15/04/2025

Network Analysis

« Bitcoin Transactions » and

« Madoff Fraud »

Ozren Pain

BACHELOR OF ECONOMICS AND MANAGEMENT – 3RD YEAR

Analysis of the Bitcoin Transactions Network

This network represents bitcoin transactions covering the period from January 2009 to April 2013. The nodes are public key “addresses” at a given moment within the given period, and each edge is labelled with the time (to a resolution of a few seconds) of the transaction. This makes it possible to trace precisely the chronology of exchanges, which is fundamental to understanding the temporal dynamics and the evolution of economic activity within the network. The dataset is provided in the form of two CSV files: one containing the links (with the source address, the target address, the number of transactions, and the associated extreme dates), the other listing the nodes, each associated with the date of its first transaction. This type of network is particularly interesting from an economic and systemic analysis perspective because it represents the actual flows of value in a decentralised system without a central regulating entity, thus shedding light on the dynamics specific to monetary exchanges in crypto-economies.

The complete network is very vast, with about 1,000,000 addresses (nodes) and more than 1,000,000 edges (transactions). Faced with this scale, and due to the computational limits of standard environments such as Google Colab, it was necessary to opt for a mixed approach. On the one hand, certain global measures were extracted from the giant component of the network, that is to say the subgraph containing the largest part of the nodes connected together (about 519,000 nodes out of more than a million, i.e. nearly 42% of the total network). On the other hand, for metrics particularly demanding in resources such as eigenvector centrality, clustering coefficient, community detection or triangle analysis, it was necessary to extract a representative random sample of 2000 nodes belonging to this giant component. This makes it possible to preserve the statistical validity of the analysis while ensuring reasonable calculation times.

The structural analysis of the network reveals an extremely sparse graph. The calculation of density, that is to say the ratio between the number of existing edges and the theoretical maximum number of possible edges, gives a value close to zero. This result is consistent with the nature of a transactional network in a system where most addresses are used only once, or very occasionally, which is a well-documented characteristic in Bitcoin research. This low density reflects a peer-to-peer economy where confidentiality takes precedence, leading to star-like structures around a few actors and a multitude of unique interactions. The majority of addresses play a marginal role in the network, which is also reflected in the degree distributions. These show a strong asymmetry: many addresses have only a single incoming or outgoing link, while a minority concentrate many links, giving the network a heterogeneous structure.

Degree centrality makes it possible to identify these particular nodes that receive or emit a large number of transactions. On the sample of 2000 nodes, several addresses appear as hubs. However, when one considers betweenness centrality, which measures the importance of a node in the routing of flows between other nodes, one observes that most addresses have no mediating role. The betweenness score is often zero, which confirms that the network is little hierarchised, with a very flat structure. This observation is reinforced by closeness centrality, which remains relatively homogeneous in the sample, and eigenvector centrality, which does not reveal dominant figures. This indicates a form of effective decentralisation, where economic activity is distributed without excessive concentration of transactional power.

From a topological point of view, the Bitcoin network presents certain characteristics of “small-world” networks. The average length of the shortest paths in the giant component is about 3.9, and the diameter reaches 9. These values are low in view of the size of the network, indicating that provided a path exists, transactions can circulate rapidly between nodes. This low average distance favours a certain transactional efficiency, despite the apparent fragmentation. However, this apparent efficiency must not mask the fact that the network is made up of a large number of small components not connected to the giant component, or of very weakly linked nodes. From this point of view, the global structure remains very fragmented.

The Bitcoin network also seems extremely fragile. For example, by measuring the 10% of nodes with the highest degrees and by measuring the relative size of the remaining giant component. This drops to about 7% of the initial network, which indicates a structural dependence on a minority of highly connected nodes. This property is typical of networks with degree distribution following a power law, which seems to be the case here judging by the shape of the log-log scale histograms. This implies that, if a malicious actor succeeded in isolating or neutralising the few most connected addresses, the network as a whole could find itself strongly fragmented, which raises the question of the resilience of the blockchain in its transactional use. This structural fragility suggests that the illusion of decentralisation may conceal a strong dependence on a few key actors of the system.

Community analysis makes it possible to go further in the understanding of the modularity of the network. By applying on the sample of 2000 nodes a detection method based on modularity (greedy modularity communities), one finds nearly 2000 distinct communities. This means that, on this sample, almost every address is isolated in its own sub-structure, or forms a very small group with a few other addresses. This reflects the ephemeral and anonymous nature of Bitcoin transactions, where users often generate new addresses for each transaction in order to increase their anonymity. The fact that the densest core (maximal k-core) of the network is equal to 1 confirms this low structural density: there does not exist a sub-network in which each node would be connected to at least two others, which contrasts with classical social networks, where communities often form dense cores. This extreme modularity illustrates a model of economic interaction without lasting commitment, specific to the logics of automated and pseudonymous exchange.

