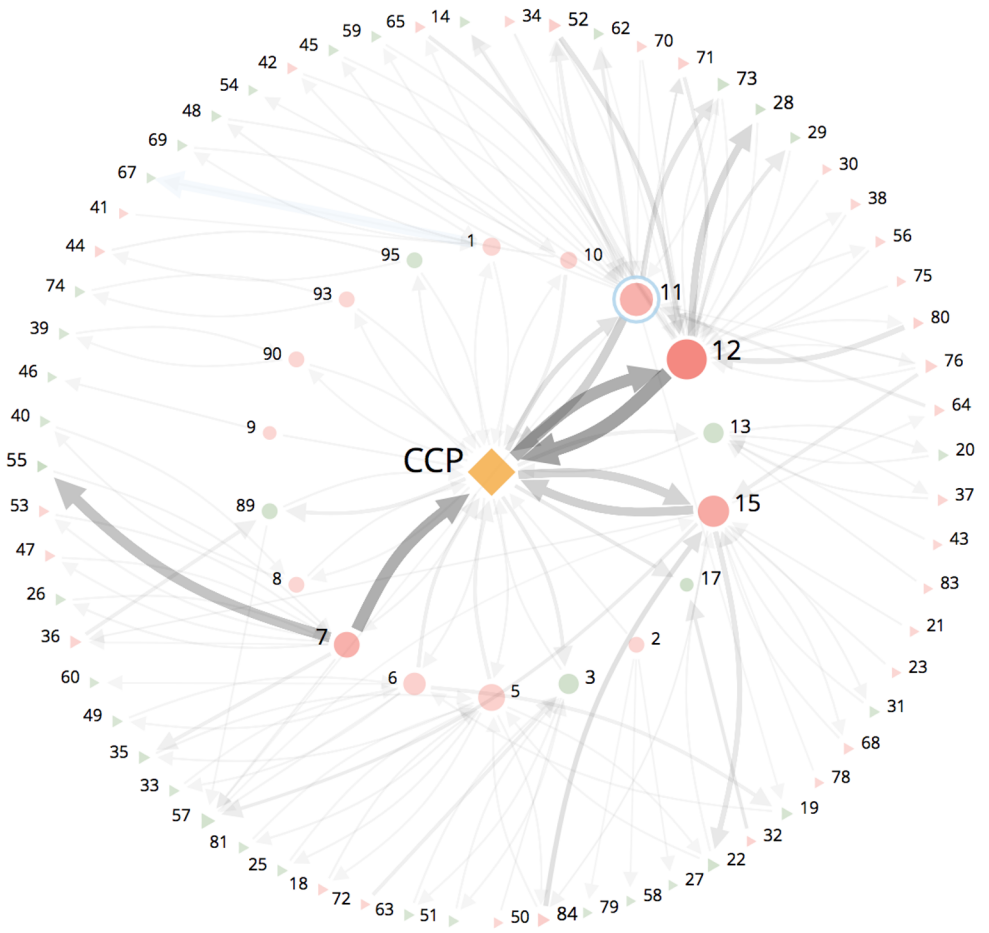
Insight
Bank 11 was not among the most active settlement members on a normal day, but might need to build operational capacity to cover for rare failure days.



Rewiring for Minimum Concentration

Findings
... or clearing members might use different settlement members resulting in a much higher number (18 instead of 10) of settlement members for the day.

Insight
The CCP may need to build operational capacity to be able to complete settlement.



