Abstract

We explore the network topology of the interbank payments transferred between commercial banks over the Fedwire® Funds Service. We find that the network is compact despite low connectivity. The network includes a tightly connected core of money-center banks to which all other banks connect. The degree distribution is scale-free over a substantial range. We find that the properties of the network changed considerably in the immediate aftermath of the attacks of September 11, 2001.

Key words: network, topology, interbank, payment, Fedwire, September 11, 2001
I. INTRODUCTION

At the apex of the U.S. financial system is a network of interconnected financial markets by which domestic and international financial institutions allocate capital and manage their risk exposures. The events of September 11, 2001 and, to a lesser extent, the North American blackout of August 14, 2003 underscored that these markets are vulnerable to wide-scale disruptions. The inability of one of these markets to operate normally can have wide-ranging effects not only for the financial system but potentially for the economy as a whole. Currently, the financial industry and regulators are devoting considerable resources to strengthen the resiliency of the U.S. financial system [35, 37]. Critical to the smooth functioning of these markets are a number of wholesale payments systems and financial infrastructures that facilitate clearing and settlement.

Despite their importance, little empirical research on the impact of disruptions these systems and infrastructures is available. One branch of the literature has focused on simulating the effects from a default of a major participant [4, 10, 16, 25]. Another branch has done detailed case studies of disruptions to the U.S. financial system, e.g. the 1987 stock market crash and the events following September 11th [11, 20, 28, 30].

However, the payment system can be treated as a specific example of a complex network. In recent years, the physics community has made significant progress towards understanding the structure and functioning of complex networks [5, 7, 18, 32, 39]. The literature has focused on characterizing the structure of networked systems and how the properties of the observed topologies relates to stability, resiliency and efficiency in case of perturbations and disturbances [5, 15].

A few recent papers [12, 22, 26] have started to describe the actual topologies observed in the financial system using this methodology. This paper adds to this literature by describing the network topology of the interbank payment flows in the U.S. Moreover, we add new insight to the response of complex networks to perturbations by analyzing the effects of September 11th on the network.

The paper is organized as follows. Section II introduces network theory and the main concepts applied. Section III describes the data. Section IV presents a visualization of the data. Section V defines and discusses the topological characteristics of the interbank payment flows. Section VI looks at the impact of September 11th on these characteristics. Section VII concludes.

II. NETWORKS

A network consists of two types of elements, nodes and the connections between them, links. Links can have weights attached to them representing the importance of the relationship between nodes. Links can be either undirected or directed. A link from a node to itself is called a loop. The neighbors of a node are all the nodes to which it has a link. The predecessors of a node are the nodes that have a link to the node and the successors are the nodes that have a link from the node. A walk is a sequence of nodes in which each node is linked to the next. A walk is a path if all its nodes are distinct. The length of a path is measured by the number links. If the start node and the end node of a path are one and the same, then it forms a cycle.

A complete network is a network where all nodes have a link to each other. A tree is a network in which any two nodes are connected by exactly one path. In a star network all nodes connects to a central node called the hub. A component of a network is a subset of nodes in a network such that any two nodes can be joined by a path. A connected network consists of a single component, while a disconnected network is made up of two or more components. These concepts are illustrated in Fig. 1a.

There are two classes of network formation models some times referred to as equilibrium and non-equilibrium models [18]. Equilibrium models have a fixed set of nodes with randomly chosen pairs of nodes connected by links. Erdős and Rényi [19] proposed a basic model of a network with n nodes, where each pair of nodes is connected by a link with probability p. This type of network is commonly referred to as a classical random network. Non-equilibrium network models grow a network by successively adding nodes and setting probabilities for links forming between the new nodes and existing nodes and between already existing nodes. Many of these models, notably the Barabasi and Albert (BA) model, are based on preferential attachment. Preferential attachment assigns a probability of a link forming with a node that is increasing with the number of links of the node. Both the classical random network and the BA network will be used as benchmarks in the following sections.

