A Robustness Analysis of the Rabobank Intrabank Network

Candidate Number: SCQZ8*

MEng Mathematical Computation

Supervisor: Fabio Caccioli

Submission date: April 27, 2022

Abstract

Many complex real-life systems can be represented as a network, where the parties and their various interactions are vertices and edges respectively. A question that appears often in these models is whether the overall system is robust to the failure of its components, be it through random error or targeted attack. This question can be tackled by investigating how the topology of the network varies in response to the removal of vertices and edges according to some attack strategy. In this report, we study the robustness of the Rabobank Intrabank network by performing various attack strategies and comparing these results with those of random networks sharing the same degree distributions. This will be the first ever robustness analysis on an intrabank network to our knowledge, in which users of the bank (in this case Rabobank) define the nodes and their transactions between other users define the edges.

Contents

1 Introduction **5**

2 Background and Literature Review **7**
2.1 Graph Theory 7
2.1.1 Graph Matrices and Spectra 7
2.1.2 Clustering or Transitivity 8
2.1.3 Assortativity 8
2.1.4 Centrality Measures 9
2.2 Random Graph Theory 10
2.2.1 The Erdős–Rényi Model 10
2.2.2 Graph Evolution and the Giant Component 11
2.2.3 Scale-Free Models 11
2.2.4 The Configuration Model 12
2.2.5 Maximum Entropy Models 12
2.3 Percolation Theory 13
2.3.1 The Infinite Cluster 13
2.3.2 Phase Transitions 13
2.3.3 Links to Graph Theory 14
2.3.4 Bounding the Percolation Threshold 15
2.4 Markov Chains 16
2.4.1 Total Variation Distance and Mixing Times 16
2.5 Previous Work 17

3 Methodology **20**
3.1 The Rabobank Transactions Dataset 20
3.2 Dataset Cleaning 20
3.3 Network Construction 20
3.4 Exploiting Network Sparsity 21
3.5 Computing and Estimating Centrality Measures 21
3.6 Performing and Evaluating Percolation 22
3.6.1 Vertex Attack Strategies 22
3.6.2 Edge Attack Strategies 23
3.6.3 Executing Attack Strategies 23
3.6.4 Measuring Strategy Effectiveness 24
3.7 Choosing a Configuration Model 24
3.8 Sampling from a Configuration Model 25
3.9 Using the Configuration Model as a Null Model 27
3.10 Tools for Network Analysis 28

4 Results **29**
4.1 Vertex Attacks 29
4.2 Edge Attacks 30
4.3 Graph Measures 35

5 Conclusion and Future Work **38**

A Appendix **46**
A.1 Source code 46

1 Introduction

The solvency of all banks does not imply zero systemic risk. As demonstrated by the global financial crisis in 2007/08, a small shock in the liquidity or solvency of a financial institution can cascade across the linkages of each institution, in a process known as financial contagion. Recent events such as these have prompted academic focus into interbank networks. This includes extensive research on how these networks respond to the insolvency of single banks, and how central banks can regulate the provision of liquidity across the network (and thus its topology as a whole). Allen and Gale [1] examined a model in which contagion arises from uncertainty about when depositors should consume, they considered - using a simple interbank network of four banks - the trade-off between the probability of contagion and the sharing of risk between banks. Freixas et al. [2] showed that in their model, consumers are instead uncertain about *where* to consume. Acknowledging that information regarding solvency of each bank is imperfect, they proposed a set of policies which central banks can use to intervene in the cases of insolvency and speculative gridlock. Both papers demonstrate that homogeneity of interbank claims across the network results in increased robustness to contagion. Both Gai and Kapadia [3] and Acemoglu, Ozdaglar, and Tahbaz-Salehi [4] reinforced this claim, showing that dense networks are more robust to shocks, however, the increased risk of contagion due to larger shocks in highly connected networks was also emphasised. Elliott, Golub and Jackson [5] analysed the tradeoffs between diversification (the spread of assets to other banks) and integration (reliance on other banks). They showed that financial networks with middle ranges in both diversification and integration are most susceptible to cascading failure.

The desire to discern properties of biological, technological, social, and information-based systems has elicited the study of network science. Robustness of complex networks is one such example. In the Internet, it is important to understand the effect a random failing router has on its connectivity and by extension, its overall functionality. In a food-web network (a network of predator-prey relations), we gain an increased understanding of the importance of each species to the ecosystem by studying how robust the food-web is to their removal. Resilience studies of physical contact contagion networks gives us insight into the impact of vaccination. Analysis of structure and robustness has been performed on many other complex networks. Cohen, Erez, ben-Avraham, and Havlin [6] showed analytically that scale-free networks are mostly resilient to random error, but vulnerable to targeted attack. Jeong *et al.* [7] studied complex networks representing metabolic pathways, a network formed from substrates and products connected by the various chemical reactions that take place. They showed that these networks possess a similar error tolerance - implying a resilience to random substrate mutation - but again are vulnerable to targeted attack. Onnela *et al.* [8] considered a network of phone call records, they studied the robustness of the network to targeted link attacks based on overlap, weight, and betweenness. Broder *et al.* [9] analysed the macroscopic structure of the World Wide Web using web crawlers. Interestingly,

they found that it comprises four main segments, the central core (SCC), pages disconnected from the SCC, pages that cannot be reached by the SCC yet can reach it, and vice versa.

Although substantial work has been done to understand the structure and dynamics of many complex networks, *intra*-bank networks have not been studied enough. The study of inter-bank networks gives us a macroeconomical rather than microeconomical understanding of the flow of securities. Saxena *et al.* [10] were the first to study the properties of intra-bank networks, considering the Rabobank transactions dataset. However, the robustness of this network was not investigated. In this report, we construct a network using the Rabobank transactions dataset, and perform a detailed robustness analysis of it by comparing the performance of multiple node and edge attack strategies. We additionally investigate the robustness of networks sampled from a configuration model using the same degree sequence as our network, and attempt to justify why these results differ. This will be the first study of the robustness of publicly available intrabank (transaction) networks to our knowledge, and as such, we aim in this report to further our understanding of the resilience of money flow *within* financial institutions. As described by Barabási *et al.* [11], "we will never understand complex systems unless we develop a deep understanding of the networks behind them"; in our case, studying the robustness of transaction networks provides insight into the influence each buyer/seller and their actions exude over the flow of securities within the system.

The report is organised as follows. In section II we present the reader with a brief review of the tools and concepts present within graph theory, random graph theory, and percolation theory. Markov chains are also briefly introduced. We use these tools and concepts in section III to describe the methods we use to analyse robustness, with a detailed discussion of our findings in section IV. In section V we give our conclusions, summarising our results and describing potential future works.

2 Background and Literature Review

2.1 Graph Theory

A graph [12] is a tuple $G = (V, E)$, where V and $E \subseteq V \times V$ denotes the set of vertices and edges respectively. These edges may be either directed (corresponding to a digraph) or undirected. We can define a function $w \colon E \to \mathbb{C}$, representing the weight of each edge. Graphs with edge weights are known as weighted graphs. The number of edges incident to a vertex is referred to as its degree, and its strength refers to the sum of the incident weights. For digraphs, we also use the terms in/out-degree and in/out-strength, where we keep the direction of the edges into account.

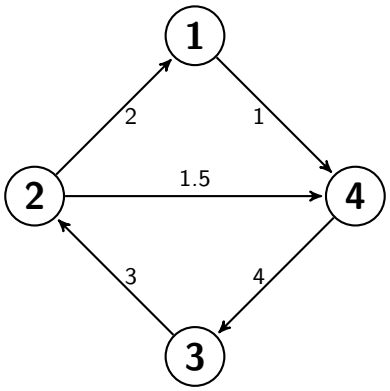


Figure 1: A weighted digraph with $|V| = 4$ vertices and $|E| = 5$ edges. $V = \{1, 2, 3, 4\}, E = \{(1, 4), (4, 3), (3, 2), (2, 1), (2, 4)\}$, $w((1, 4)) = 1, w((4, 3)) = 4, w((3, 2)) = 3, w((2, 1)) = 2, w((2, 4)) = 1.5$.

Additionally, a subgraph $G' \subseteq G$ is defined as the tuple (V', E') where $V' \subseteq V$ and $E' \subseteq E$. Defining a path of a graph G as a sequence of edges in G, we call G connected if there exists a path between all pairs of vertices in G. We then call a subgraph of G a connected component if it is connected and adding more edges does not preserve connectivity. This definition is extended to digraphs, in which case they are referred to as strongly connected components.

2.1.1 Graph Matrices and Spectra

The adjacency matrix [13] A of a graph G is a $|V| \times |V|$ matrix where $A_{i,j} = 1$ if $(i, j) \in E$ and 0 otherwise. This extends to weighted graphs by letting $A_{i,j} = w((i, j))$, for example, the graph in Figure 1 has the following weighted adjacency matrix

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 1.5 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 4 & 0 \end{pmatrix}$$

Defining the degree matrix D of G as $D_{i,j} = \delta_{ij}\, deg(i)$ where δ_{ij} is the Kronecker Delta Function ($\delta_{ij} = 1 \Leftrightarrow i = j$), we call the matrix $L = D - A$ the Laplacian matrix of G. In the digraph case, we use the out-degree [14].

The spectrum [15] of these matrices is defined as their set of eigenvalues. Graph spectra encodes many properties of their corresponding graphs [16, 17], and has various applications, including bottleneck [18, 19] and community [20] detection.

Another popular matrix in spectral graph theory is the Hashimoto [21] matrix $\mathbf{h}$, which for a graph (V, E) is a $2|E| \times 2|E|$ matrix indexed by edges, where

$$h_{i\to j,k\to l} = \begin{cases} 1, & \text{if } k \neq j, l = i \\ 0, & \text{otherwise.} \end{cases} \tag{1}$$

Entries can also be given in the more compact form $h_{i\to j,k\to l} = \delta_{jk}(1 - \delta_{il})$. $h_{i\to j,k\to l} = 1$ implies the existence of a path from i to j, proceeding to k, and not backtracking to i, thus $\mathbf{h}$ is also called the non-backtracking matrix. The spectrum of this matrix can be used to lower bound the percolation threshold of a graph, which will be discussed later in this section.

2.1.2 Clustering or Transitivity

Vertices possessing some degree of transitivity is a property that often arises in networks. By this we mean that if $(i, j), (j, k) \in E$, it is also likely that $(i, k) \in E$. Thus, a high transitivity implies a high number of triangles in the network. We can quantify transitivity in networks using the global clustering coefficient [22]

$$C = 3 \times \frac{\text{number of triangles}}{\text{number of connected triples}} \tag{2}$$

where a triple is a vertex connected to two other vertices. Note that a triangle consists of three triples, so C can be interpreted as a proportion of closed triples (triples forming a triangle) within the network. Hence, $0 \leq C \leq 1$.

2.1.3 Assortativity

The assortativity of a graph $G = (V, E)$ is the propensity of its vertices to connect to ones with similar properties. We can measure this property using the assortativity coefficient [23] r, defined as

$$r = \frac{\sum_{i=1}^{N} e_{ii} - \sum_i a_i b_i}{1 - \sum_i a_i b_i} \tag{3}$$

where e_{ij} denotes the proportion of edges to and from a type j and i vertex respectively, $a_i = \sum_j e_{ij}$, and $b_j = \sum_i e_{ij}$. The type of a vertex depends on the similarity measure being used. For instance, working with degrees, vertices are of the same type if and only if their degrees are equal. In this report, and

various other literatures, we use this measure of similarity, writing

$$r = \frac{\sum_{i,j=1}^{N}(A_{ij} - d_i d_j/2M)d_i d_j}{\sum_{i,j=1}^{N}(d_i\delta_{ij} - d_i d_j/2M)d_i d_j} \tag{4}$$

where $M = |E|$ and $d_i = deg(i)$. Noting that $-1 \leq r \leq 1$, we call a graph perfectly assortative if $r = 1$, non-assortative if $r = 0$, and perfectly disassortative if $r = -1$.

2.1.4 Centrality Measures

Centrality measures are tools for providing orderings of vertices based on their influence within a network. There are several measures of centrality, and the rank of importance of each vertex is dependent on the measure used.

The first measure is **degree centrality**, where we use the degree of each vertex. This measure is concerned with the immediate effect of a vertex, rather than how it can propagate across a network. For example, in a financial contagion model for interbank networks, the probability of immediate failure for a given node is dependent on its degree, as a high degree results in a higher chance it is linked to an insolvent bank.