The other metrics confirm this portrait: the average degree of neighbours (k-nearest neighbours) is very low, often zero, which suggests that addresses do not connect to clusters but to isolated targets. The number of detected triangles is also very low, which attests to a very low rate of transitivity and an absence of redundancy in the connections. In other words, addresses rarely exchange with several partners who also exchange between themselves, which is contrary to what is observed in networks of social or professional type. This lack of redundancy reflects a compartmentalised transactional structure, suited to a logic of occasional micro-exchange rather than collective dynamics.

Finally, although it was not possible to visualise the complete network due to its size, the structural properties observed on the giant component and the random sample make it possible to deduce probable visual characteristics. For example, the star-like structure around a few highly connected nodes, as well as the multitude of weakly linked or isolated nodes, suggest a globally fragmented graph, without dense clusters nor marked community structures. This configuration perfectly illustrates the common practice of the “one-time use address” in the Bitcoin ecosystem. Even without direct visualisation, the structural indicators point towards an atomised network, where interactions are dispersed, little redundant, and rarely recurrent.

This analysis of the Bitcoin Transactions network between 2009 and 2013 therefore reveals a transactional system vast but profoundly fragmented, weakly connected and weakly redundant. The combination of low density, extreme modularity, great structural vulnerability, and a flattened hierarchy makes this network unique in its kind. It is neither a social network, nor a classical economic network, but indeed a digital artefact resulting from a logic of confidentiality, immediacy, and automation of exchanges. This network does not reflect a community of users connected to one another, but rather a succession of micro-interactions without collective memory, without redundancy, and without stable long-term structure. It embodies an economic model of fluid but impersonal exchange, proper to a radical vision of decentralisation.

Analysis of the Madoff Network

The second network analysed within the framework of this assignment concerns the financial flows involved in Bernard Madoff's fraud, one of the largest financial scams in contemporary history. Madoff, former president of NASDAQ and investment fund manager, was found guilty of having orchestrated a Ponzi-type scheme of unprecedented scale, causing the loss of tens of billions of dollars for individuals, banks and institutions across the world. The network studied here was reconstructed from public sources, notably press articles, judicial documents and media investigations, and it represents the flows of money between the financial entities having invested, directly or indirectly, in Madoff's fund.

The network is made up of 61 nodes, representing financial institutions, private banks, management companies and investment funds. It is a directed graph, where each edge corresponds to a monetary flow from one actor to another. The network is dense in information despite its modest size, because it reflects a complex entanglement of financial relations, management delegations, and financial arrangements aimed at channelling the investors' money towards the central entity of the fraudulent scheme: Bernard_Madoff_Investment. Contrary to the Bitcoin network, where the links can be temporary and massively distributed, here the relations are more stable, structural and intentional, which reflects a dynamic of institutional network highly organised.

The global properties of the network confirm this hierarchised structure. The graph is weakly dense (density about 0.033), but nevertheless connected: all the nodes are linked in a single component. This means that, despite a low proportion of links compared with the theoretical maximum, the whole system remains unified around a nerve centre. The average degree is 2, which is relatively low, but certain institutions display much higher degrees, beginning with Bernard_Madoff_Investment, which alone holds a centralised degree of 0.45, by far the highest of the network. This immediately confirms its position as the point of convergence of all financial flows.

The analysis of centralities goes in the same direction. In addition to being the most connected node, Bernard_Madoff_Investment is situated at the heart of the network in terms of betweenness centrality: the links that lead to it, notably those emanating from Cohmad_securities, Fairfield_Greenwich, Tremont_Group_Holdings or Gabriel_Capital, have the highest betweenness scores of the network. These connections are not trivial: they in fact represent "feeder funds", that is to say specialised funds that collected money from multiple clients or other institutions before transferring it directly to Madoff. In this sense, these funds played the role of transmission belts, sometimes concealing from their own clients the true destination of the capital. The structuring role of these intermediary nodes in the functioning of the network is striking, and their removal would have a major impact on the connectivity of the graph.

This is precisely what the analysis of the structural robustness of the network shows. By simulating the removal of the 10% of nodes with the highest degrees, one observes that the size of the main component falls abruptly to 6.5% of the initial network. The network is therefore extremely vulnerable to targeted attacks, confirming that its structure rests on a critical minority of intermediaries. This property is typical of centralised fraudulent networks: their apparent diversity conceals in reality a star-shaped architecture around a single centre, here Bernard Madoff, and a handful of pivotal nodes.