III. INTERBANK PAYMENTS

We use transaction data from the Fedwire® Funds Service (Fedwire) service to create the interbank payment network. Fedwire is a real-time gross settlement (RTGS) system, operated by the Federal Reserve System, in which more than 9,500 participants initiate funds transfers that are immediate, final, and irrevocable when processed. Participants use Fedwire to process large-value, time-critical payments, such as payments for the settlement of interbank purchases and sales of federal funds; the purchase, sale, and financing of securities transactions; the disbursement or repayment of loans; and the settlement of real estate transactions. Fedwire is used also for the settlement of ancillary payment systems such as automated clearing houses (ACH) and other large
value payment systems e.g. CHIPS and CLS.\textsuperscript{1}

We analyze at the network of the actual payments flows transferred over Fedwire. We choose to model the payment flows as a directed network and establish a link from the sender of payment to the receiver of payment on the basis of payments sent. While Fedwire participants include a variety of entities, including government agencies, we consider only the subset of payments between commercial banks. Thus, commercial banks constitute the nodes in the network, and a directed link from one bank to another is present in a day if at least one transaction debits the account of former and credits the account of the latter.\textsuperscript{2} Additional transactions between any two banks add to the associated link weights in terms of value and volume (number) of payments settled. The network could be defined in alternative ways. From a technical perspective, Fedwire is a star network where all participants are linked to a central hub, i.e., the Federal Reserve, via a proprietary telecommunications network. From a payment processing perspective Fedwire is a complete network as all nodes (participants) are linked in the sense that they can send and receive payments from each other. However, these representations do not represent the actual behavior of participants and the flow of liquidity in the system.

We consider data for the first quarter of 2004. Each day is modeled as a separate network, for an ensemble of 62 daily networks. The average daily value of funds transfers between commercial banks amounts to $1.3$ trillion and the daily number of payments to 345,000. On the peak activity day, 644,000 payments worth more than $1.6$ trillion were processed. The average value per payment is $3$ million, but the distribution is highly right-skew with a median payment of only $30,000$. Both the daily value and volume of payments show periodicity around the first and last days of the month as well as on mid month settlement days for fixed income securities (see Fig. 2).

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{fig1.png}
\caption{a) Simple networks and some commonly used terms. b) Fedwire interbank payment network. First day of sample. 6600 nodes and 70,000 links. c) Core of Fedwire Interbank Payment Network, largest links equivalent to 75 percent of daily value transferred. d) Network Components. GWCC = giant weakly connected component, DC = disconnected component, GSCC = giant strongly connected component, GIN = giant in component, GOUT = giant out component.}
\end{figure}

\textsuperscript{1} The Clearing House Inter-bank Payment System (CHIPS) and Continuous Linked Settlement (CLS).
\textsuperscript{2} We use master-accounts, and exclude loops that result from banks making transfers across their own sub-accounts.
IV. VISUALIZING THE NETWORK

An intuitive way to analyze a network is to draw it as a graph, as in Fig. 1a. The interbank payment network on the first day of our sample is illustrated in Fig. 1b. The figure includes over 6,600 nodes and more than 70,000 links. Each link is shaded by the associated weight, with darker shades indicating higher values. Despite the appearance of giant fur ball, the graph suggests the existence of a small group of banks connected by high value links. To gain a clearer picture of this group, we graph a subset of our network in Fig. 1c where we focus on high value links. This graph shows the undirected links that comprise 75 percent of the value transferred. This network consists of only 66 nodes and 181 links. The prominent feature of this network is that 25 nodes form a densely connected sub-graph, or clique, to which the remaining nodes connect. In other words, we find that only a small number of banks and the links between them constitute the majority of all payments sent over the network.

V. TOPOLOGY CHARACTERISTICS

The large number of nodes and links makes detailed analysis of the structure by visualization difficult and comparisons across time and between networks almost infeasible. The complexity of our network leads us to consider statistical measures. In this section, we describe a series of commonly used statistical measures of topological characteristics for the interbank payment network.

A. Components

A starting point for the quantitative analysis of a network is to partition the set of nodes into components according to how they connect with other nodes. Dorogovtsev et al [17] divide a network into a single giant weakly connected component (GWCC) and a set of disconnected components (DCs). The GWCC is the largest component of the network in which all nodes connect to each other via undirected paths. The DCs are smaller components for which the same is true. In empirical studies the GWCC is found to be several orders of magnitude larger than any of the DCs [13]. This is also the case here.