A different measure known as **eigenvector centrality** considers both the number of neighbouring vertices and their importance. The eigenvector centrality $\mathbf{v}$ is the principal eigenvector of the adjacency matrix A. This can be written as

$$A\mathbf{v} = \lambda\mathbf{v} \tag{5}$$

where λ denotes the largest eigenvalue of A. By the Perron-Frobenius theorem, $\mathbf{v}$ has no negative components. Thus, for a vertex i, we take its eigenvector centrality to be $\mathbf{v}_i$.

Another measure of centrality is betweenness. The **betweenness centrality** b_v of a node v is defined as

$$b_v = \sum_{\substack{s\neq v\neq t\in V \\ s\neq t}} \frac{\sigma(s,t|v)}{\sigma(s,t)} \tag{6}$$

where $\sigma(s,t)$ denotes the number of geodesic (shortest) paths between nodes i and j, and $\sigma(s,t|v)$ denotes the number of these paths that contain v. Betweenness centrality can be interpreted as the share of geodesic paths that need v, and can therefore be thought of as a measure of how much the flow of information within the network depends on v.

We also use the idea of *closeness* to rank importance in networks. The **closeness centrality** of a vertex v is defined as

$$c_v = \frac{1}{\sum_u d_{uv}} \tag{7}$$

where d_{uv} denotes the distance from vertex u to v[1]. The closeness centrality of a vertex can be interpreted as its ability to propagate information across a network; the higher the centrality, the closer the vertices are on average, resulting in easier spreading of information.

The final measure we will consider is **PageRank centrality**, focusing on directed graphs. The PageRank centrality of a vertex v is defined recursively as

$$PR(v) = d \sum_{u \in V} \frac{A_{uv}}{d^+(u)} PR(u) + \frac{1-d}{|V|} \tag{8}$$

where $d^+(u)$ denotes the out-degree of u, A is the adjacency matrix and $d \in [0, 1)$ is a damping factor. PageRank centrality assigns higher values to vertices with a high in-degree, vertices with incoming neighbors of high PageRank, and vertices with incoming neighbors possessing small out-degrees.

2.2 Random Graph Theory

Random graph theory - pioneered by Erdős and Rényi [24, 25] - is concerned with the probability space associated with graphs as the number of vertices N tends to infinity, and the properties of such spaces. In this section we give a brief overview of the study.

2.2.1 The Erdős–Rényi Model

The Erdős–Rényi Model [24] was the first model used to study random graphs. The model $G(N, M)$ takes N vertices and samples M edges uniformly from the $\binom{N}{2} = \frac{N(N-1)}{2}$ possible edges. As Erdős and Rényi [25] explain, we can interpret M as time, and $G(N, M)$ as a *stochastic process* over discrete time, where at time $t = m$ we sample a single edge from the $\binom{N}{2} - m - 1$ possible edges. These stochastic processes are called *graph processes*. The probability of sampling a graph G from $G(N, M)$ is

$$P(G) = \binom{\binom{N}{2}}{M}^{-1}. \tag{9}$$

Another formulation of the model is $G(N, p)$, where p denotes the probability of an edge being formed between two of the N vertices. Under this model, the probability of a vertex having degree k - known as the degree distribution - follows a binomial distribution $B(N-1, p)$

$$P(k) = \binom{N-1}{k} (1-p)^{N-k-1} p^k \tag{10}$$

and the probability of sampling a graph G with M edges is

$$P(G) = (1-p)^{\binom{N}{2}-M} p^M \tag{11}$$

[1] We set d_{uv} to zero if no path exists

which is not uniform. The main difference between the two formulations is that the latter is constrained by an *expected* edge count, rather than an exact one.

2.2.2 Graph Evolution and the Giant Component

We define an evolution of a graph to be a trajectory of its graph process. One of the more surprising results of the work by Erdős and Rényi was that for almost every[2] graph evolution in their model, there is an abrupt change in topology. This sudden 'phase transition' occurring at $t = t_c \approx \lfloor N/2 \rfloor$ gives rise to what is known as the *giant component*, which contains approximately $N^{2/3}$ vertices [25]. For times $t < t_c$, the largest component has $\mathcal{O}(\log N)$ vertices.

Erdős and Rényi state that $G(N, p)$ yields similar results, in which case we can think of this threshold not as time, but rather as a *probability*. That is, there exists a critical probability p_c for which a giant component is formed, and for $p < p_c$ the largest component again has $\mathcal{O}(\log N)$ vertices. These fascinating results were further generalised by Bollobás and Thomason [26], showing that every non-trivial monotone graph property possesses such a threshold.

2.2.3 Scale-Free Models

A network is said to be scale-free if its degree distribution follows a power-law [36]

$$P(k) \sim k^{-\gamma} \tag{12}$$

where γ is some exponent, usually such that $2 < \gamma < 3$. Scale-free networks possess a slowly decaying degree distribution, resulting in a higher likelihood of a node of large degree existing. Many real-life complex networks have been shown to be scale-free, including interbank markets [27, 28] and the Internet [29].

Barabási and Albert [30] proposed two principles critical to the existence of scale-free networks, namely *growth* and *preferential attachment*. The growth mechanism is where the number of nodes in the network can be represented as a monotonic nondecreasing function of time, while preferential attachment is where new nodes have a propensity to connect to nodes of high degree. An example of preferential attachment is evident in social networks, where new users are more likely to be friends with already popular users.

Most scale-free networks boast a high resilience to random breakdown, with a critical probability $p_c \approx 1$. Cohen *et al.* [31] showed that as the number of nodes $N \to \infty$ we have

$$\kappa_0 \to \frac{\gamma - 2}{\gamma - 3} \begin{cases} m, & \text{if } \gamma > 3 \\ m^{\gamma-2} K^{3-\gamma}, & \text{if } 2 < \gamma < 3 \\ K, & \text{if } 1 < \gamma < 2 \end{cases} \tag{13}$$

where m and K are the minimum and maximum degrees respectively, and

$$1 - p_c = \frac{1}{\kappa_0 - 1} \tag{14}$$

[2] 'Almost every' means that the probability tends to 1 as $N \to \infty$

implying that $p_c \to 1$ for all $\gamma < 3$. The resilience to random error of scale-free networks is due to the high number of nodes with low connectivity, resulting in a high probability of random error affecting these nodes, barely impacting the overall connectivity of the network.

2.2.4 The Configuration Model

In statistical mechanics, the configuration model fixing a given degree sequence[3] is known as a microcanonical ensemble [32]. Thus it can also be described as a probability space over networks of the same degree sequence, with a uniform distribution. Configuration models serve as a null model, which we can use to compare the properties observed from real-world networks to those of graphs sampled from a graph space.

These models heaviliy depend on the choice of graph space. For instance, the space of graphs that can include parallel edges and the space of simple graphs correspond to different configuration models, since we cannot sample a graph with parallel edges from the latter. It is this property that makes the choice in graph space important when using configuration models as null models.

2.2.5 Maximum Entropy Models

Given a probability measure P and graph space $\mathcal{G}$, we say $\mathcal{G}$ is a graph ensemble if P is defined on it. We can then write the Shannon entropy

$$\mathcal{S}[P] = -\sum_{G \in \mathcal{G}} P(G) \log P(G). \tag{15}$$

This is equivalent to the Gibbs entropy of $\mathcal{G}$. We can identify a unique distribution P^* that maximises $\mathcal{S}[P]$ under some constraint, which we call the maximum-entropy ensemble [33]; if the constraint is exact, we say P^* is microcanonical, otherwise it is known as canonical. Intuitively, we can consider this method of maximum entropy as an optimisation problem, where we seek to minimise the uncertainty that P^* contains in a "maximally noncommital" fashion [34], making little assumptions about the distribution. Maximum entropy models given some constraint are unbiased models of random graphs under the same constraint, and can thus be referred to as null models.

Consider the simple example of finding the maximum-entropy ensemble given the exact constraint of having a fixed number N and M of nodes and edges respectively. We wish to maximise the Gibbs entropy under the ensemble $\mathcal{G}$. Finding P^* given this constraint is equivalent to maximising with no constraint the Gibbs entropy under the ensemble $\mathcal{G}_{N,M}$, the space of graphs with M edges and N nodes. It is known that the continuous uniform distribution is the entropy maximising probability distribution under no constraints [35], and therefore

$$P^*(G) = |\mathcal{G}_{N,M}|^{-1} = \binom{\binom{N}{2}}{M}^{-1} \tag{16}$$

[3]The degree sequence of a graph is a monotonic nonincreasing sequence of the degrees of each of its vertices

implying that the Erdős–Rényi model $G(N, M)$ is a microcanonical ensemble given this constraint. We can also show that $G(N, p)$ is a canonical maximum-entropy ensemble under the soft constraint of expected number of edges. Finally, the configuration model can be shown using maximum entropy to be a micro-canonical maximum-entropy ensemble, under the degree sequence constraint. This makes all three models suitable null models for their given constraints.

2.3 Percolation Theory

Consider a magnetic system. It has been shown that an abrupt emergence of spontaneous magnetization occurs below some critical temperature T_C. Additionally, a temperature above this yields a system with misaligned magnetic spins, and thus zero magnetism. Consider also the phase transition from a liquid to a gas. This transition also occurs abruptly beyond some critical temperature, at which point the densities of the liquid and gaseous form are equal. Both systems are examples of *critical phenomena*, where the system changes abruptly due to the variation of some parameter. Percolation theory exists to model these phenomena.

2.3.1 The Infinite Cluster

A question that often occurs when considering regular lattices is whether or not there exists a path that *percolates* the lattice. That is, does there exist a path from the top of the lattice to the bottom? We can model these lattices to have bonds/edges form with probability p, and study how the structure of the lattice varies as we adjust p. For a small value of p, only a small number of bonds will be present, forming small clusters. However, as p reaches some threshold p_c, a percolating cluster suddenly forms, spanning the top and bottom of the lattice. This cluster is known as the infinite cluster.

The process described above is known as bond percolation (or edge percolation). An alternative form of percolation is site percolation (or vertex/node percolation), where sites of the lattice exist with probability p. The infinite cluster emerges for this form too.

2.3.2 Phase Transitions

Consider a d-dimensional lattice with size L^d in the limit[4] of $L \to \infty$, where bonds are formed with probability p. Let $\theta(p)$ denote the probability that an infinite cluster has formed. It can be shown, due to Kolmogorov's zero–one law, that

$$\theta(p) = \begin{cases} 0, & \text{if } p < p_c \\ 1, & \text{if } p \geq p_c \end{cases} \tag{17}$$

which leads very well to the concept of the lattice having phases. The first phase is the subcritical phase ($p < p_c$), this is where the lattice consists of many small

[4]Note that we concern ourselves only with infinite lattices, as percolation occurs for every $p \neq 0$ with non-zero probability in a finite lattice

clusters. The next phase is the critical phase ($p = p_c$), where the infinite cluster has just formed. The final phase ($p > p_c$) is known as the supercritical phase. This is where all finite clusters begin to decay exponentially in size [36].

There are multiple quantities we can use to analyse the properties of these phase transitions. One such quantity is the average finite[5] cluster size $\langle s \rangle$, defined as

$$\langle s \rangle = \frac{\sum_{s<\infty} s^2 n_s(p)}{\sum_{s<\infty} s n_s(p)} \tag{18}$$

where n_s is the density of the system with respect to its size, also referred to as the cluster size distribution. Another popular quantity is the correlation length ξ, defined as

$$\xi^2 = \frac{\sum_{\mathbf{r}} |\mathbf{r}|^2 g(\mathbf{r})}{\sum_{\mathbf{r}} g(\mathbf{r})} \tag{19}$$

where $g(\mathbf{r})$ denotes the probability that a site deviated from an occupied site by the vector $\mathbf{r}$ is located within the same cluster. ξ represents the expected distance between two sites belonging to the same cluster.

Interestingly, it is expected that both quantities diverge like a power law as $p \to p_c$, since it holds that

$$\langle s \rangle \propto |p - p_c|^{-\gamma} \tag{20}$$

$$\xi \propto |p - p_c|^{-\nu} \tag{21}$$

for some $\gamma, \nu \in \mathbb{R}$. These constants are known as *critical exponents*.