The analysis of the shortest paths and the diameter (APL ≈ 3.43, diameter = 7) shows a certain efficiency in the circulation of flows, reinforcing the idea that the network was designed to channel funds rapidly towards Madoff, whatever their initial origin. However, contrary to a “natural” social or transactional network, here this efficiency is not the fruit of organic interactions, but of a construction deliberately oriented towards a single goal: to conceal the fraud behind a curtain of apparent complexity.

The clustering measures confirm this absence of horizontal interactions. The average clustering coefficient is zero, and no triangle has been detected in the network. This means that there are no groups of actors interconnected with one another, no relational redundancy. Each link goes from an investor to an intermediary, or from an intermediary to Madoff, but very rarely from one investor to another, or from one fund to several others. This absence of triplet closure reflects a total lack of cross-checking between the actors: nobody verifies what the other is doing, and each operates in relative opacity, which no doubt contributed to the longevity of the fraud.

The detection of communities made it possible to identify 10 modules in the network. Each community corresponds overall to a distinct fund-raising channel, often centred on one or two pivotal actors. This underlines Madoff’s strategy of segmentation: rather than accumulating all the flows in a single path, he multiplied the parallel circuits, which allowed him to broaden his collection base while dispersing responsibilities. Significantly, these communities do not present strong internal density: as indicated by the maximal k-core (equal to 1), there does not exist any subset of nodes strongly interconnected among themselves. This reveals a total absence of community structure in the strict sense: the funds are linked vertically to Madoff, but not horizontally between themselves.

Finally, the structure of the network is reinforced by a strong degree disassortativity (≈ -0.37). This means that the nodes of high degree (notably Madoff and his close collaborators) are mainly connected to nodes of low degree, that is to say isolated entities that have no other connections. This architecture accentuates the centralisation of the system and isolates each flow, reducing the risks of mutual control or of alert in case of dysfunction. This type of structuring is a classical signature of Ponzi schemes, in which a small number of entities collect the capital of a large number of disconnected investors, by promising them fictitious returns.

The analysis of this network thus highlights the close link between the topology of a financial graph and the functioning of a scheme of fraud. The Madoff network, behind its apparent simplicity (only 61 nodes), reveals a sophisticated organisational engineering, founded on the centralisation of flows, the fragmentation of collectors, and the absence of transparency. Each network metric comes to confirm this observation: low density, absence of triangles, extreme centrality of a few nodes, modularity without density, fragility to targeted removal. The whole outlines a quasi-perfect architecture for a Ponzi scheme: a system which rests on blind trust, the dispersal of responsibilities, and the difficulty of having a global vision of the flows.

Comparison of the Bitcoin and Madoff Networks

The comparative analysis of the Bitcoin (2009-2013) and Madoff networks reveals two radically opposed architectures, both in their structure and in their purpose. The Bitcoin network, stemming from a decentralised technology, is characterised by a fragmented topology weakly connected and little redundant. In contrast, the Madoff network, built around a fraudulent scheme, presents a centralised hierarchised structure and highly vulnerable to targeted attacks.

The Bitcoin network is marked by low density and an absence of redundancy, reflecting the nature both ephemeral and anonymous of transactions. Addresses are often used only once, and the interactions between them are limited. This structure favours confidentiality as well as resilience, but complicates the analysis of financial flows. By contrast, the Madoff network is dense and centralised with financial flows converging towards a single entity. This centralisation facilitates the management of funds but makes the system extremely vulnerable to the failure of key nodes.

On the level of centralities, the Bitcoin network does not present dominant nodes, which indicates a relatively equitable distribution of interactions. On the opposite side, the Madoff network is dominated by a few central nodes, notably Bernard Madoff Investment Securities which concentrate the essential part of the financial flows. This concentration is typical of Ponzi schemes, where the funds of new investors are used to pay the returns of the older ones without genuine underlying economic activity.

The detection of communities in the Bitcoin network reveals a multitude of small weakly connected groups, without clear hierarchical structure. This contrasts with the Madoff network, where the communities are structured around specific investment funds, playing the role of intermediaries between the investors and Madoff. This organisation facilitates the concealment of the fraud and complicates the traceability of funds.