The GWCC consists of a giant strongly connected component (GSCC), a giant out-component (GOUT), a giant in-component (GIN) and tendrils. The GSCC comprises all nodes that can reach each other through a directed path. A node is in the GOUT if it has a path from the GSCC but not to the GSCC. In contrast, a node is in the GIN if it has a path to the GSCC but not from it. Tendrils are nodes that have no directed path to or from the GSCC. They have a path to the GOUT and/or the GIN (see Fig. 1d).

Over our sample period a total of 7,584 different banks are part of the network. We find that the network’s GWCC is composed of on average 6,490 ± 83 (mean ± standard deviation over the 62 days) banks. On 36 of the 62 days we also find a small number of DCs consisting of between two to eight banks. Over the sample period 6,854 different banks were part of the GSCC. Of these, 2,578 were present in the network on all days. The GSCC contains 78 percent of the nodes in the GWCC on average whereas the GIN, GOUT and tendrils contain 8, 12 and 2 percent, respectively. In terms of value transferred, 90 percent occur within the GSCC and 7 percent is from GIN to GSCC. We will focus on the GSCC component in the analysis below.

B. Size, connectivity and reciprocity

Definition The most basic properties of a network are the number of nodes \( n \) and the number of links \( m \). The number of nodes defines the size of the network while the number of links relative to the number of possible links defines the connectivity of a network. The connectivity \( (p) \) is the unconditional probability that two nodes share a link. For a directed network, the connectivity is \( p = \frac{m}{n(n-1)} \). It ranges from \( \frac{1}{n} \) for a tree network to 1 for a complete network. Reciprocity is the fraction of links for which there is a link in the opposite direction in the network.

Discussion The average size of the daily network was 5,086 ± 128 nodes. Almost 710,000 different links were found between banks over the sample period, with only 11,000 of them present on all days. On average the network had 76,614 ± 151 directed links. In comparison, a complete network of similar size has over 25 million links. The connectivity is only 3 ± 0.1 per mil. In other words, the interbank payment network is externally sparse as 99.7\% of the potential links are not used on any given day. The reciprocity averages 22 ± 0.3 percent. Hence, less than a quarter of the relationships that exist between banks had payments going in both directions.

The number of nodes and links are almost perfectly correlated across days and are both highly correlated with the value and volume of payments settled (see Tab. I). In particular, the size and number of links spike on the high value and volume days identified in section III (see Fig. 2). Interestingly, the connectivity is also highly correlated with value and volume. On high payment activity days, the network not only grows but it also becomes denser as the level of interactions between banks increases faster than size. However, the same is not true for reciprocity. Reciprocity is uncorrelated with value and volume and connectivity. The extent to which the relationships between banks are bilateral does not appear to depend on either the overall level of payment activity or the connectivity between banks.
Amplitude of the time series of the number of nodes and links in giant strongly connected component (GSCC). Bottom: Connectivity and reciprocity in GSCC.

The periodicity in the size and number links suggests that it might be insightful to model high payment activity days separately. For simplicity, we ignore this and treat the networks as coming from the same data generating process.

C. Distance and diameter

Definition The distance from node $i$ to node $j$ ($d_{ij}$) is the length of the shortest path between the two nodes. If node $i$ has a link to node $j$, then $d_{ij} = 1$. The average distance from a node to any other node, commonly referred to as the average path length of a node, is $\ell_i = \frac{1}{n-1} \sum_{j \neq i} d_{ij}$. The average path length of a network is defined as $\langle \ell \rangle = \frac{1}{n} \sum_{i} \ell_i$. In a classical random network $\langle \ell \rangle \approx \frac{\ln(n)}{\ln(p)}$. The eccentricity of a node ($\varepsilon_i$) is the maximum distance to any other node in the network, i.e., $\varepsilon_i = \max_j d_{ij}$. The diameter of a network ($D$) is the maximum eccentricity (or distance) across all nodes, i.e., $D = \max_i \varepsilon_i$. Goh et al. [23] defines the mass distance function as the fraction of nodes within a certain distance of a node. At the network level it is defined as $M(x) = \frac{1}{n(n-1)} \sum_{i} \sum_{j \neq i} 1(d_{ij} \leq x)$, where $1(\cdot)$ is the indicator function taking the value one if true and zero otherwise.