2.3.3 Links to Graph Theory

Section 2.2.2 may have already shone light upon the relationship that random graph theory has with percolation, the emergence of an infinite cluster beyond some critical point; the giant cluster that forms in random graphs can be interpreted as the infinite cluster in percolation. In fact, at the critical threshold, the size of the infinite cluster is $N^{2/3}$ [36], in line with the results of Erdős and Rényi [25].

Percolation theory studies finite dimensional infinite lattices. However, random graph theory studies random graphs with N vertices as $N \to \infty$. We can arrange the vertices in a graph to form an N-dimensional lattice, where connected nodes are neighbours [36]. Random graph theory can therefore be considered the study of infinite dimensional lattices.

It is believed - and has been demonstrated by Hara and Slade [37] - that there exists a critical dimension $d_c = 6$ for which the exponents are independent[6] of d for $d > d_c$. Thus it holds that for $d > d_c$, percolation on a d-dimensional lattice is equivalent to infinite dimensional percolation, which indeed demonstrates a duality between percolation and graph theory.

[5] We exclude the infinite cluster as otherwise $\langle s \rangle = \infty$

[6] And therefore possess the same critical exponents as in infinite dimensional percolation

Although there are many parallels between the two theories, the issue with applying percolation theory to real networks is that they are *finite*. This implies that the critical probability p_c is not an exact constant, but rather a region $[p_c - \Delta p_c, p_c + \Delta p_c]$. Kalisky and Cohen [38] showed that the width of this region is inversely proportional to the average length of the infinite cluster, $\Delta p_c \sim 1/N^{\nu_{\text{opt}}}$. Hence, this issue can be alleviated by studying larger networks.

2.3.4 Bounding the Percolation Threshold

An estimate for the critical probability was given by Bollobás *et al.* [39] to be

$$p_c \approx 1/\lambda_A \tag{22}$$

for dense graphs, where λ_A is the leading eigenvalue of its adjacency matrix. However, this estimate is not necessarily close for sparse networks. Karrer, Newman and Zdeborová [40] showed that taking the reciprocal of the largest eigenvalue of the Hashimoto matrix yields a more accurate approximation of p_c for networks, as long as their neighbourhoods are acyclic. For sparse networks that do not possess this property, we instead use this as a lower bound for p_c.

2.4 Markov Chains

We call a set of points a *time-series* if they can be ordered by a singular natural dimension. By writing

$$v_{1:T} \coloneqq v_1, \ldots, v_T \tag{23}$$

and applying the law of total probability we have

$$p(v_{1:T}) = \prod_{t=1}^{T} p(v_t | v_{1:t-1}) \tag{24}$$

It is useful to consider a time-series that exhibits a level of conditional independence, resulting in a model in which we only need a set window n of time to encapsulate all of the required information about our current state:

$$p(v_{1:T}) = \prod_{t=1}^{T} p(v_t | v_{t-n:t-1}) \tag{25}$$

We call such models n^{th}-order Markov chains. Consider a vector of marginals $\pi_i = p(v_t = i)$ for a first-order Markov chain; we call π a stationary distribution on the states if it satisfies

$$\pi = \mathbf{P}\pi \tag{26}$$

where $\mathbf{P}$ is the transition matrix, $\mathbf{P}_{ij} = p(v_{t+1} = i | v_t = j)$ encoding the probability of a transition from state i to j. Markov chains with a nonzero probability of reaching any state beyond some time T_0 (said to be ergodic) will always have a unique stationary distribution.

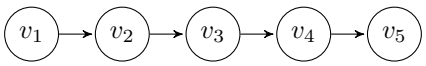


Figure 2: A first-order Markov chain

2.4.1 Total Variation Distance and Mixing Times

Given two probability distributions μ and ν on a sample space Ω, we define the *total variation distance* [41] between them by

$$||\mu - \nu||_{TV} = \max_{A \subset \Omega} |\mu(A) - \nu(A)|, \tag{27}$$

in a less mathematically verbose sense, it is the largest possible difference (or distance) between the probabilities that μ and ν map to an event in their shared sample space. An important result utilizing this tool is that ergodic Markov chains exponentially converge to a stationary distribution, that is, for $\alpha \in (0, 1)$ and $C > 0$

$$d(t) \leq C\alpha^t \tag{28}$$

where

$$d(t) \coloneqq \max_{x \in \Omega} ||P^t(x, \cdot) - \pi||_{TV} \tag{29}$$

This leads very well to the notion of *mixing time*, a measure of the minimum time required for the total variation distance between the distribution of the Markov chain and its stationary distribution to be sufficiently small. We define it by

$$t_{\text{mix}}(\varepsilon) \coloneqq \min\{t \,:\, d(t) \leq \varepsilon\} \tag{30}$$

when sampling from Ω, we wish for $t_{\text{min}} \ll |\Omega|$ so that time is not an impediment to sampling. We call a markov chain *rapidly mixing* [42] if $t_{\text{min}} = \mathcal{O}(S)$, where S denotes the number of possible states. Mixing time is especially important when sampling from a Markov chain, as we wish to sample from the stationary distribution as soon as possible, and sample independently of the initial state. We discuss the implications of this in section 3.8.

2.5 Previous Work

There are two fields that relate to our work, both of which are intertwined: the study of financial systems & systemic risk, and the study of network science. We first review the literature on the former.

The collapse of a financial system can be modelled by the process of leverage cycles, first introduced by Geanakoplos [43]. This model interprets such systems to be oscillatory as a result of the heterogeneous valuation of investors, where increasing leverage enables large asset prices in booming economies. Inversely, asset prices plummet during crises due to collateral constraints imposed upon consumers, resulting in decreasing leverage. Danielsson *et al.* [44] explain that during these crises, investor valuations degenerate into a cynical homogeneous outlook as asset prices begin to correlate.

DebtRank - proposed by Battiston *et al.* [45] - is a centrality measure that can be used recursively to rank institutions by the potential impact their financial distress or default would have on the underlying financial system. Bardoscia *et al.* [46] observed that the original DebtRank algorithm had a tendency to underestimate the effect of financial contagion in some networks, due to its limiting property that institutions can propagate shocks across the network only once. In such cases, a small shock followed by a large shock is much less impactful than the reverse. They thus proposed a more general variant of the algorithm, propagating all shocks it receives. Thurner and Poledna [47] devised a scheme in which the DebtRank of all institutions are visible. They demonstrated that systemic risk is significantly reduced if institutions are incentivized to pritorise institutions with low DebtRank when borrowing; they also showed that trading volumes under their model are not impacted by the introduction of this scheme to the network.

Two main channels through which financial contagion can be spread are overlapping portfolios and counterparty risk (the possibility of an institution defaulting on an obligation to a trade). Contagion spreads through overlapping portfolios when an institution experiences a shock, causing a fire-sale which

drastically devalues its assets. Consequentially, institutions investing in similar (or overlapping) assets experience a shock as the value of their portfolio abruptly diminishes [48]. Caccioli *et al.* [49] studied the Austrian banking system and demonstrated that the interraction of both channels pose a much greater threat to the stability of the system than the existence of a single one. It is not only channels such as these that introduce systemic risk within a financial system, but also its topology. Studies such as [1, 2, 3, 4] demonstrate that dense financial networks exhibit robustness to financial contagion, absorbing the effect of small shocks experienced by single institutions; it is also highlighted that the risk of large shocks being propagated through the network increases as the network becomes more dense. Iazzetta *et al.* [50], Boss *et al.* [27, 51] and De Masi *et al.* [28] displayed the scale-free nature of interbank markets, which Lenzu *et al.* [52] showed theoretically to be less robust to liquidity shocks than Erdős–Rényi topologies. The assortativity of interbank networks has also been of particular interest, as Newman [23] found that disassortative networks are more vulnerable to targeted vertex attack. Consequently cementing the notion that systemic risk resides within interbank networks, Soramäki *et al.* [53] and Bech and Atalay [54] examined the Fedwire payments network and Federal funds network respectively, showing that both are disassortative.

As shown earlier in the report, the study of complex networks beyond those of financial systems has also been of particular interest; the spread of infection through networks is one such area. Sexual contact networks have been studied extensively to understand how sexually transmitted infections spread [55, 56, 57]. In a similar way, the spread of computer viruses (typically through emails) has been studied by Newman *et al.* [58]. The authors demonstrated that email networks are vulnerable to targeted attack and robust to random removal, suggesting that targeted distribution of antivirus software is many times more effective than random distribution. Both networks have been shown to be scale-free [57, 58]. The SIR model of epidemic disease [59] models a population using three classes, susceptible, infected, and recovered. Grassberger [60] displayed the duality between the SIR model and the problem of bond percolation over networks, where the probability of infection being spread between two parties directly maps to the probability of a bond forming between two sites. A probability above the critical threshold under this representation yields a system where an epidemic is possible. Other social networks have also been studied, including actor collaboration [61] and paper coauthorship [62] networks. Networks such as these demonstrate what is known as the 'small-world' property - first discussed by Milgram [63] - where the size of networks are significantly larger than the average distance between their nodes. [36, 61, 62, 64].

Networks encapsulating the information stored within a system are known as information networks. Redner [65] studied the degree distribution and its evolution over time in a network formed by paper citations, finding that they exhibit a power-law distribution which slowly diminishes over time. Broder *et al.* [9] studied the structure of the WWW, showing that its in and out-degree distributions have power-law tails with $\gamma_{in} = 2.1$ and $\gamma_{out} = 2.72$; the vulnerability of the network when targeting the most connected nodes was highlighted,

as only a small fraction of nodes needed to be removed in order to break the network (similar results were also found by Albert *et al.* [66]). An interesting finding was that the network is comprised of four distinct structures, which was then found in other real networks [58]. Saxena *et al.* [10] released the Rabobank transactions dataset and used it to perform a series of statistical analyses on the corresponding network, drawing parallels between other scale-free networks, but acknowledging that some common features (such as a clear in vs. out-degree/strength correlation) are not present. They also examined the community structure of the network, discovering some essence of determinism in the evolution of the network. However, a minor issue with their dataset is described and resolved in section 3.2.

Biological systems have also been studied from a network perspective. Watts and Strogatz [61] looked at the neural network of the *caenorhabditis elegans* nematode worm, showing that the network has a much higher clustering coefficient than similar random networks. Jeong *et al.* [7] studied metabolic pathway networks for multiple organisms, showing that the distribution of substrate reaction involvement follows a power-law, and thus demonstrating that these networks are scale-free. Like other scale-free networks, the robustness of the metabolic pathways to random attack (or mutation in this context) was made evident. Solé and Montoya [67] analysed the effect of random and targeted species removal on three popular food webs; they found that the majority of the networks are scale-free and thus robust (vulnerable) to random (selective) extinction.

Finally, technological networks - man-made networks used to distribute some resource - are of great interest to researchers. Onnela *et al.* [8] analysed the characteristics of a network constructed from phone call records, demonstrating its assortative behaviour and the relationship between overlap, strength, and betweenness of links; the authors also explored the robustness of the network to link removal based on the three quantities, showing that targeting links with the highest betweenness was the most effective strategy. Watts and Strogatz [61] investigated the statistical properties of the western United States power grid, finding that it has a large clustering coefficient relative to other random networks. Chen *et al.* [68] constructed a network from the Internet at the Autonomous System (AS) level, refining the results from Faloutsos *et al.* [69] and showing evidence that the Internet does not exhibit a strict power-law degree distribution.

3 Methodology

3.1 The Rabobank Transactions Dataset

In our experiments we use the Rabobank Transactions Dataset, available in the GitHub repository https://github.com/akratiiet/RaboBank_Dataset. The Dataset is in CSV format, separated using semicolon ';' delimiters. Each row represents an aggregate transaction over some time period, and has 6 columns (`start_id`, `total`, `count`, `year_from`, `year_to`, `end_id`). `start_id` and `end_id` denote unique identifiers for accounts that initiate and receive the transaction respectively. `total` denotes an aggregate sum over the amount sent from `start_id` to `end_id`, similarly, `count` denotes an aggregate count of transactions. Finally, `year_from` and `year_to` represent the year of the earliest and latest transaction respectively from `start_id` to `end_id`.

3.2 Dataset Cleaning

Exploring the dataset, we found that some (`start_id`, `end_id`) pairs occurred in multiple rows, resulting in a network with parallel edges. This does not make sense, as the dataset contains aggregate transactions, yet the existence of duplicate (`start_id`, `end_id`) pairs contradicts this. To resolve this, we grouped the dataset by each (`start_id`, `end_id`) pair, aggregating duplicates by summing `count` and `total`, and taking the minimum and maximum of `year_from` and `year_to` respectively. We saved the updated dataset to a new CSV file, yielding a network without parallel edges.