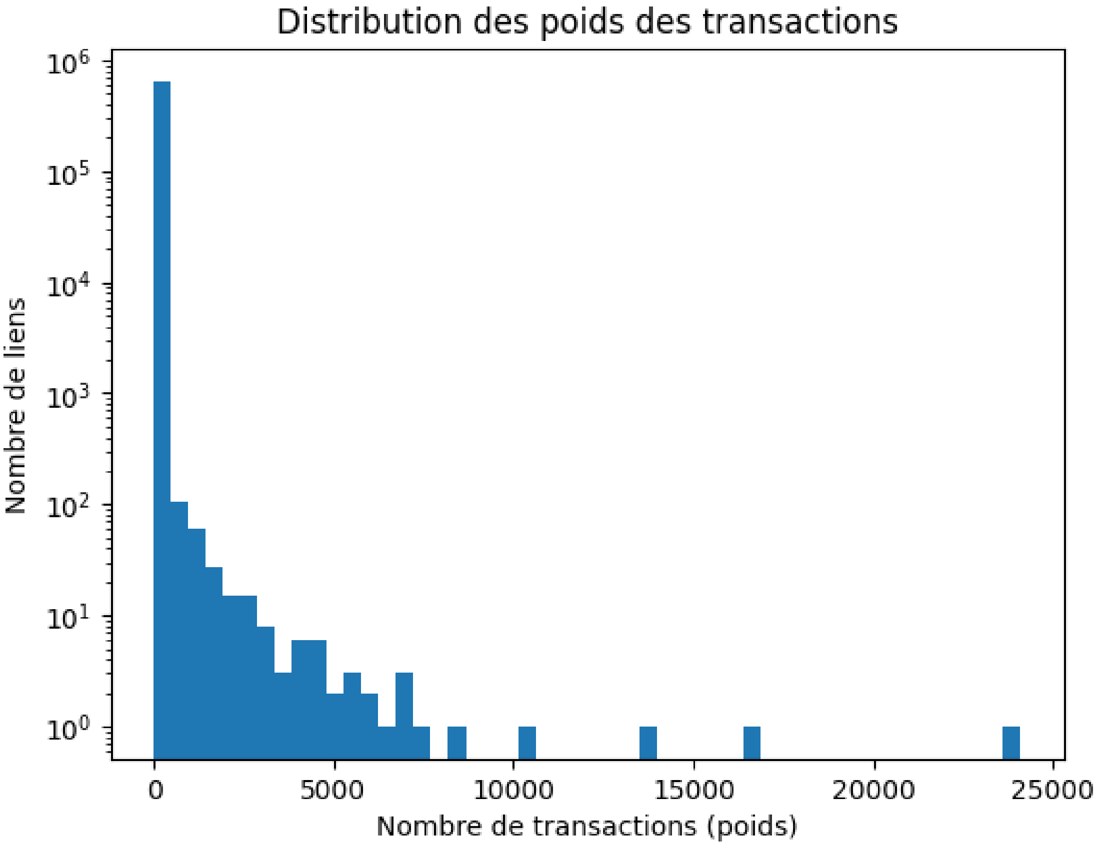
Finally, the resilience of the two networks differs considerably. The Bitcoin network is fragmented but is robust in the face of the removal of nodes, thanks to its decentralised nature. By contrast, the Madoff network is extremely fragile: the removal of a few central nodes suffices to disintegrate the whole system. This fragility is inherent to Ponzi schemes, which rest on trust and the continuity of incoming flows.

The comparative analysis of these two networks thus highlights the fundamental differences between a decentralised system conceived for resilience and confidentiality, and a centralised system structured around fraud, which therefore illustrates the importance of network topology in the understanding of economic dynamics and associated risks.