Discussion The average path length is $\langle \ell \rangle = 2.6 \pm 0.2$ across our sample. In comparison, the average path length of a same size classical random network is 3.2. The mean eccentricity is $\langle \varepsilon \rangle = 4.7 \pm 0.33$, and the diameter ranges between 6 and 7 across days (see Tab. II). The interbank payment network exhibits the small-world phenomenon common for many complex networks. Informally, small world means that any node can be reached from any other node in only a few steps. A short path length to any other node is a common property for all nodes in the network as illustrated by the mass distance function is shown in Tab. II. It shows that it is possible for a sparse network with low connectivity to be extremely compact. Although few nodes directly connect, 41 percent are within two links, and 95 percent are within three links from each other. This further reflects the notion that the interbank payment network is comprised of a core of hubs with whom smaller banks interact.

D. Degree distribution

Definition Two important characteristics of a node in a directed network are the number of links that originate from the node and the number of links that terminate
The degree distribution of a classical random network is found to follow the power law,
\[ P(k) \propto k^{-\gamma} \]
where \( P(k) \) is the probability of finding a node with degree \( k \), and \( \gamma \) is the exponent of the power law distribution. Many real networks have fat-tailed degree distributions and a large number have been found to follow power law distributions. The maximum likelihood estimate of the exponent is \( \hat{\gamma} = 2.11 \pm 0.01 \) with a standard error of \( \sigma_{\gamma} = 0.03 \pm 0.001 \). Appendix I describes the estimation procedure. The correlation between in and out degrees across nodes is 0.97 and the in-degree distribution looks similar to the out-degree distribution. It has a lower power law coefficient of \( \hat{\gamma} = 2.15 \pm 0.01 \) with the same standard error. The degree distributions are comparable to those of the Japanese interbank payment system (BOJ-NET) reported in Inaoka et al. [26].

A degree distribution following a power law distribution with a coefficient between 2.1 and 2.3, is not unique to payment systems, and appears to be a common feature in complex networks. Albert et al. [3], and Crucitti et al. [15] find that scale-free networks are robust to random failures, but vulnerable to targeted attacks.

### Table II: Turnover, component and network statistics for the Fedwire interbank payment network, fourth quarter 2004

<table>
<thead>
<tr>
<th>Payments</th>
<th>Volume (trln)</th>
<th>Value ($tr)</th>
<th>Average ($mn)</th>
<th>Components</th>
<th>GWCC</th>
<th>DC</th>
<th>GSCC</th>
<th>GOUT</th>
<th>Tendrils</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mean</td>
<td>Median</td>
<td>Min.</td>
<td>Max.</td>
<td>SD</td>
<td>Mean</td>
<td>Median</td>
<td>Min.</td>
<td>Max.</td>
</tr>
<tr>
<td></td>
<td>436</td>
<td>411</td>
<td>371</td>
<td>644</td>
<td>60.3</td>
<td>3.01</td>
<td>3.06</td>
<td>2.48</td>
<td>3.35</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Distance Measures</th>
<th>Mean</th>
<th>Median</th>
<th>Min.</th>
<th>Max.</th>
<th>SD</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \langle \ell \rangle )</td>
<td>2.62</td>
<td>2.63</td>
<td>2.56</td>
<td>2.66</td>
<td>0.02</td>
</tr>
<tr>
<td>( \langle \varepsilon \rangle )</td>
<td>4.67</td>
<td>4.63</td>
<td>4.18</td>
<td>5.74</td>
<td>0.33</td>
</tr>
<tr>
<td>( D )</td>
<td>6.6</td>
<td>7</td>
<td>6</td>
<td>7</td>
<td>0.5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Components</th>
<th>M(2) (%)</th>
<th>M(3) (%)</th>
<th>M(4) (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>GWCC</td>
<td>41.6</td>
<td>41.3</td>
<td>38.9</td>
</tr>
<tr>
<td>DC</td>
<td>47.3</td>
<td>97.1</td>
<td>100.0</td>
</tr>
<tr>
<td>GSCC (n)</td>
<td>95.9</td>
<td>95.8</td>
<td>95.1</td>
</tr>
<tr>
<td>GOUT</td>
<td>99.9</td>
<td>99.9</td>
<td>99.8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Connectivity and Reciprocity</th>
<th>Max ( k_{out} )</th>
<th>Min ( k_{in} )</th>
<th>Max ( \varepsilon )</th>
<th>( \hat{\gamma}^{out}_{MLE} )</th>
<th>( \hat{\gamma}^{in}_{MLE} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( m )</td>
<td>1,922</td>
<td>1,772</td>
<td>2,269</td>
<td>121</td>
<td></td>
</tr>
<tr>
<td>( p ) (%)</td>
<td>2.097</td>
<td>2.070</td>
<td>1.939</td>
<td>2.394</td>
<td>115</td>
</tr>
<tr>
<td>( r ) (%)</td>
<td>2.11</td>
<td>2.11</td>
<td>2.09</td>
<td>2.14</td>
<td>0.01</td>
</tr>
</tbody>
</table>