3.3 Network Construction

We construct a network basing its topology on the `start_id` and `end_id` columns. We create nodes from each identifier, and form a directed link from `start_id` to `end_id` for each row. We additionally assign two weights to each link, corresponding to its `total` and `count`. In this report, we ignore the temporal data for each transaction as it does not contribute to the characteristics and topology of the overall underlying network of interest.

The cleaned dataset consists of 3823167 rows and 1624030 unique identifiers, corresponding to a network with 1624030 nodes and 3823167 links. We take the largest weakly connected component (LWCC) of this network, with 1622173 nodes and 3821514 links. We performed the remainder of our study on this component, as the other components had at most 27 nodes, a negligible size relative to the LWCC. Additionally, using the LWCC ties well to the idea of the infinite cluster, which benefits our percolation experiments.

3.4 Exploiting Network Sparsity

The large scale of our network has many implications, the main issue is that storing matrices has a $\mathcal{O}(n^2)$ space complexity. There are 1622173 nodes, resulting in a 1622173×1622173 adjacency matrix; assuming that 32 bits are allocated in memory for each integer in the matrix, this means we must allocate at least 10TB of memory[7]. Even worse, the non-backtracking matrix is a 7643028×7643028 matrix. Consequentially, it is computationally infeasible to store and utilize these matrices through this naive method.

However, note that our network is *sparse*, possessing significantly less links than its maximum ${}^{1622173}C_2$. We can exploit this fact when working with these matrices, by storing them in a data structure known as a compressed sparse row (CSR) matrix. CSR matrices comprise three one-dimensional arrays, respectively storing *nonzero* values alongside their row, and column indices. The row index array additionally stores a final element denoting the number of nonzero values. For instance, we can represent the matrix

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 3 & 4 & 0 & 0 \end{pmatrix}$$

as the following CSR matrix

$$\begin{aligned} \text{VALUES} &= [1, 3, 4] \\ \text{COLS} &= [3, 0, 1] \\ \text{ROWS} &= [0, 3, 3, 3] \end{aligned}$$

which evidently scales very well as the matrix size increases, as long as it is sparse.

Additionally, it is not the non-backtracking matrix B itself that we are seeking, but rather its spectrum. Krzakala *et al.* [70] showed that the eigenvalues of

$$B' = \begin{pmatrix} \mathbf{0} & D - \mathbb{I} \\ -\mathbb{I} & A \end{pmatrix}$$

are always eigenvalues of B, where $\mathbf{0}$ is the $|V| \times |V|$ zero matrix, and D and A are the degree and adjacency matrices respectively. B' is a $2|V| \times 2|V|$ matrix, and thus is a more compact version of B, saving even more memory, especially in CSR format.

3.5 Computing and Estimating Centrality Measures

Given the size of our network, it may be computationally infeasible to compute centralities exactly. Consider computing the betweenness centrality for each node in the network: To do so, we must compute the geodesic paths for each

[7] Even implementing it as a matrix of bits is computationally infeasible, requiring 329GB

pair of vertices. A naive implementation would have a $\mathcal{O}(|V|^3)$ and $\mathcal{O}(|V|^2)$ time and space complexity respectively. We can improve upon this by utilizing Brandes [71] algorithm, which has a $\mathcal{O}(|V||E| + |V|^2 \log |V|)$ and $\mathcal{O}(|V||E|)$ respective time and space complexity, but for large $|V|$ and $|E|$ even this algorithm is infeasible. Consider also the problem of computing closeness centralities. This requires the distances between each pair of nodes to be computed, which - in a naive implementation - requires us to perform breadth first traversal for each node. Hence, this algorithm has a $\mathcal{O}(|V||E|)$ time complexity.

Therefore, we must resort to estimation. For betweenness, we follow the approach proposed by Brandes and Pich [72], randomly sampling a set S of pivot nodes without replacement and computing

$$\hat{b}_v = \frac{|V|}{|S|} \sum_{s \in S} \sum_{t \neq v,s} \frac{\sigma(s,t|v)}{\sigma(s,t)} \tag{31}$$

which we do using Brandes algorithm. Brandes and Pich showed that by sampling uniformly without replacement, $\hat{b}_v$ becomes an unbiased estimator of b_v, where its variance is a function of $|S|$. With that in mind, we chose $|S|$ to be as large as possible without impeding heavily on runtime. We estimate closeness centrality using the algorithm proposed by Cohen *et al.* [73], which in a similar fashion to Brandes and Pich, uses randomly sampled pivots to obtain an unbiased estimate of closeness.

To compute the eigenvector centrality for each node, we performed power iteration on the adjacency matrix A of our network to approximate the principal eigenvector $\mathbf{v}$. That is, given an initial nonzero estimate $\mathbf{v}_0$, we recursively compute

$$\mathbf{v}_{k+1} = A\mathbf{v}_k \tag{32}$$

and stop on convergence. To ensure that the algorithm does not run for an unreasonable time, we say the sequence $(\mathbf{v}_n)$ has converged at $n = N$ if

$$\sum_i |(\mathbf{v}_N - \mathbf{v}_{N-1})_i| < \epsilon \tag{33}$$

for some parameter ϵ which we set to $1\mathrm{e}-6$. PageRank is computed in a similar way, iterating its recursive equation until convergence.

3.6 Performing and Evaluating Percolation

In this subsection, we describe the techniques and strategies used to attack our network, alongside the methods we use to evaluate the effectiveness of each attack.

3.6.1 Vertex Attack Strategies

When performing targeted attack on a network, we aim to break the network by removing the most important nodes. Attacking nodes in descending order of

centrality therefore aligns very well with this goal, as the centrality of a node is a measure of importance. Additionally, we wish to study the networks robustness to random error, so we also perform the attack strategy of random removal. To summarise, we perform the following node attacks:

- Random node removal
- Removing nodes in descending order of degree centrality
- Removing nodes in descending order of betweenness centrality
- Removing nodes in descending order of eigenvector centrality
- Removing nodes in descending order of closeness centrality
- Removing nodes in descending order of PageRank centrality

3.6.2 Edge Attack Strategies

Our network is weighted, and thus we can dedicate a portion of edge attack strategies to edge weight. This yields three strategies: Strongest link first, weakest link first, and average-strength first. Strongest and weakest link first attacks are where we target edges in descending and ascending order of weight respectively. Average-strength first is where we target edges with weight closest to the average first.

Additionally, we attempt to rank edges based on their source and target nodes. The first of these attacks ranks each edge (i, j) by $C(i)C(j)$ where $C(\cdot)$ is a centrality measure. We consider this strategy because a link having a high rank implies it is connected to at least one important node, so the link may be key to the flow of information across the network.

We also propose a class of edge attacks, ranking edges by the (dis)similarity of their source and target nodes according to some centrality measure, by constructing the similarity score

$$S((i,j)) = e^{-\beta(C(i)-C(j))^2} \tag{34}$$

where β is a parameter. Edges with source and target nodes of similar centrality will have a similarity score close to 1, while dissimilar centralities yield a similarity score of 0. Note that S is monotonic, and thus β is pointless in theory. However, we introduced it to control how S handles underflow, since a smaller β results in larger $S((i,j))$. We perform this attack strategy to study the impact the existence of (dis)similar nodes has on the information flow within our network.

3.6.3 Executing Attack Strategies

Our network consists of one weakly connected component. As mentioned earlier, we consider this to resemble the infinite cluster encountered in percolation. Thus we can take the approach of removing a fraction p of nodes or links from the

network then recording $\langle s \rangle$ and the size of the LWCC at that point. Although our network is finite, we ignore the largest component of our network when computing $\langle s \rangle$ as the largest component is assumed to be the infinite cluster under our model. Once we have reached the critical point p_c of the network under that strategy, a phase transition will occur and the network will fragment into many isolated clusters. This process is identical to graph evolution, except we remove nodes/links rather than add them.

After the attack has terminated, we plot the LWCC size and $\langle s \rangle$ against p. This will allow us to analyse and evaluate the attack, as we will discuss in the next subsection.

3.6.4 Measuring Strategy Effectiveness

The plots obtained through each attack provides a quantitative measure of its effectiveness. When inspecting the LWCC plot, we can estimate the region of p that the phase transition occurred by inspection, determining the first point where the plot experiences a permanent change in gradient. By (20) we know that $\langle s \rangle$ diverges as $p \to p_c$, hence, we can also estimate the critical point through the peak of our $\langle s \rangle$ plot. We also take an exact approach, finding the R-index [74] of each attack:

$$R_v = \frac{1}{|V|} \sum_{i=1}^{|V|} s(p_i) \tag{35}$$

$$R_e = \frac{1}{|E|} \sum_{i=1}^{|E|} s(p_i) \tag{36}$$

where $s(p_i)$ denotes the size of the LWCC upon removing a proportion p_i of nodes/links. A high R-index implies resilience to the attack, and a low R-index implies vulnerability. We can interpret the R-index as an approximate area under the LWCC plot, i.e.

$$R \approx \int_0^1 s(p) dp \tag{37}$$

Evaluating attacks in this manner allows us to measure the robustness of our network against attacks not only by considering the critical region at which abrupt collapse occurs, but also by the damage the network receives elsewhere.

3.7 Choosing a Configuration Model

In order for our configuration model to be a suitable null model, we need to consider the properties of our intra-bank network. The characteristics of our configuration model will ultimately dictate the structure and dynamics of the empirical networks we generate. The graph space we work in will also influence the way we sample, reinforcing the necessity of choosing the correct one [75]. Our task in this subsection is therefore to choose a graph space for our null

model. Fosdick *et al.* [75] introduced three questions we can use to guide our decision:

Question 1: "Are there self-loops in the graph?" A graph (V, E) contains a self-loop if there exists a vertex $i \in V$ such that $(i, i) \in E$. To perform this check, we checked each vertex for a self-loop, and found none. This is intuitive, it makes no sense for a user to perform a transaction with themselves, and if they do, there is no net change in the flow of securities within the underlying transactions network, so it can be ignored. Therefore, our desired graph space does not include self-loops.

Question 2: "Are there multiedges in the graph?" Multiedges are also known as *parallel edges*, that is, there exists some nodes $i, j \in V$ such that $(i, j), (i, j)' \in E$ and $(i, j) \neq (i, j)'$. In section 3.2, we explained the issue with multiedges in our network, and described the process of removing them entirely. Thus our network has no multiedges. Therefore, our desired graph space does not include multiedges either.

Question 3: "Is the graph space stub-labeled or vertex-labeled?" A stub-labeled graph is one in which each of its stubs (also known as half-edges) can be uniquely labeled. This means that edges correspond to a pair of stub labels. A vertex-labeled graph is one where each vertex is uniquely identified by a label. The main difference between the two is that vertex-labeled graphs have a unique adjacency matrix, while stub-labeled graphs do not. Our answers to question 1 and 2 implicitly yield a solution. Our graph space is *simple* (has no loops or multiedges), so in the context of sampling from a configuration model, there is no difference between sampling from either graph space.

To summarise, the configuration model we will use for our experiments will sample from the graph space of simple graphs. Indeed, our network belongs within this space, so our configuration model is a suitable null model.

3.8 Sampling from a Configuration Model

We can sample graphs from a configuration model, using our network as a starting point. We make use of a technique known as the double edge swap [76, 77], where edges $(u, v), (x, y) \rightsquigarrow (u, y), (x, v)$. The process of repeated random double edge swaps on a graph is a Markov process, so we can sample graphs by taking a random walk on the corresponding Markov chain. This is equivalent to using a Markov chain Monte Carlo (MCMC) sampler on double edge swaps. To ensure that the sampled graph does not deviate from our desired simple graph space, we verify after each swap that we are in the same space, and resample the current graph if not.

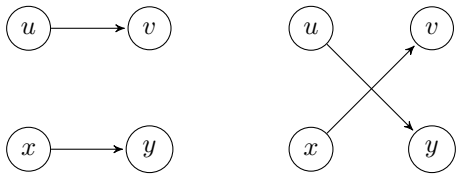


Figure 3: An illustration of the double edge swap $(u, v), (x, y) \rightsquigarrow (u, y), (x, v)$. To the left is the original graph, to the right is the graph after the swap has been performed.