Appendices

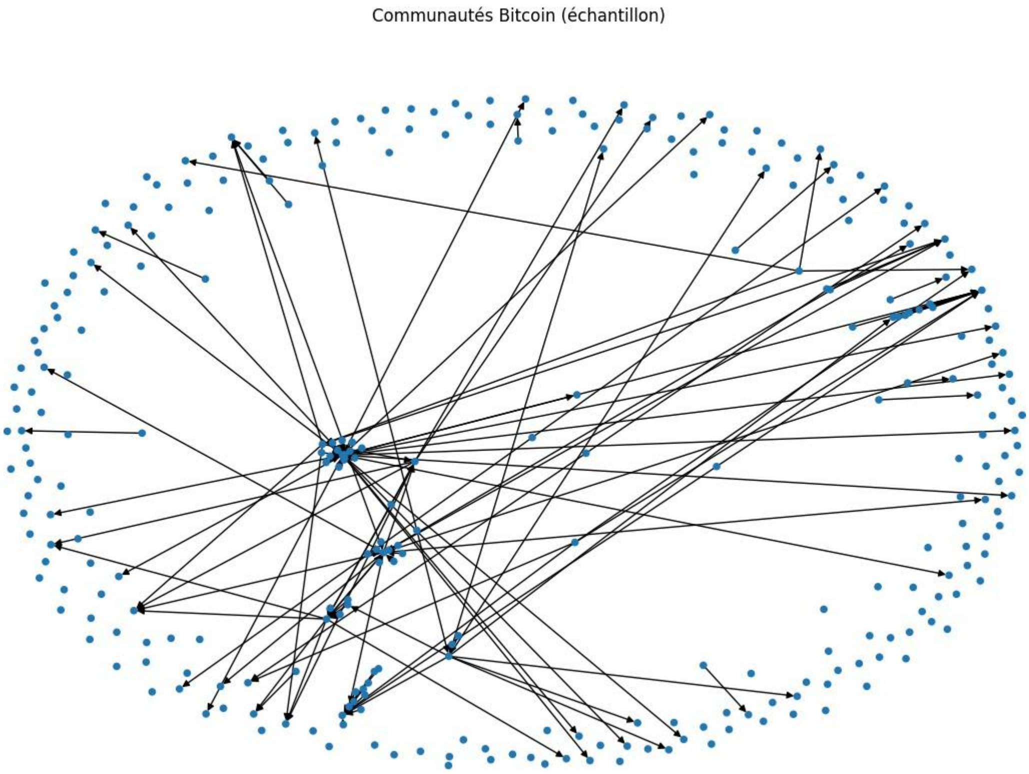
1) Bitcoin Transactions

a. Distribution of transaction weight



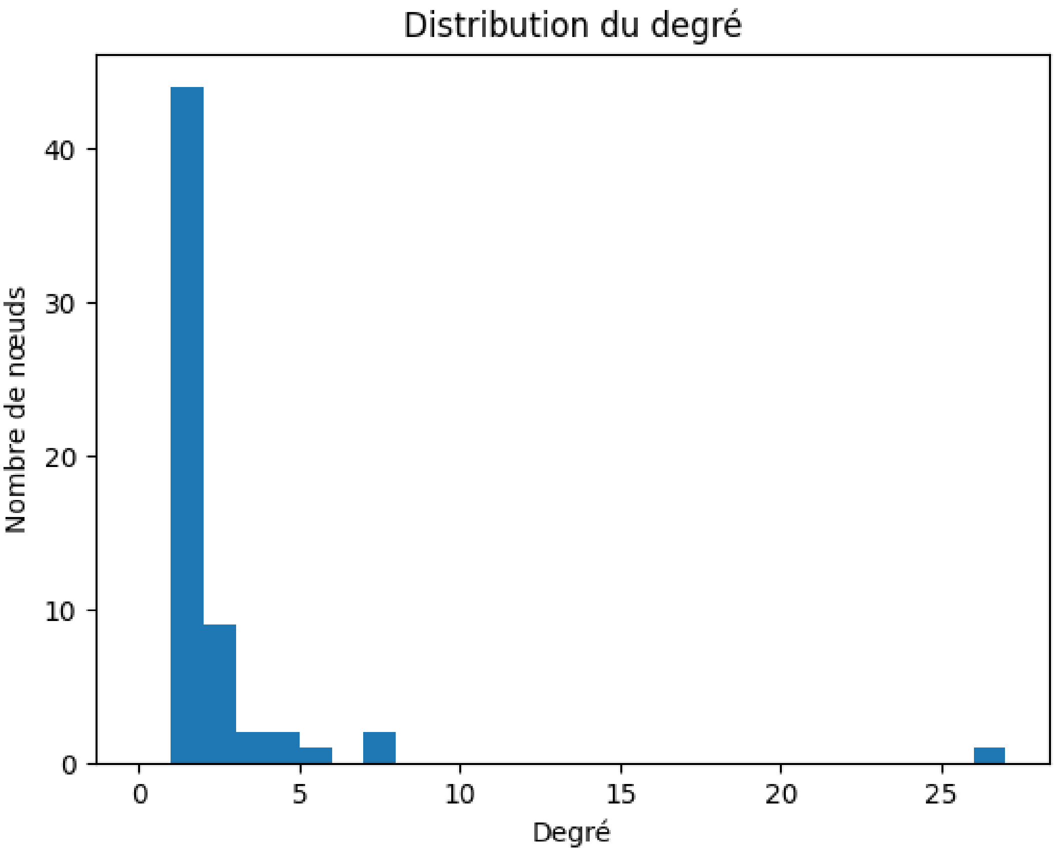
*y:Number of links, x:Number of transactions