The average degree in the network is \( \langle k \rangle = 15.2 \pm 0.8 \). However, most banks have only a few connections and a small number of "hubs" have thousands of links to other banks. Almost half of all banks have 4 or fewer outgoing links and 15 percent have only a single outgoing link. The banks with the largest in- and out-degrees averaged 2,097±115 and 1,922±121 links respectively. The out-degree distribution of the interbank payment network is shown in Fig. 3a together with the degree distribution for a classical random network with the same connectivity. For degrees greater than 1, the distribution follows a power law. The maximum likelihood estimate of the coefficient is \( \hat{\gamma} = 2.11 \pm 0.01 \) and the in-degree distribution looks similar to the out-degree distribution. It has a lower power law coefficient of \( \hat{\gamma} = 2.15 \pm 0.01 \). Appendix I describes the estimation procedure. The correlation between in and out degrees across nodes is 0.97 and the in-degree distribution looks similar to the out-degree distribution. It has a lower power law coefficient of \( \hat{\gamma} = 2.15 \pm 0.01 \). The degree distributions are comparable to those of the Japanese interbank payment system (BOJ-NET) reported in Inaoka et al. [26].

A degree distribution following a power law distribution with a coefficient between 2.1 and 2.3, is not unique to payment systems, and appears to be a common feature in complex networks. Albert et al. [3], and Crucitti et al. [15] find that scale-free networks are robust to random failures, but vulnerable to targeted attacks.

---

3 The term "scale-free" refers to the fact the the distribution remains unchanged within a multiplicative factor under a rescaling of the random variable, i.e., \( P(ak) = aP(k) \) (Newman [32] p. 186). For example, if a bank with four links is twice as likely as one with eight links, then a bank with eight links should also be twice as likely as a bank with 16 links and so on.

4 Inaoka et al [26] and Boss et al. [12], both find evidence of scale-free distributions in their tails of their networks. Inaoka et al. report a degree distribution with a power law tail of 2.3 for \( k > 20 \) and Boss et al. report a coefficient of 3.1 for the out-degree and 1.7 for in-degree \( k > 40 \).

5 Power law degree distributions have been observed in a wide variety of systems, including the phone call network [1], the metabolic network of E. coli bacteria [27], the movie actor collaboration network [6], and the World Wide Web [2]. Although the observation of power-law behavior in complex networks is recent, the phenomena was observed by as long ago as 1896, by Vilfredo Pareto in the distribution of income [34].
E. Degree correlations

Definition The probability that a node connects to another node may depend on the characteristics of the respective nodes. One characteristic of a node that is endogenous to the structure of the network is its degree. In an uncorrelated network there is no dependence between the degree of a node and the degrees of its neighbors. A network is said to be assortative if nodes with a given degree are more likely to have links with nodes of similar degree. A network is said to be disassortative if the opposite is true, i.e., nodes with low degrees are more likely to be connected to nodes with high degrees, and vice versa (e.g., Catanzaro et al [14]). The sign of the Pearson correlation coefficient between the degree of each node at the end of a link shows the direction of the dependency: zero for uncorrelated networks, positive for assortative networks and negative for disassortative networks. Another method is to compute the average degree of the nearest neighbors of a node as a function of the node degree. This is known as the average nearest neighbor degree (ANND) function, \( \langle k_{nn} \rangle (k) \).