The main underlying issue with this approach is that the probability distribution over our graph space will be dependent on our network if the number of transitions taken is sufficiently small. It can be shown that the Markov chains with transition probabilities given by the MCMC algorithms are ergodic with a uniform stationary distriution [75], implying that after a certain number of double edge swaps, we will be sampling uniformly from our simple graph space. Concerns about the mixing time of such chains therefore arise. How many swaps must we perform to ensure that we reach the mixing time? The KTV conjecture [76] states that double edge swap Markov chains are rapidly mixing for all degree sequences over a simple graph space. Additionally, Erdős, Greenhill, Mezei *et al.* [78] showed that these Markov chains are rapidly mixing on "P-stable unconstrained, bipartite, and directed degree sequence classes.". Let $G(\mathbf{d})$ denote the set of graphs with degree sequence $\mathbf{d}$. We say the set $\mathcal{D}$ of degree sequences is P-stable if, for all $\mathbf{d} \in \mathcal{D}$ we have that

$$\left| G(\mathbf{d}) \cup \left(\bigcup_{x,y \in [n],\, x \neq y} G(\mathbf{d} + \mathbb{1}_x + \mathbb{1}_y) \right) \right| = \mathcal{O}(p(n)) \tag{38}$$

where $p(\cdot)$ is some polynomial function, n is the number of vertices in the degree sequence, $[n] \coloneqq \{1, \ldots, n\}$, and $[\mathbb{1}_k]_i = \delta_{ik}$.

The guarantee of rapid mixing in our MCMC sampling algorithms implies a polynomial bound in $|V|$ for the mixing time. This *does not*, however, guarantee that the mixing time is small. While there is no method to our knowledge to measure/estimate the mixing time, we take the approach of performing sweeps over each edge, ensuring that swaps have been performed for every edge at least once. We additionally perform this operation twice to further reduce the total variation distance between our transition probability distribution and the stationary probability distribution.

3.9 Using the Configuration Model as a Null Model

We will use our configuration model to compare the topological properties of our network with random graphs. We wish to investigate various properties of our sampled graphs, including transitivity, assortativity, R-index, and a measure of its scale-free property (we will use the γ exponent). We sample 100 graphs and obtain these properties for each of them. By acquiring R-indices for each sampled graph, we learn whether the robustness of our intra-bank network is likely a that cannot be explained purely by its degree sequence, or a property shared by many graphs in our graph space. We can then use the other properties to reason about why that is the case.

In order to reason about our data, and perform statistical hypothesis tests using it, we need knowledge regarding its distribution. It may be the case that these properties are not distributed according to common ones such as the Gaussian distribution, so we take a nonparametric approach to estimating the probability distribution P of the data, fitting a distribution to our data without any prior information about the one it was originally sampled from. We use the technique of Kernel Density Estimation [79], where given a set of datapoints $(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_m)$, we estimate P as

$$\hat{P}(x) = \frac{1}{mh} \sum_{i=1}^{m} K\left(\frac{x - x_i}{h}\right) \tag{39}$$

where $K(\cdot)$ is a positive function known as a *kernel*, and h is referred to as the bandwidth, a parameter controlling the smoothness of $\hat{P}$. We will use the Gaussian kernel

$$K(x) \propto \exp\left(-\frac{x^2}{2h^2}\right) \tag{40}$$

If the hypothesis of normality is not rejected (which we will test using the Anderson-Darling test [80]), then it is optimal [79] to use the bandwidth

$$h = (4/3)^{1/5} \hat{\sigma} m^{-1/5} \tag{41}$$

where $\hat{\sigma}$ is the empirical standard deviation. If the hypothesis is rejected, we will select h using cross-validation.

Working with our intrabank network $\hat{G}$, a general framework of the approach we will take for each property $\mathcal{P}$ is as follows: Let the null hypothesis $H_{0,\mathcal{P}}$ be that $\mathcal{P}(\hat{G})$ can be explained by its degree sequence. Next, we create an alternate hypothesis $H_{1,\mathcal{P}}$. We then fit a kernel density estimator to our data, which we use to compute a p-value. Finally, we use the p-value to either reject $H_{0,\mathcal{P}}$ or conclude that it cannot be rejected.

We additionally perform the two-sample Kolmogorov-Smirnov test to compare the robustness of our network and random networks to random attack. We record two samples each with 100 observations, corresponding to the R-indices of random networks and our real network. We then take an unbiased estimate

of their cumulative distribution functions

$$F(x) \approx \frac{1}{100} \sum_{i=1}^{100} \mathbb{I}[X_i < x] \tag{42}$$

where X_i is an observation in the sample, and $\mathbb{I}$ is the indicator function. We use these to compute the test statistic

$$D = \sup_x |F_{\text{real}}(x) - F_{\text{random}}(x)| \tag{43}$$

allowing us to test the likelihood that both samples were drawn from the same distribution, which would imply that our network is as robust to random error as random networks sampled from our configuration model. We can also use it to test whether a distribution is greater/less than another.

3.10 Tools for Network Analysis

Three toolkits were used in this report, namely NetworkX, NetworKit, and graph-tool. NetworkX is a popular toolkit for network analysis, but due to its pure Python implementation it is more suitable for small to medium sized networks. However, its ease of use made it a good choice for our preliminary analysis; it additionally allows us to load graphs through adajcency matrices, which helped us overcome memory issues encountered by other toolkits.

Unlike NetworkX, graph-tool and NetworKit use a `C++` backbone to enhance performance, making both of them suitable for our network. We found that graph-tool yields the best performance on percolation studies by a large margin, with the downfall that it does not provide an interface through which we can approximate closeness centralities, we therefore used NetworKit to remedy this.

4 Results

We now begin our study of the robustness of the Rabobank Intrabank network. We first analyse the impact of vertex removal on the network, then proceed to edge removal. In both studies we perform a comparison with networks sampled from a configuration model. Finally, we analyse some of the topological properties of the network relative to random networks, which will yield further insights into the behaviour of buyers and sellers within the network.

4.1 Vertex Attacks

Figure 4 demonstrates the damage each vertex attack inflicts on the network, where the x and y axes denote the fraction of vertices removed and the normalised largest component size respectively. We additionally plot the average outcome of vertex attacks performed on networks sampled from a configuration model (in the rest of the report we shall refer to these as random networks). We provide the R-Index of each attack in Table 1, and plot the effect of each attack on the average finite cluster size in Figure 5.

As similarly demonstrated by many other scale-free networks, we observe a significant robustness to random error, with a critical probability close to 1. We additionally see that this property is shared with random networks; performing a Kolmogorov–Smirnov test on the samples of R-Indices taken from 100 runs of random attacks for both random networks and our network yielded a p-value of 0.97, implying that we cannot reject the hypothesis of the robustness of our network to random error being distributed likewise to random networks. It is therefore possible that the robustness of our network to random error can be explained by its degree sequence.

Another similarity is that the network is prone to targeted vertex attack, in which case a phase transition occurs after removing only a small proportion of nodes. We highlight that, interestingly, removing vertices in descending order of degree centrality - a local centrality measure - is the most effective strategy we have found to disconnect the network, boasting the lowest R-index and critical probability. Therefore, the direct transactions performed by users may convey enough information to measure their importance to the flow of securities within the network; considering transactions they are not directly involved with (i.e. using global information) appears to diminish the importance of more influential users within the network, prioritising less influential users for removal instead. Ranking performance by R-index, we see that PageRank centrality attacks perform second best, followed by betweenness, eigenvector, closeness, and finally random attacks. A possible explanation for degree centrality attacks being the most effective is that the removal of a highly influential user based on a global measure perturbs the ranking of users to a greater extent than removing users based on local measures such as degree. Note that the betweenness and closeness centralities are estimates and thus extra uncertainty has been introduced to their corresponding R-indices.

One additional result is that random networks are likely more robust to most

targeted attacks. Under the alternate hypothesis that the R-index computed from the network according to some attack is less than the R-index computed from almost every random network according to the same attack, we acquired p-values close to zero for all targeted attacks except eigenvector. Similarly, we found strong evidence that the network is more robust to eigenvector attacks than random networks. We can thus reject the hypothesis that the robustness of the intrabank network to targeted vertex attacks is unable to be explained purely by its degree sequence.

The majority of our claims are reinforced in Figure 5, showing that the critical probability p_c of our network when under degree centrality attack ($p_c \approx 0.016$) is lower than every other attack, followed by betweenness & PageRank ($p_c \approx 0.020$), eigenvector ($p_c \approx 0.30$), closeness ($p_c \approx 0.68$) and finally random ($p_c \approx 0.95$). Additionally, the figures provide evidence that random networks possess a larger critical probability under all[8] attacks except eigenvector, which correlates with our findings with their R-indices.

Table 1: R-Indices for each vertex attack strategy[9]. Removing nodes in descending order of degree centrality breaks the network fastest, followed by betweenness, PageRank, eigenvector, closeness, and finally random. The intrabank network appears to be less robust to node removal than random networks, with only eigenvector and random attacks possessing a lower and approximately equal average R-index respectively.

Strategy	**Real Network**	**Random Network Avg**
Degree	0.00507	0.00834 ± 0.00001
Betweenness	0.0082	0.0227 ± 0.0003
PageRank	0.0064	0.0106 ± 0.0001
Eigenvector	0.0288	0.0145 ± 0.0002
Closeness	0.0457	0.1082 ± 0.0005
Random	0.360 ± 0.002	0.360 ± 0.002

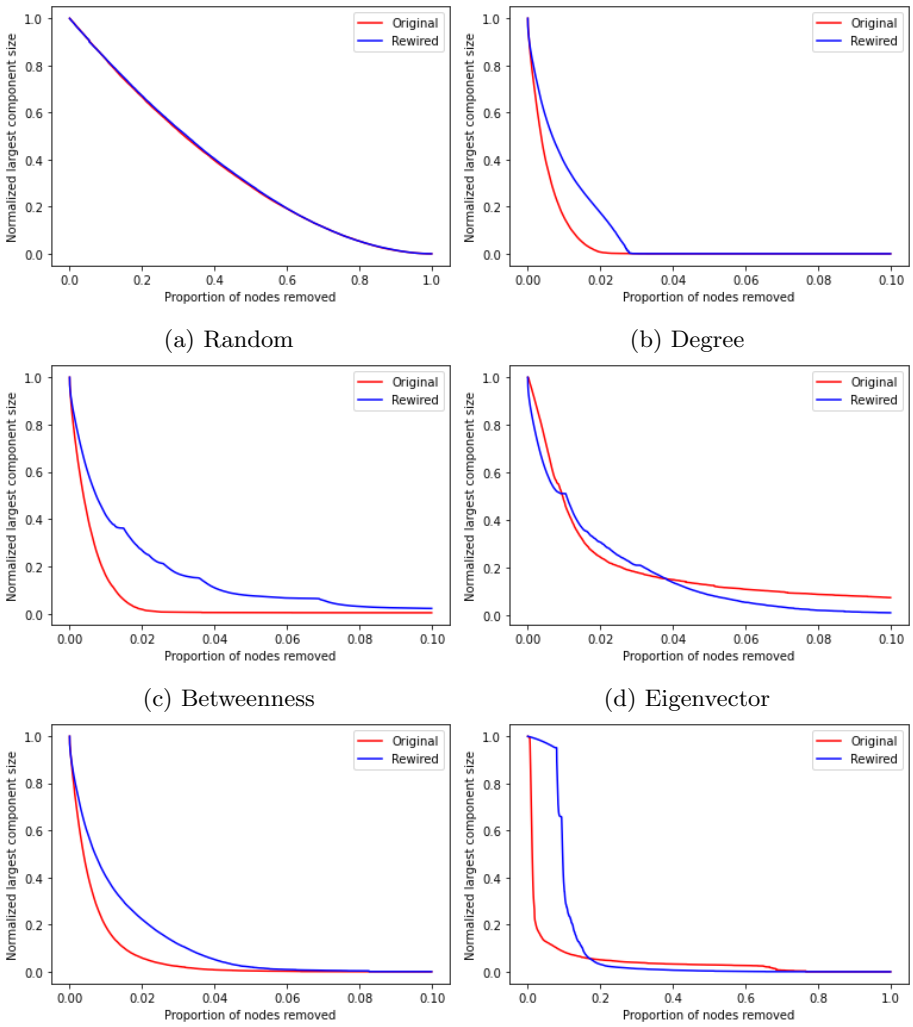
4.2 Edge Attacks

Figure 7 demonstrates the damage each edge attack inflicts on the network, alongside the average outcome of vertex attacks performed on networks sampled from a configuration model. We provide the R-Index of each attack in Table 2.