b. Bitcoin communities



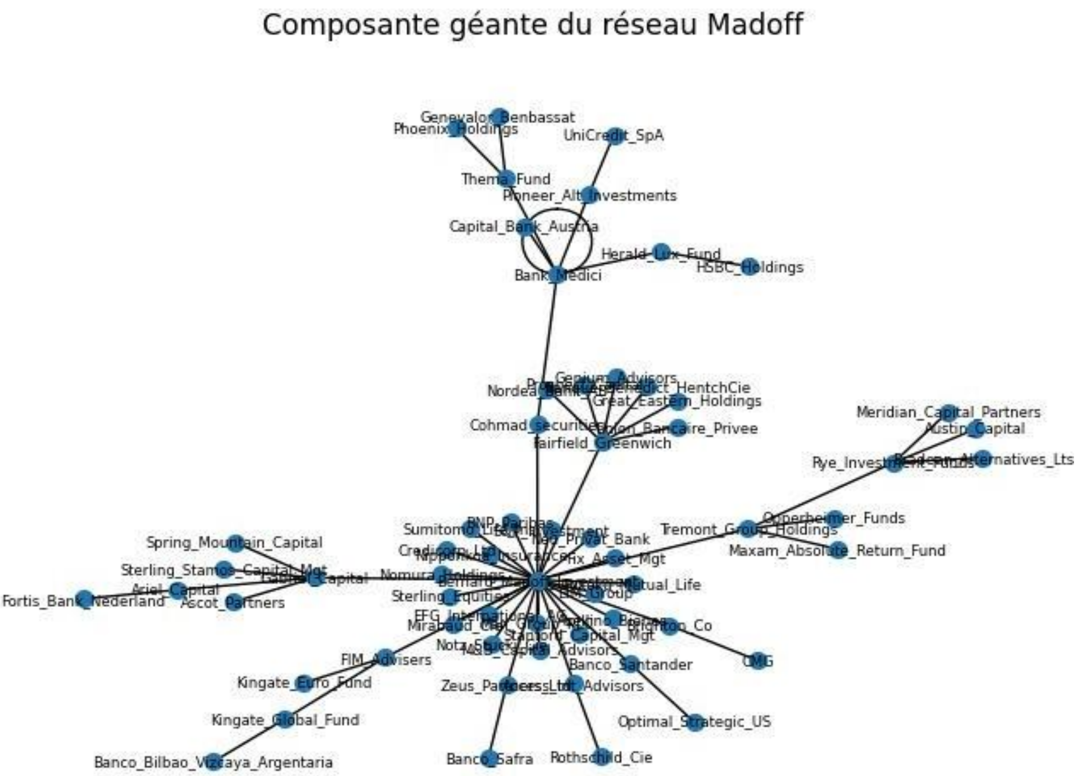
2) Madoff Fraud

a. Distribution of degree

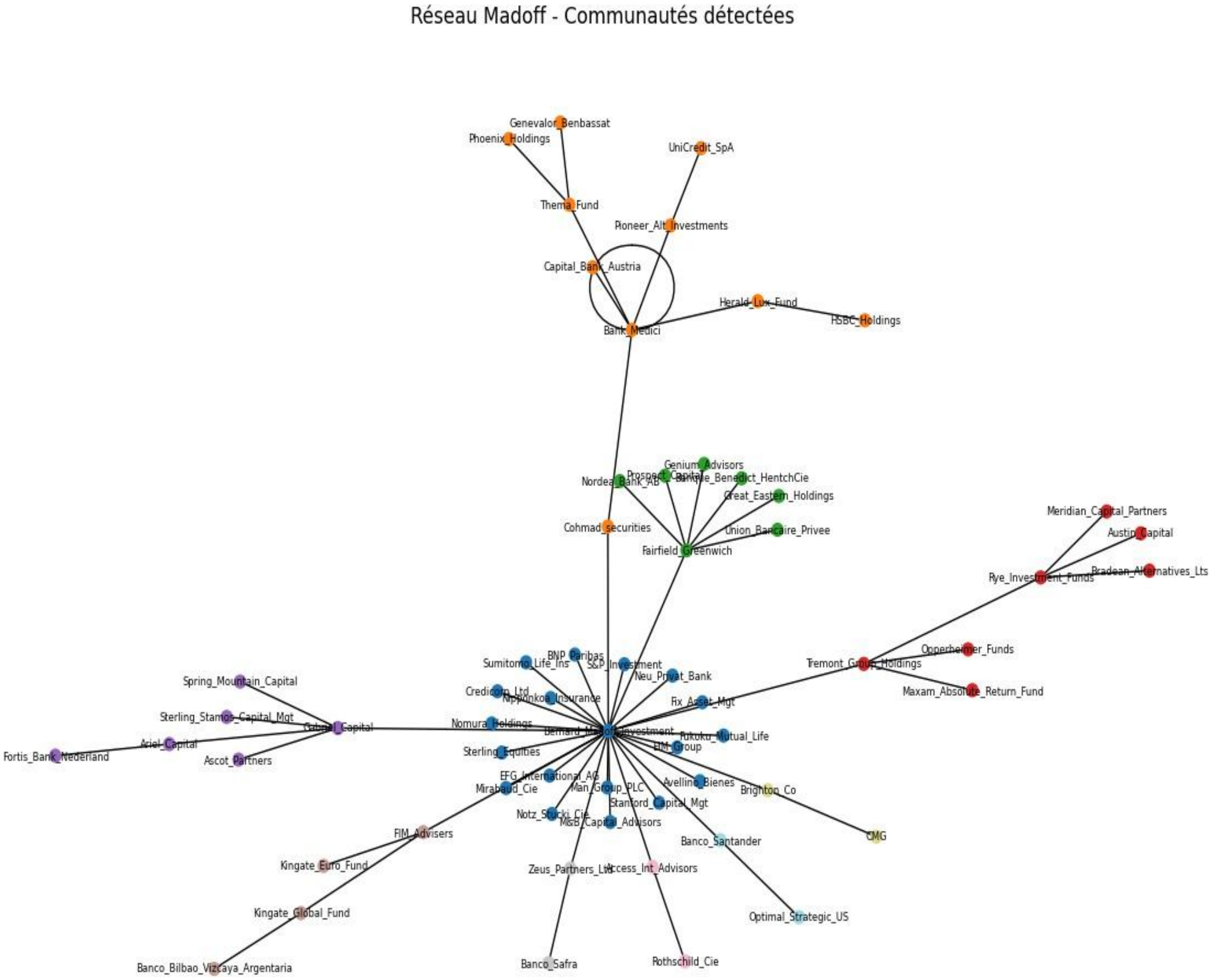


y: Number of nodes, x: Degree

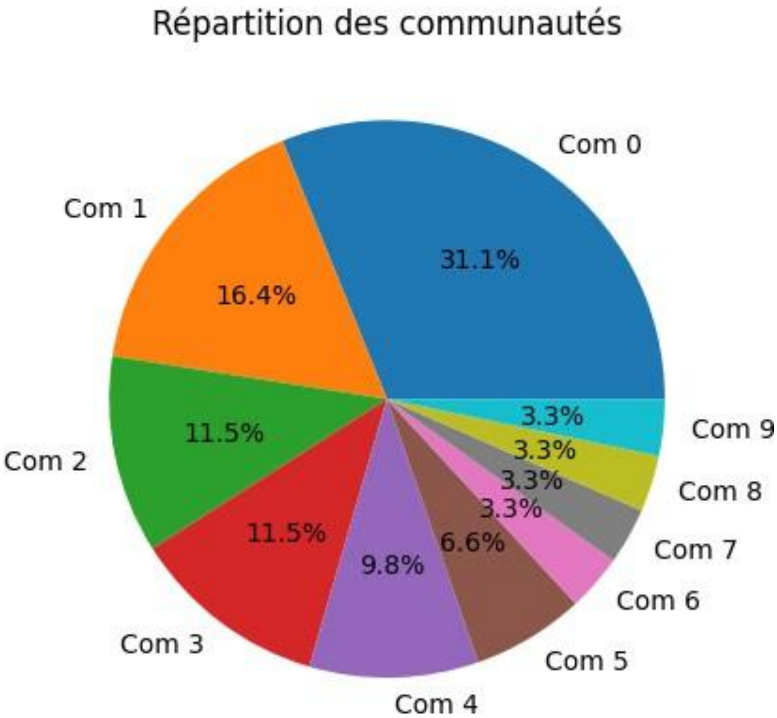
b. Giant component of Madoff Network



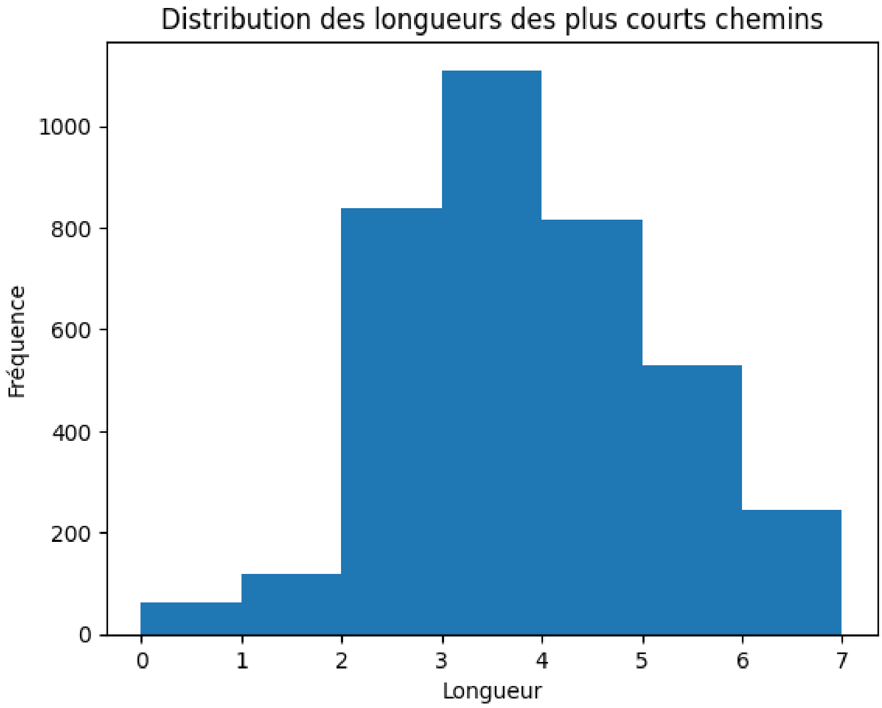
c. Madoff Communities



d. Repartition of communities