Discussion Both the correlation coefficients and the average nearest neighbor degree functions show that the interbank payment network is disassortative. For example, the correlation of out degrees is \(-0.31\) and the ANND defined for the out-degree of successors is inversely related to the out degree of a node as shown in Fig. 3b. Using other combinations of neighbors and degree direction, we get similar coefficients. Disassortivity is more common among technological and biological networks, as opposed to social networks which tend to exhibit assortativity.

\[ P(k'|k) \] denote the probability of two nodes, with degrees \( k' \) and \( k \), being joined by a link. The conditional probability of a node with degree \( k \) being joined to a node of degree \( k' \) node is given by

\[
P(k'|k) = \frac{P(k', k)}{P(k)}
\]

where \( P(k) \) is the degree distribution. The average nearest neighbor degree (ANND) function is given by

\[
\langle k_{nn} \rangle (k) = \sum_{k'} k' P(k'|k).
\]

6 In general, the correlations as well as the ANND function can be defined for any combination of in and out degree of nodes. Moreover, the ANND function can be defined for any set of nearest neighbors e.g. predators or successors (see Serrano et al [36]).
tative properties [32]. Moreover, Newman [31] shows that assortative networks percolate more easily than disassortative networks and that they are more robust to node removal.

F. Clustering coefficient

Definition Another common correlation between nodes is the probability that two nodes which are the neighbors of the same node, themselves share a link. This is equivalent to the observation that two people, each of whom is your friend, are likely to be friends with each other. One way of measuring the tendency to cluster is the ratio of the actual number of directed links between the neighbors of a node \((m_{nn,i})\) over the number of potential links among them

\[
C_i = \frac{m_{nn,i}}{k_i(k_i - 1)}
\]

The clustering coefficient for the entire network, \((C)\), is given by the average of all individual coefficients [38]. A tree network has a clustering coefficient of zero, and a complete network a coefficient of one. In a classical random network, the clustering coefficient is the unconditional probability of connection, i.e., \((C) = p\).

Discussion The average clustering coefficient for the networks calculated for the successors of node is 0.53 ± 0.01 suggestive of cliquishness in the interbank payments. As such the observed clustering coefficient of the network is 90 times greater than the clustering coefficient of a comparable random network. However, the clustering coefficient for the network as a whole conceals the fact that the clustering across nodes is highly disperse, as illustrated in Fig. 3c. More than 35 percent of the nodes have either a coefficient of zero or one. This is largely the result of low degree nodes.\(^7\) Ignoring nodes with a degree smaller than three increases the average clustering coefficient to 0.62. A high level of clustering is observed in many other real world networks [38].

G. Link Weights and Node Strength

Definition Weights \((w_{ij})\) are assigned to the links in a network to show the importance of each link. Barrat et al. [8] define strength \((s_i)\) of a node as the sum of the weights of all the links attached to it, i.e., \(s_i = \sum_j w_{ij}\), and suggest calculating the average strength as a function of the degree of a node, \(s(k)\), in order to investigate the relationship between these two node characteristics. For a directed network, strength can be defined over both the incoming and outgoing links.

Discussion The average weight per link in terms of value and volume are $15.2 ± 0.8$ million and $5.2 ± 0.3$ payments, respectively. The distribution of link weights follow a power law when weighted by the volume of payments but when weighted by the value of payments, the distributions of the link weights is closer to a lognormal distribution. The same is true for the distribution of node strengths (see Fig. 3d).