One of the most peculiar results is that the intrabank network is incredibly robust to edge removal, where most of our strategies incur a phase transition near $p_c \approx 1$. This included every strategy concerned with the weights of each edge; we see that strongest and closest-to-average (total) link attacks performed

[8] We exclude betweenness and closeness here, attributing the undiscernible nature of p_c from the betweenness and closeness attacks to the fact that both measures were approximated.

[9] The uncertainty in each measurement corresponds to a single standard deviation



(a) Random

(b) Degree

(c) Betweenness

(d) Eigenvector

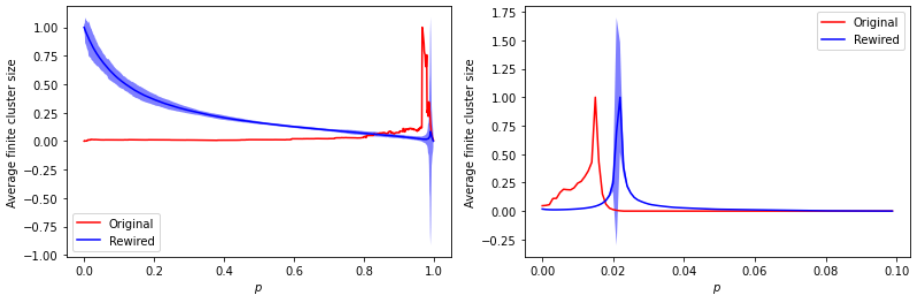
(e) PageRank

(f) Closeness

Figure 4: Robustness of the network to vertex attack strategies[10], we plot the normalized largest component size as a function of the proportion of nodes removed. For random networks, we took the average across 100 attacks on networks sampled from a configuration model.

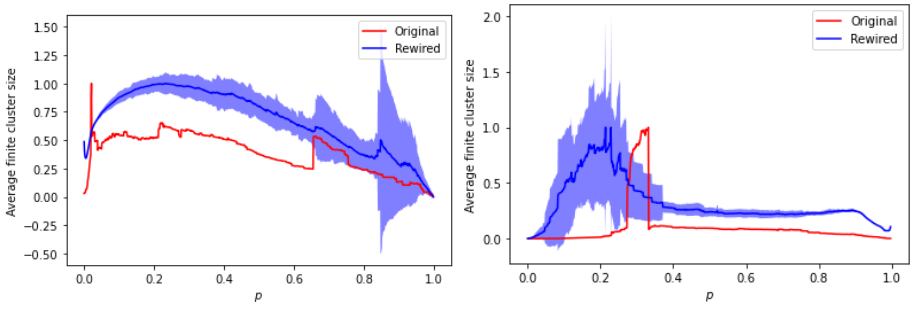
worse than random link attacks, with weakest and furthest-from-average link attacks performing slightly better. Consequentially, the transactions with the least weight have slightly more influence on the flow of securities within the network than the transactions with the most weight.

[10]In all plots, we include shaded error bars corresponding to two standard deviations, in



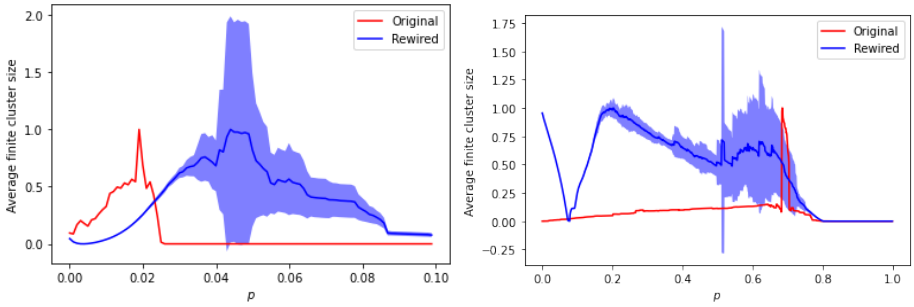
(a) Random

(b) Degree



(c) Betweenness

(d) Eigenvector



(e) PageRank

(f) Closeness

Figure 5: Average finite cluster sizes of the intrabank network (in red) and random networks (in blue) as a function of the proportion of edges removed. A peak indicates a phase transition occurring at that point. For most attack strategies, phase transitions occur later on average for random networks, implying that it takes less node removals to break the intrabank network into small clusters than it does for random networks. Betweenness and closeness measures introduce additional uncertainty as they are approximated, which hinders our ability to discern where the phase transition occurs.

this plot and its edge counterpart, however, they are unnoticeable

It is also evident that attacks based on the count of a transaction (the number of transactions from one user to another) bear a similar shape to its total (the total amount sent from one user to another) counterpart, albeit less smooth. We found that counts and totals of each transaction are correlated, with a Spearman's rank correlation coefficient of 0.73 (see Figure 6). Indeed, this is intuitive: we expect the total amount of money sent over a series of transactions to increase alongside the total number of transactions. A perhaps less intuitive finding is that all count-based attacks perform better than their total counterparts, implying that the number of transactions between two users is more important to the structure of the network than the total amount sent between them.

An additional result is that edges formed between similar and dissimilar vertices do not exude any significant influence over the network, but edges joining dissimilar vertices are - to some degree - more important than those connecting similar ones. Thus, transactions executed between two users who respectively perform large and small amounts of transactions are more important to the structure of the network than those executed between users who have performed similar amounts.

The only strategy we have considered that exhibits a clear phase transition after removing a small fraction of edges is the degree centrality product attack, possessing a lower R-index than any other edge attack, and being the only such attack that has a lower R-index than random vertex removal. This result indicates that transactions performed between users of high influence are of somewhat high importance themselves. It is likely that the similarity attack does not perform as well due to the additional presence of low influence pairs.

Contrasting our results with vertex attacks, it is evident that random networks are in most cases more *vulnerable* than the intrabank network. Under the alternate hypothesis that the distribution of R-indices from random attacks on our network is greater than that from random networks, we performed a Kolmogorov–Smirnov test on samples of R-Indices taken from 100 runs of random edge attacks for both random networks and our network. This yielded a p-value of 1.0 and thus there is strong evidence that the intrabank network is more robust to random edge error than random networks. Additionally, under the alternate hypothesis that the R-index from attacks on the intrabank network exceeds those computed from random networks, we obtained p-values close to zero for all attacks excluding dissimilarity and degree product.

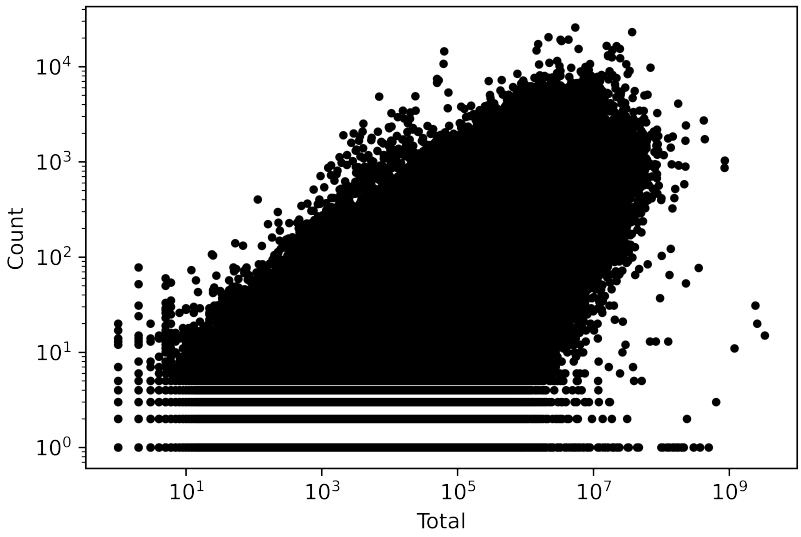
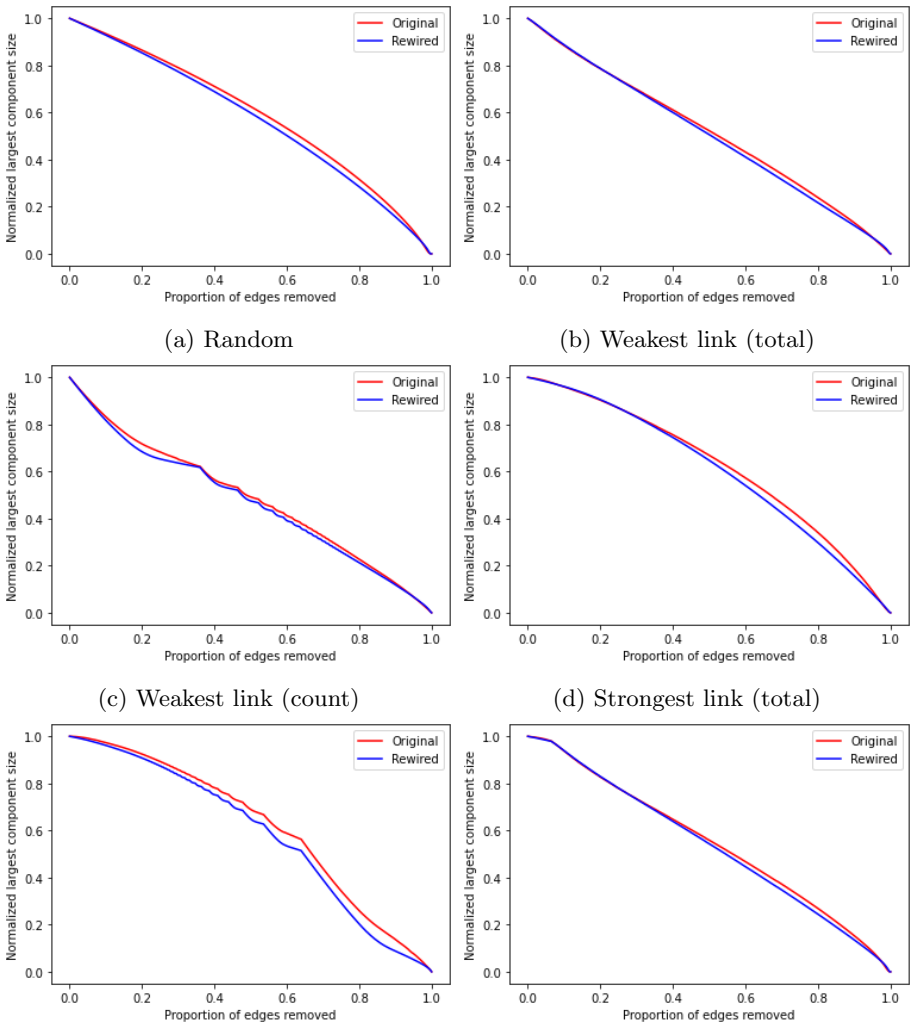


Figure 6: Correlation of edge weights total and count, with a Spearman's rank correlation coefficient of 0.73.

Table 2: R-Indices for each edge attack strategy, in ascending order of real network R-index. Removing nodes in descending order of degree centrality product is the most effective strategy regarding R-index, followed by weakest link, similarity, dissimilarity, average link (count), random, average link (total) and finally strongest link. The intrabank network appears to be more robust to edge removal than random networks, and more vulnerable to count-based attacks than total-based attacks.