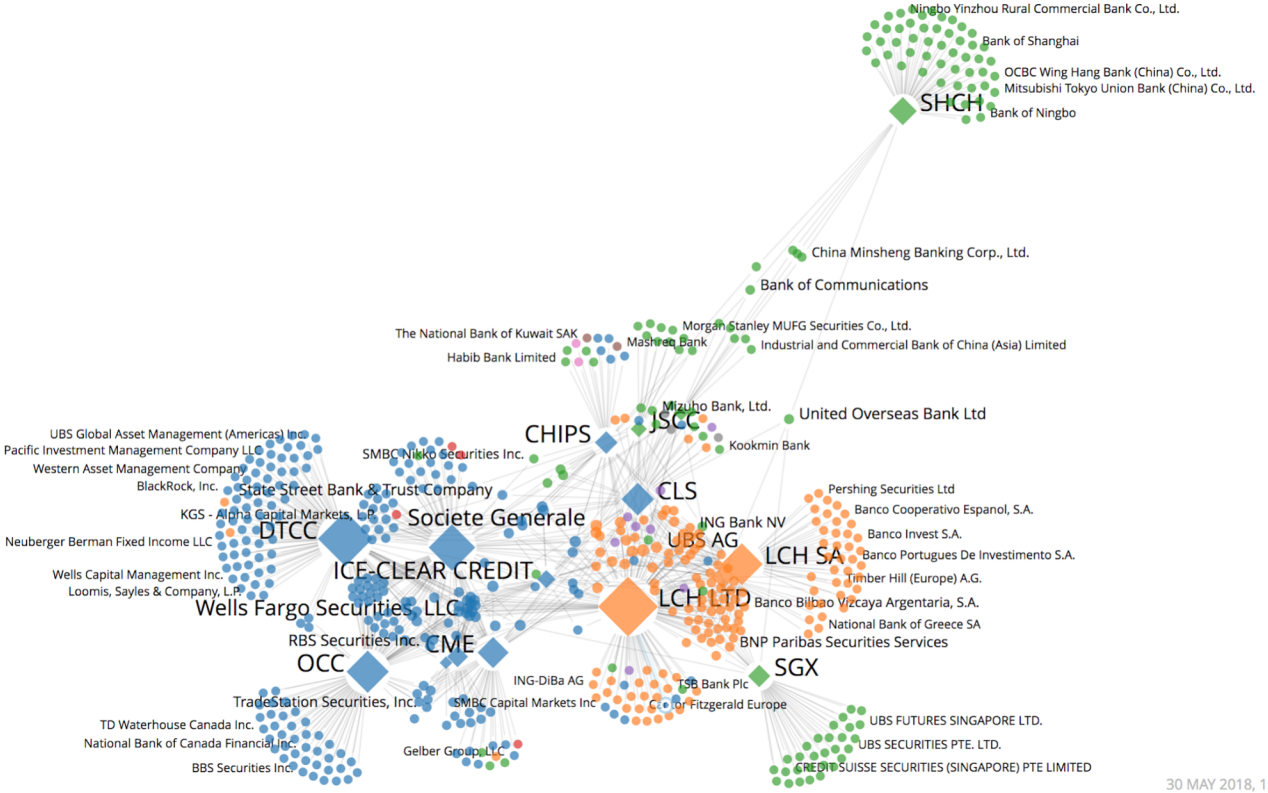
The Vision - Simulate System of FMIs

Stress testing in practice means simulation.

For realistic scenarios, we need to understand how everything is interconnected within and across FMIs.

This means CCPs, Payment Systems, CLS, ICSDs, etc.

FMI Simulators are valuable alone, and more valuable when connected.

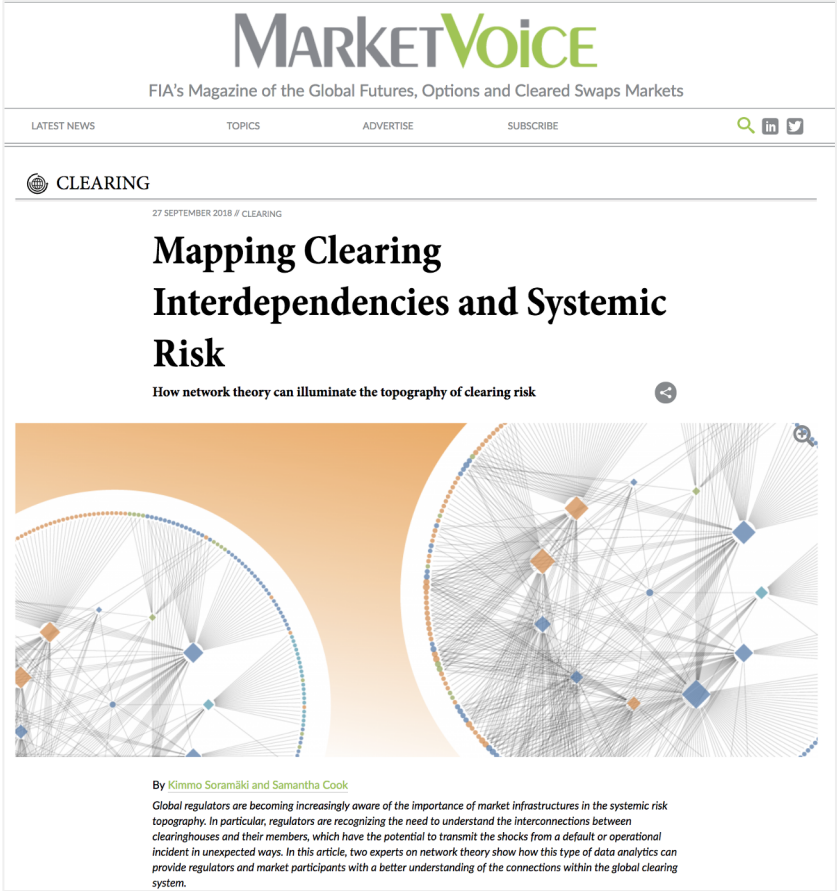


Visualizations

The visualizations were created for FIA MarketVoice article :

"Mapping Clearing Interdependencies and Systemic Risk: How network theory can illuminate the topography of clearing risk"

Links to interactive versions are available on FNA Website and in the following slides.