For both weight measures, strength increases faster than the degree of a node. Like Barrat et al. [8], we see a power-law relationship between (out) strength and the degree of a node, \(s(k) \sim k^\beta\). The coefficient is \(\hat{\beta}_{\text{volume}} = 1.2\) when volume is used as weight and it is \(\hat{\beta}_{\text{value}} = 1.9\) when value is used (see Fig. 4). More connected nodes transact a higher value and volume of payments than would be suggested by their degree alone. For example, if a bank has twice as many out links as another bank, it would be expected to send 2.4 times the number of payments, and 3.8 times the value of payments.

VI. THE IMPACT OF SEPTEMBER 11TH ON NETWORK TOPOLOGY

The terrorist attacks of September 11th, 2001 disrupted the financial systems of the United States, including the interbank payment system. The attacks affected the structure of the interbank payment network in two ways. First, the massive damage to property

\(^7\) In a scale-free network low degree nodes are plentiful as discussed above. If a node has a degree of one, then the clustering coefficient is by definition zero. Moreover, all nodes in a triplet, which consists of nodes with degree two, have a clustering coefficient of one.
and communications systems in lower Manhattan made it more difficult, and in some cases impossible, for many banks to execute payments to one another [21, 28], i.e., some nodes were removed from the system or had their strength reduced. Second, the failure of some banks to make payments disrupted the payment coordination by which banks use incoming payments to fund their own transfers to other banks. Once a number of banks began to be short of incoming payments, others became more reluctant to send out payments themselves, i.e., links were either removed or had their weight reduced [21, 30].

Both effects reduced the circulation of funds and collectively banks were growing short of liquidity. The Federal Reserve recognized this trend toward illiquidity and provided liquidity through the discount window and open market operations in unprecedented amounts in the following week [21]. The impact on the interbank payment network is summarized in Table III and Figure 5. The number of nodes in the giant weakly connected component decreased by 5 percent from 6,755 to 6,466, while the number of nodes in the giant strongly connected component (GSCC) decreased by 10 percent, from 5,325 to 4,795. The relative size of the GSCC on September 11th was 6 percentage points lower than typical, as non-offsetting payment flows placed more nodes in the giant in- and giant out-components. The number of nodes in the GSCC did not return to its normal level until September 14th.

The connectivity on September 11th dropped from 3.0 per mil to 2.6 per mil. After two days of low connectivity, the connectivity shot up to over 3 per mil from the 14th to 17th. This “overshooting” is likely the result of banks settling payments they had delayed in the days after September 11th.

As the connectivity decreased and key nodes were removed from the system, the average distance between nodes increased. The mass distance function on September 11th was well below its normal range. Thus both the average path length and the average eccentricity rose (see Table III). The local structure of the network was also disrupted. Reciprocity fell from 24 percent to 22 percent, and the clustering coefficient from 0.52 to 0.47. These results are indicative of the breakdown in the coordination between banks found in [30].
that the topology of the network was significantly altered by the attacks of September 11th, 2001. The number of nodes and links in the network and its connectivity was reduced, while the average path length between nodes was significantly increased.

Because scale-free networks are found in many areas, the performance of such networks under ordinary and disrupted conditions is receiving increasing attention. Static scale-free networks, for example, have been found to preserve their connectivity under random node removal yet to be vulnerable to disconnection following removal of high-degree nodes [3]. The vulnerability of a particular network depends both on its structure and on the mechanisms of contagion. As these differ across networks, we cannot extrapolate this conclusion to payment networks. In the case of a payment system, understanding the dynamics of the liquidity flows is essential for assessing network robustness. A question for further research is how the degree distribution and other topological measures relate to contagion of disturbances.

Finally, many of the network statistics appear to vary periodically and abruptly. An interesting question is whether the networks of daily payments naturally form distinct clusters, and what processes create such distinctions. The scale-free daily network is constructed from individual payments accumulated over the day. Analysis of the intra-day payment data will give us insights into how the network forms and on the regularity of this process.

### VII. CONCLUSION

In this paper, we analyzed the topology of the 62 daily networks formed by the payment flows between commercial banks over Fedwire. These networks share many of the characteristics commonly found in other empirical complex networks, such as a scale-free degree distribution, high clustering coefficient and the small world phenomenon. The network is disassortative like many other technological networks. We also found that, apart from a few holidays, the statistics characterizing the network are quite similar from day to day. Moreover, we found that the topology of the network was significantly altered by the attacks of September 11th, 2001. The number of nodes and links in the network and its connectivity was reduced, while the average path length between nodes was significantly increased.