Strategy	**Real Network**	**Random Network Avg**
Degree Centrality Product	0.3124	0.3206 ± 0.0001
Weakest Link (Count)	0.4862	0.4714 ± 0.0001
Weakest Link (Total)	0.5146	0.5046 ± 0.0001
Similarity	0.5449	0.5510 ± 0.0001
Dissimilarity	0.5633	0.5399 ± 0.0002
Average Link (Count)	0.5724	0.5456 ± 0.0001
Random	0.5784 ± 0.0002	0.5580 ± 0.0002
Average Link (Total)	0.6054	0.5828 ± 0.0001
Strongest Link (Count)	0.6178	0.5848 ± 0.0001
Strongest Link (Total)	0.6198	0.6017 ± 0.0002



(a) Random

(b) Weakest link (total)

(c) Weakest link (count)

(d) Strongest link (total)

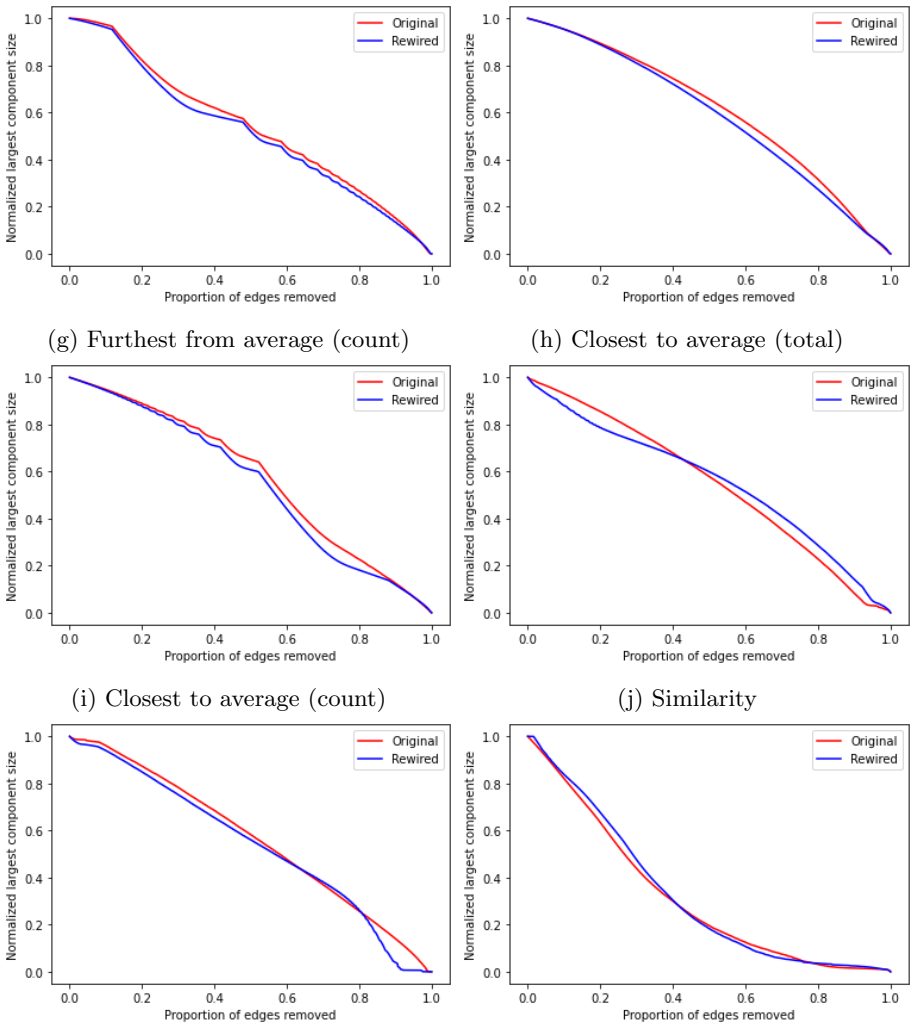
(e) Strongest link (count)

(f) Furthest from average (total)

4.3 Graph Measures

We now begin our study of a subset of measures of our network and their random counterparts, investigating how the analytical critical probability lower bound and topological properties of the intrabank network varies to those of random networks.

Table 3 shows the degree assortativities, transitivities, and p_c lower bounds for the Rabobank network. We also include the corresponding random network average for comparison. Observing the low transitivity of the network, we can see that cliques between users appear remarkably infrequently, to the extent that random networks are approximately five times as transitive. Another interest-



(g) Furthest from average (count)

(h) Closest to average (total)

(i) Closest to average (count)

(j) Similarity

(k) Dissimilarity

(l) Degree Centrality Product

Figure 7: Robustness of the intrabank network (in red) and random networks (in blue) to edge attack strategies, we plot the normalized largest component size as a function of the proportion of edges removed. For random networks, we took the average across 100 attacks on networks sampled from a configuration model.

ing finding is that the network exhibits significantly less disassortative mixing than interbank networks, i.e. users frequently involved in transactions have a very small tendency to perform ones with those who are rarely involved. It is also apparent that random networks are significantly less disassortative than

the Rabobank network, further cementing the notion that the topology of the Rabobank network is not fully explainable by its degree sequence. This contrast in assortativity can help explain why the robustness of the intrabank network differs from random networks: since the degree sequence is preserved, a higher disassortativity implies that the hubs residing in the network are less likely to be neighbours, increasing the likelihood of a larger number of nodes being disconnected from the network after removing a hub. Conversely, a larger transitivity implies that the network uses up more edges to form triangles, rather than building up a larger giant component. This property makes it easier to disconnect the network, and therefore makes the network less robust to targeted attack. Hence, for targeted vertex attacks, it is clear that the effect that an increased disassortativity imposes over the intrabank network outweighs the effect of its lower transitivity. Likewise, for edge attacks, the effect of decreased transitivity outweighs that of increased disassortativity.

Overall, we can see that the analytical lower bound of the critical probability p_c of the intrabank network is slightly lower than that of random networks. Consequently, *in the worst case*, the Rabobank intrabank network is less robust than random networks sharing the same degree sequence. These results complement the previous ones excellently, demonstrating that not only is the robustness of the intrabank network a property likely unique to itself, but also its underlying structure and topology.

Table 3: Statistics for the intrabank network and the corresponding average from random networks. While the intrabank network possesses a very small disassortativity compared to interbank networks, it is noticably larger in magnitude than random networks. However, random networks are five times more transitive than the intrabank network. It is evident that the network has a smaller lower bound for the critical probability p_c than random networks.

	Real Network	**Random Network Avg**
Degree Assortativity	-0.02339	-0.00031 ± 0.00007
In-Degree Assortativity	-0.01457	-0.00021 ± 0.00007
Out-Degree Assortativity	-0.02239	-0.00030 ± 0.00008
Transitivity	0.00117	0.00494 ± 0.00002
p_c Lower Bound	0.01047	0.01266 ± 0.00003

5 Conclusion and Future Work

In this report we analysed the robustness of the Rabobank intrabank network to the removal of its components, specifically, we investigated how the underlying structure of the network changes as a consequence of node and link removal. Our results provided evidence that removing users in descending order of degree (the number of transactions they have been involved in) is among the most effective methods of breaking the network, suggesting that degree centrality is a useful measure of the influence a user has on the overall structure and connectivity of the network. However, it is necessary to highlight a major caveat with our results, which is that the closeness and betweenness centrality measures were estimated due to the large scale of the network and thus may have led to inaccurate results. We also showed strong evidence of the network being more susceptible to targeted and random attack than networks sampled from a suitable configuration model, with most attack strategies yielding a lower R-index and critical probability.

Our results are significantly different for edge attacks, however. We found that the network is significantly more robust to edge removal than vertex removal, breaking only after a large percentage of edges are removed. It was additionally shown - for most attack strategies - that the network is *less* susceptible to edge removal than networks sampled from a suitable configuration model. Amongst the edge attacks used was a proposed similarity measure for edges, which showed that aggregate transactions performed between similar users are slightly more important than those performed between dissimilar ones. The only edge attack strategy that exhibited a convex plot was the degree centrality product attack, so it is possible that information contained within the edges (aggregated transaction count and total) do not provide any significant measure to determine the influence they exude over the underlying topology of the Rabobank network; only by including information about the source and target nodes did we obtain an effective attack strategy.

The final set of results in this report was a comparison of analytical and topological properties of the network to random networks: we demonstrated that although the network possesses an exceedingly small amount of disassortativity relative to interbank networks, it is considerably more disassortative than random networks. Conversely, the network was shown to be around five times less transitive than random networks. The differences in these measures were then used to provide an intuition as to why the robustness of the intrabank network differs to random networks sharing the same degree sequence. We finally computed the p_c lower bound for the network, and found it to be lower than those of random networks, indicating that analytically, the Rabobank network is in the worst case less robust than random networks. It is worth noting that the graph measures used to explore the properties that make the network special are only a subset of the possible ones we can use. As a result, the explanation we provide is only from an intuitive standpoint rather than one with theoretical or empirical evidence; future works can expand upon the measures used for comparison with random networks to fully grasp the unique properties of the

intrabank network.

Future works can further the knowledge we have acquired through this study by extending the robustness analysis of the network; so far we have only considered attacks based on a precomputed value for each vertex/edge (known as simultaneous attacks), by instead recomputing these values after each removal we can acquire insight into how the network would respond to *sequential* attack. As a result, we can refine our understanding of the structure of intrabank networks and what makes users and their transactions influential to it, this can also further elucidate the topological differences between theoretical networks and intrabank networks. Additionally, we have only considered a network constructed from aggregate transactions, leaving the temporal information for each transaction redundant. Constructing a network from singular transactions and their dates enables us to learn about the dynamics of intrabank networks over time, and how their underlying topology and robustness evolves. An understanding of the temporal dynamics of intrabank networks can also lead to the proposal of generative models for them, which provides both a better theoretical grounding and null model for empirical study. An introduction of refined null models for intrabank networks leads to the construction of simulated systems that closely mimic reality and is thus an interesting direction for future work.

Given the novelty of intrabank networks, it may be the case that new centrality measures yield better solutions to identify systemic importance within them. For example, it could be beneficial in the future to use a centrality measure that takes into account the temporal information of each transaction, and to see if interbank centrality measures such as DebtRank and SinkRank can be adapted for use in intrabank environments. The latter approach can be an important avenue for future research as it highlights the similarities between interbank and intrabank networks, comparing the behaviours of financial instutions and the users within them.

Bibliography

[1] F. Allen and D. Gale, "Financial contagion," *Journal of political economy*, vol. 108, no. 1, pp. 1–33, 2000.

[2] X. Freixas, B. M. Parigi, and J.-C. Rochet, "Systemic risk, interbank relations, and liquidity provision by the central bank," *Journal of money, credit and banking*, pp. 611–638, 2000.

[3] P. Gai and S. Kapadia, "Contagion in financial networks," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 466, no. 2120, pp. 2401–2423, 2010.

[4] D. Acemoglu, A. Ozdaglar, and A. Tahbaz-Salehi, "Systemic risk and stability in financial networks," *American Economic Review*, vol. 105, no. 2, pp. 564–608, 2015.

[5] M. Elliott, B. Golub, and M. O. Jackson, "Financial networks and contagion," *American Economic Review*, vol. 104, no. 10, pp. 3115–53, 2014.

[6] R. Cohen, K. Erez, D. Ben-Avraham, and S. Havlin, "Breakdown of the internet under intentional attack," *Physical review letters*, vol. 86, no. 16, p. 3682, 2001.

[7] H. Jeong, B. Tombor, R. Albert, Z. N. Oltvai, and A.-L. Barabási, "The large-scale organization of metabolic networks," *Nature*, vol. 407, no. 6804, pp. 651–654, 2000.

[8] J.-P. Onnela, J. Saramäki, J. Hyvönen, G. Szabó, M. A. De Menezes, K. Kaski, A.-L. Barabási, and J. Kertész, "Analysis of a large-scale weighted network of one-to-one human communication," *New journal of physics*, vol. 9, no. 6, p. 179, 2007.

[9] A. Broder, R. Kumar, F. Maghoul, P. Raghavan, S. Rajagopalan, R. Stata, A. Tomkins, and J. Wiener, "Graph structure in the web," in *The Structure and Dynamics of Networks*, pp. 183–194, Princeton University Press, 2011.

[10] A. Saxena, Y. Pei, J. Veldsink, W. van Ipenburg, G. Fletcher, and M. Pechenizkiy, "The banking transactions dataset and its comparative analysis with scale-free networks," in *Proceedings of the 2021 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, pp. 283–296, 2021.

[11] A.-L. Barabási, "Network science," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 371, no. 1987, p. 20120375, 2013.

[12] D. B. West *et al.*, *Introduction to graph theory*, vol. 2. Prentice hall Upper Saddle River, 2001.

[13] C. Godsil and G. F. Royle, *Algebraic graph theory*, vol. 207. Springer Science & Business Media, 2001.

[14] Y. Li and Z.-L. Zhang, "Digraph laplacian and the degree of asymmetry," *Internet Mathematics*, vol. 8, no. 4, pp. 381–401, 2012.

[15] G. H. Golub and C. F. Van Loan, "Matrix computations. edition," 1996.

[16] G. Kirchhoff, "Ueber die auflösung der gleichungen, auf welche man bei der untersuchung der linearen vertheilung galvanischer ströme geführt wird," *Annalen der Physik*, vol. 148, no. 12, pp. 497–508, 1847.

[17] M. Fiedler, "Algebraic connectivity of graphs," *Czechoslovak mathematical journal*, vol. 23, no. 2, pp. 298–305, 1973.