MARKETVOICE

FIA's Magazine of the Global Futures, Options and Cleared Swaps Markets

LATEST NEWS TOPICS ADVERTISE SUBSCRIBE

CLEARING

27 SEPTEMBER 2018 // CLEARING

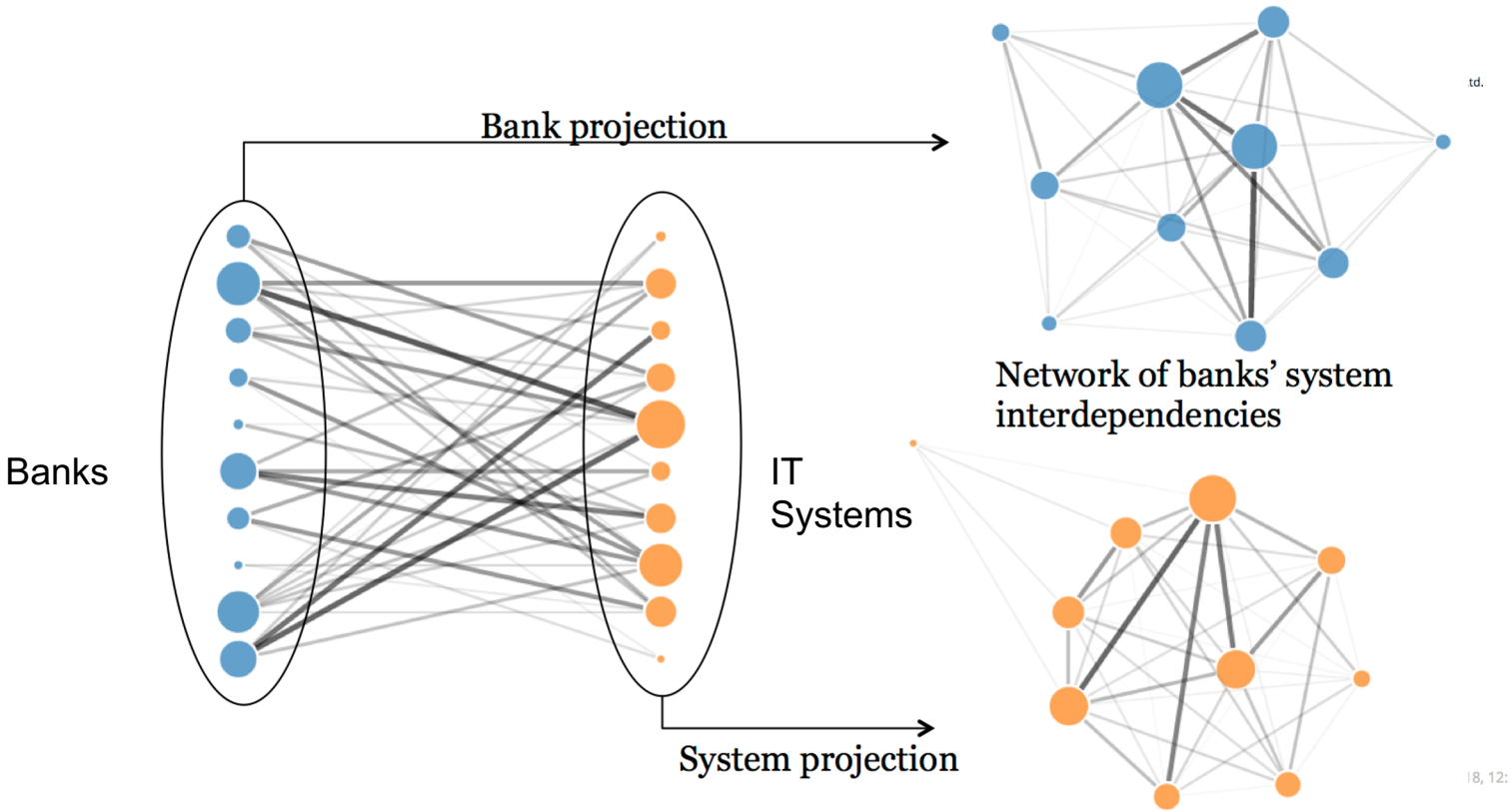
Mapping Clearing Interdependencies and Systemic Risk

How network theory can illuminate the topography of clearing risk

By Kimmo Soramäki and Samantha Cook

Global regulators are becoming increasingly aware of the importance of market infrastructures in the systemic risk topography. In particular, regulators are recognizing the need to understand the interconnections between clearinghouses and their members, which have the potential to transmit the shocks from a default or operational incident in unexpected ways. In this article, two experts on network theory show how this type of data analytics can provide regulators and market participants with a better understanding of the connections within the global clearing system.