Because scale-free networks are found in many areas, the performance of such networks under ordinary and disrupted conditions is receiving increasing attention. Static scale-free networks, for example, have been found to preserve their connectivity under random node removal yet to be vulnerable to disconnection following removal of high-degree nodes [3]. The vulnerability of a particular network depends both on its structure and on the mechanisms of contagion. As these differ across networks, we cannot extrapolate this conclusion to payment networks. In the case of a payment system, understanding the dynamics of the liquidity flows is essential for assessing network robustness. A question for further research is how the degree distribution and other topological measures relate to contagion of disturbances.

Finally, many of the network statistics appear to vary periodically and abruptly. An interesting question is whether the networks of daily payments naturally form distinct clusters, and what processes create such distinctions. The scale-free daily network is constructed from individual payments accumulated over the day. Analysis of the intra-day payment data will give us insights into how the network forms and on the regularity of this process.

### I. MAXIMUM LIKELIHOOD ESTIMATION OF THE POWER LAW EXPONENT

In recent years, a significant amount of research has focused on showing that the distribution of many physical and social phenomena follow a power-law, i.e., \( P(k) \sim k^{-\gamma} \). Maximum likelihood estimators for slope coefficient \( \gamma \) for the discrete and continuous case are derived in Goldstein et al. [24] and Newman [33], respectively. Since, many empirical distributions are found only to follow a power law in the right hand tail of the distribution, i.e., \( P(k) \sim k^{-\gamma} \) for \( k > a \), we derive the maximum likelihood estimator for a truncated power law distribution. The probability distribution of a truncated random variable is given by

\[
P(k|k > a) = \frac{P(k)}{1 - P(k \leq a)}
\]

In the discrete case the power law distribution is given by

\[
P(k) = \frac{k^{-\gamma}}{\zeta(\gamma)}
\]

where \( \zeta(\gamma) \) is the Riemann Zeta function. Hence, we have

\[
P(k|k > a) = \frac{k^{-\gamma}}{1 - \sum_{k=1}^{\infty} \frac{k^{-\gamma}}{\zeta(\gamma)}} = \frac{k^{-\gamma}}{\zeta(\gamma, a)}
\]

where \( \zeta(\gamma, a) \) is the Hurwitz Zeta function. Analogous to Goldstein et al [24] we have that maximum likelihood estimator, \( \hat{\gamma}_{MLE} \), equates the negative logarithmic derivative of the Hurwitz Zeta function with the average logarithm of the data in the sample, i.e.,

\[
\frac{\zeta'(\gamma, a)}{\zeta(\gamma, a)} = \frac{1}{n} \sum_{i} \log(x_i)
\]
The equation can be solved numerically for $\hat{\gamma}_{{MLE}}$. An estimate of the standard error of the maximum likelihood estimator can be computed by evaluating the second derivative of the log-likelihood function at $\hat{\gamma}_{{MLE}}$

$$\hat{\sigma}_{{MLE}} = \frac{1}{\sqrt{n}} \sqrt{\frac{\zeta''(\hat{\gamma}_{{MLE}}, a)^2}{\zeta''(\hat{\gamma}_{{MLE}}, a) \zeta'(\hat{\gamma}_{{MLE}}, a) - \zeta'(\hat{\gamma}_{{MLE}}, a)^2}}$$

Acknowledgments

The authors would like to thank Doug Conover and Travis Nesmith for helpful comments. R.J. Glass and W.E. Beyeler were supported through the National Infrastructure Simulation and Analysis Center (NISAC), a program of the Department of Homeland Security’s Infrastructure Protection/Risk Management Division and comprised of a core partnership of Sandia National Laboratories and Los Alamos National Laboratory. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company for the United States Department of Energy’s National Nuclear Security Administration under contract DE-AC04-94AL85000. Algorithms in the Jung (Java Universal Network/Graph Framework) libraries were used to calculate network statistics and Pajek [9] to produce Figure 1b and 1c.