[18] J. Cheeger, "A lower bound for the smallest eigenvalue of the laplacian," in *Problems in analysis*, pp. 195–200, Princeton University Press, 2015.

[19] M. X. Cheng, Y. Ling, and B. M. Sadler, "Network connectivity assessment and improvement through relay node deployment," *Theoretical Computer Science*, vol. 660, pp. 86–101, 2017.

[20] M. E. Newman, "Finding community structure in networks using the eigenvectors of matrices," *Physical review E*, vol. 74, no. 3, p. 036104, 2006.

[21] K.-i. Hashimoto, "Zeta functions of finite graphs and representations of p-adic groups," in *Automorphic forms and geometry of arithmetic varieties*, pp. 211–280, Elsevier, 1989.

[22] M. E. Newman, "The structure and function of complex networks," *SIAM review*, vol. 45, no. 2, pp. 167–256, 2003.

[23] M. E. Newman, "Mixing patterns in networks," *Physical review E*, vol. 67, no. 2, p. 026126, 2003.

[24] P. Erdös and A. Rényi, "On random graphs i," *Publicationes Mathematicae Debrecen*, vol. 6, p. 290, 1959.

[25] P. Erdos, A. Rényi, *et al.*, "On the evolution of random graphs," *Publ. Math. Inst. Hung. Acad. Sci*, vol. 5, no. 1, pp. 17–60, 1960.

[26] B. Bollobás and A. G. Thomason, "Threshold functions," *Combinatorica*, vol. 7, no. 1, pp. 35–38, 1987.

[27] M. Boss, H. Elsinger, M. Summer, S. Thurner, *et al.*, "An empirical analysis of the network structure of the austrian interbank market," *Financial Stability Report*, vol. 7, pp. 77–87, 2004.

[28] G. De Masi, G. Iori, and G. Caldarelli, "Fitness model for the italian interbank money market," *Physical Review E*, vol. 74, no. 6, p. 066112, 2006.

[29] M. Faloutsos, P. Faloutsos, and C. Faloutsos, "On power-law relationships of the internet topology," in *The Structure and Dynamics of Networks*, pp. 195–206, Princeton University Press, 2011.

[30] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *science*, vol. 286, no. 5439, pp. 509–512, 1999.

[31] R. Cohen, K. Erez, S. Havlinl, M. Newman, A.-L. Barabási, D. J. Watts, *et al.*, "Resilience of the internet to random breakdowns," in *The Structure and Dynamics of Networks*, pp. 507–509, Princeton University Press, 2011.

[32] R. Swendsen, *An introduction to statistical mechanics and thermodynamics*. Oxford University Press, USA, 2020.

[33] J. Shore and R. Johnson, "Axiomatic derivation of the principle of maximum entropy and the principle of minimum cross-entropy," *IEEE Transactions on information theory*, vol. 26, no. 1, pp. 26–37, 1980.

[34] E. T. Jaynes, "Information theory and statistical mechanics," *Physical review*, vol. 106, no. 4, p. 620, 1957.

[35] S. Y. Park and A. K. Bera, "Maximum entropy autoregressive conditional heteroskedasticity model," *Journal of Econometrics*, vol. 150, no. 2, pp. 219–230, 2009.

[36] R. Albert and A.-L. Barabási, "Statistical mechanics of complex networks," *Reviews of modern physics*, vol. 74, no. 1, p. 47, 2002.

[37] T. Hara and G. Slade, "The incipient infinite cluster in high-dimensional percolation," *Electronic Research Announcements of the American Mathematical Society*, vol. 4, no. 8, pp. 48–55, 1998.

[38] T. Kalisky and R. Cohen, "Width of percolation transition in complex networks," *Physical Review E*, vol. 73, no. 3, p. 035101, 2006.

[39] B. Bollobás, C. Borgs, J. Chayes, and O. Riordan, "Percolation on dense graph sequences," *The Annals of Probability*, vol. 38, no. 1, pp. 150–183, 2010.

[40] B. Karrer, M. E. Newman, and L. Zdeborová, "Percolation on sparse networks," *Physical review letters*, vol. 113, no. 20, p. 208702, 2014.

[41] D. A. Levin and Y. Peres, *Markov chains and mixing times*, vol. 107. American Mathematical Soc., 2017.

[42] R. Bubley and M. Dyer, "Path coupling: A technique for proving rapid mixing in markov chains," in *Proceedings 38th Annual Symposium on Foundations of Computer Science*, pp. 223–231, IEEE, 1997.

[43] J. Geanakoplos, "The leverage cycle," *NBER macroeconomics annual*, vol. 24, no. 1, pp. 1–66, 2010.

[44] J. Danielsson, H. S. Shin, J.-P. Zigrand, *et al.*, "Endogenous and systemic risk," *Quantifying systemic risk*, pp. 73–94, 2013.

[45] S. Battiston, M. Puliga, R. Kaushik, P. Tasca, and G. Caldarelli, "Debtrank: Too central to fail? financial networks, the fed and systemic risk," *Scientific reports*, vol. 2, no. 1, pp. 1–6, 2012.

[46] M. Bardoscia, S. Battiston, F. Caccioli, and G. Caldarelli, "Debtrank: A microscopic foundation for shock propagation," *PloS one*, vol. 10, no. 6, p. e0130406, 2015.

[47] S. Thurner and S. Poledna, "Debtrank-transparency: Controlling systemic risk in financial networks," *Scientific reports*, vol. 3, no. 1, pp. 1–7, 2013.

[48] F. Caccioli, M. Shrestha, C. Moore, and J. D. Farmer, "Stability analysis of financial contagion due to overlapping portfolios," *Journal of Banking & Finance*, vol. 46, pp. 233–245, 2014.

[49] F. Caccioli, J. D. Farmer, N. Foti, and D. Rockmore, "Overlapping portfolios, contagion, and financial stability," *Journal of Economic Dynamics and Control*, vol. 51, pp. 50–63, 2015.

[50] C. Iazzetta and M. Manna, "The topology of the interbank market: developments in italy since 1990," *Bank of Italy Temi di Discussione (Working Paper) No*, vol. 711, 2009.

[51] M. Boss, H. Elsinger, M. Summer, and S. Thurner 4, "Network topology of the interbank market," *Quantitative finance*, vol. 4, no. 6, pp. 677–684, 2004.

[52] S. Lenzu and G. Tedeschi, "Systemic risk on different interbank network topologies," *Physica A: Statistical Mechanics and its Applications*, vol. 391, no. 18, pp. 4331–4341, 2012.

[53] K. Soramäki, M. L. Bech, J. Arnold, R. J. Glass, and W. E. Beyeler, "The topology of interbank payment flows," *Physica A: Statistical Mechanics and its Applications*, vol. 379, no. 1, pp. 317–333, 2007.

[54] M. L. Bech and E. Atalay, "The topology of the federal funds market," *Physica A: Statistical Mechanics and its Applications*, vol. 389, no. 22, pp. 5223–5246, 2010.

[55] P. S. Bearman, J. Moody, and K. Stovel, "Chains of affection: The structure of adolescent romantic and sexual networks," *American journal of sociology*, vol. 110, no. 1, pp. 44–91, 2004.

[56] J. H. Jones and M. S. Handcock, "An assessment of preferential attachment as a mechanism for human sexual network formation," *Proceedings of the Royal Society of London. Series B: Biological Sciences*, vol. 270, no. 1520, pp. 1123–1128, 2003.

[57] F. Liljeros, C. R. Edling, L. A. N. Amaral, H. E. Stanley, and Y. Åberg, "The web of human sexual contacts," *Nature*, vol. 411, no. 6840, pp. 907–908, 2001.

[58] M. E. Newman, S. Forrest, and J. Balthrop, "Email networks and the spread of computer viruses," *Physical Review E*, vol. 66, no. 3, p. 035101, 2002.

[59] H. W. Hethcote, "The mathematics of infectious diseases," *SIAM review*, vol. 42, no. 4, pp. 599–653, 2000.

[60] P. Grassberger, "On the critical behavior of the general epidemic process and dynamical percolation," *Mathematical Biosciences*, vol. 63, no. 2, pp. 157–172, 1983.

[61] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world'networks," *nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[62] M. E. Newman, "Scientific collaboration networks. ii. shortest paths, weighted networks, and centrality," *Physical review E*, vol. 64, no. 1, p. 016132, 2001.

[63] S. Milgram, "The small world problem," *Psychology today*, vol. 2, no. 1, pp. 60–67, 1967.

[64] R. J. Williams, E. L. Berlow, J. A. Dunne, A.-L. Barabási, and N. D. Martinez, "Two degrees of separation in complex food webs," *Proceedings of the National Academy of Sciences*, vol. 99, no. 20, pp. 12913–12916, 2002.

[65] S. Redner, "How popular is your paper? an empirical study of the citation distribution," *The European Physical Journal B-Condensed Matter and Complex Systems*, vol. 4, no. 2, pp. 131–134, 1998.

[66] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *nature*, vol. 406, no. 6794, pp. 378–382, 2000.

[67] R. V. Sole and M. Montoya, "Complexity and fragility in ecological networks," *Proceedings of the Royal Society of London. Series B: Biological Sciences*, vol. 268, no. 1480, pp. 2039–2045, 2001.

[68] Q. Chen, H. Chang, R. Govindan, and S. Jamin, "The origin of power laws in internet topologies revisited," in *Proceedings. twenty-first annual joint conference of the ieee computer and communications societies*, vol. 2, pp. 608–617, IEEE, 2002.

[69] M. Faloutsos, P. Faloutsos, and C. Faloutsos, "On power-law relationships of the internet topology," *ACM SIGCOMM computer communication review*, vol. 29, no. 4, pp. 251–262, 1999.

[70] F. Krzakala, C. Moore, E. Mossel, J. Neeman, A. Sly, L. Zdeborová, and P. Zhang, "Spectral redemption in clustering sparse networks," *Proceedings of the National Academy of Sciences*, vol. 110, no. 52, pp. 20935–20940, 2013.

[71] U. Brandes, "A faster algorithm for betweenness centrality," *Journal of mathematical sociology*, vol. 25, no. 2, pp. 163–177, 2001.

[72] U. Brandes and C. Pich, "Centrality estimation in large networks," *International Journal of Bifurcation and Chaos*, vol. 17, no. 07, pp. 2303–2318, 2007.

[73] E. Cohen, D. Delling, T. Pajor, and R. F. Werneck, "Computing classic closeness centrality, at scale," in *Proceedings of the second ACM conference on Online social networks*, pp. 37–50, 2014.

[74] C. M. Schneider, A. A. Moreira, J. S. Andrade, S. Havlin, and H. J. Herrmann, "Mitigation of malicious attacks on networks," *Proceedings of the National Academy of Sciences*, vol. 108, no. 10, pp. 3838–3841, 2011.

[75] B. K. Fosdick, D. B. Larremore, J. Nishimura, and J. Ugander, "Configuring random graph models with fixed degree sequences," *Siam Review*, vol. 60, no. 2, pp. 315–355, 2018.

[76] R. Kannan, P. Tetali, and S. Vempala, "Simple markov-chain algorithms for generating bipartite graphs and tournaments," *Random Structures & Algorithms*, vol. 14, no. 4, pp. 293–308, 1999.

[77] P. L. Erdös, I. Miklós, and L. Soukup, "Towards random uniform sampling of bipartite graphs with given degree sequence," *arXiv preprint arXiv:1004.2612*, 2010.

[78] P. L. Erdős, C. Greenhill, T. R. Mezei, I. Miklós, D. Soltész, and L. Soukup, "The mixing time of switch markov chains: a unified approach," *European Journal of Combinatorics*, vol. 99, p. 103421, 2022.

[79] D. W. Scott, *Multivariate density estimation: theory, practice, and visualization*. John Wiley & Sons, 2015.

[80] T. W. Anderson and D. A. Darling, "Asymptotic theory of certain" goodness of fit" criteria based on stochastic processes," *The annals of mathematical statistics*, pp. 193–212, 1952.

[81] D. Barber, *Bayesian reasoning and machine learning*. Cambridge University Press, 2012.

[82] B. Tao, H.-N. Dai, J. Wu, I. W.-H. Ho, Z. Zheng, and C. F. Cheang, "Complex network analysis of the bitcoin transaction network," *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2021.

A Appendix

A.1 Source code

Code used for this project available in the GitHub repository https://github.com/Danieldosti51/rabobank-network-robustness.