Measuring Technological Interdependence



Cyber Risks and Financial Stability

How might cyber risks and financial risks interact to cause systemic crises?

Is there anything fundamentally new or different about cyber risks?

How should economists, regulators, policymakers, and central bankers focused on financial stability incorporate cyber risks into their models and thinking?

- "The Future of Financial Stability and Cyber Risk" by Jason Healey, Patricia Mosser, Katheryn Rosen, and Adriana Tache, Brookings Institute 2018

Scenario Types

Source of stress

- Bankruptcy
- Liquidity event
- Cyber attack
- Technical failure
- Change in environment
- Incremental system change (model validation)

How it manifests

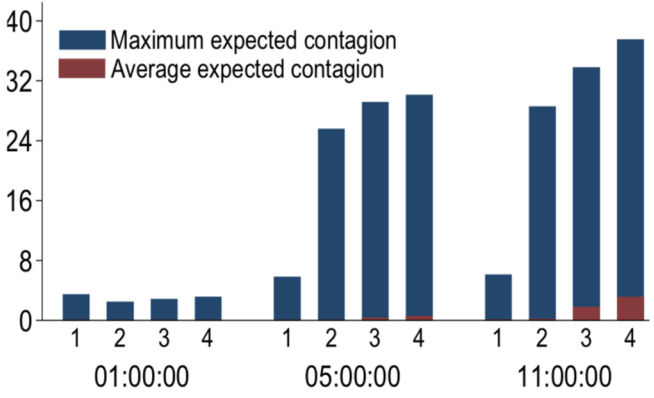
- Outage
- Triggers failure processes
- Change in parameters

How is it modeled

- Historical
- Probabilistic
- Extreme but plausible
- Worst-case

Use Case: Simulating Complex Financial Systems

Chart 10 Expected contagion for other banks' settled payments. In minutes



Norges Bank analyses the robustness of NBO, the Norwegian RTGS system

Background

Interbank payments are settled in Norges Bank's settlement system (NBO), a real time gross settlement (RTGS) system. Such payments are often time-critical and of high value. Operational disruptions that impair the ability of participants to execute payments may therefore pose a threat to financial stability.

Objective

Analyse the robustness of the settlement process in the Norges Bank settlement system (NBO) to operational problems in one of its participating banks using a large number of days with actual payments data.

Outcome

Only four banks are of systemic importance and that the systemic effects can be significantly reduced if banks react quickly by postponing their outgoing payments to the stricken bank.

Norges Bank Working Paper: "Operational problems in banks – Effects on the settlement of payments in Norges Bank"

Use Case: Complying with PFMIs

"The FNA software platform has helped the bank improve its ongoing risk management processes [...] reducing the time it takes to run analysis from weeks to only a few minutes."

Mr. Fabio Ortega
Project Manager
Central Bank of Colombia

Central Bank of Colombia simulates failures of two largest participants on a daily basis

Background

The globally agreed Principles for Financial Market Infrastructures stipulate that FMIs must be able to withstand the failure of their two largest members, and complete settlement by the end of the day of the disruption, even in case of extreme circumstances.

Objective

Ability to measure and monitor the impact of the failure of two largest participants.

Outcomes

Automated daily stress tests where simulations of failing the two largest participants in the network are carried out.

BIS: Principles for financial market infrastructures

Current State Observations - Cyber Resilience

Financial Institutions

- Historic focus predominantly on cyber-security rather than resilience
- Cyber-resilience responsibility increasingly much broader than technology/CISO functions
- Group Risk functions increasingly involved
- Need for data/information from outside the individual FI >> industry collaboration

Central Banks / Supervisors

- Increasingly playing lead or key role in:
  - Industry collaboration
  - Cross-jurisdiction regulatory collaboration
- Initiating industry mapping exercises
- Driving FMIs, G-SIFIs and D-SIFIs to take on greater systemic cyber-resilience responsibilities

FNA

Dr. Kimmo Soramäki
Founder, CEO
FNA Financial Network Analysis Ltd.

kimmo@fna.fi
tel. +44 20 3286 1111

Address
4-8 Crown Place
London EC2A 4BT
United Kingdom