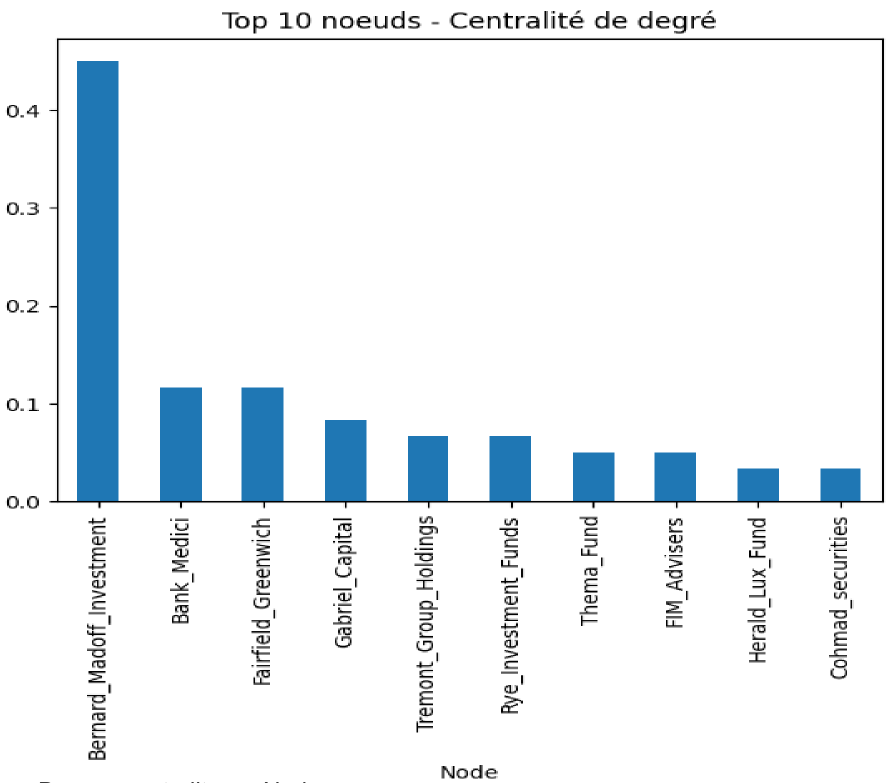


e. Distribution of the length of shortest paths



y: Frequency, x: Length

f. Top 10 nodes by degree centrality



y : Degree centrality, x : Node

References

M. Fire and C. Guestrin, "The Rise and Fall of Network Stars." Preprint (2017)

Ferretti, S., & D'Angelo, G. (2019). "Dissecting Bitcoin Blockchain: Empirical Analysis of Bitcoin Network". *Journal of Network and Computer Applications*.

Perri, F. S., & Brody, R. G. (2017). "Ponzi of All Ponzis: Critical Analysis of the Bernie Madoff Scheme". *International Journal of Economics and Financial Management*.

Schuchter, A., & Levi, M. (2019). "A Crime Script Analysis of the Madoff Investment Scheme". *Crime, Law and Social Change*.

Lischke, M., & Fabian, B. (2016). "Analyzing the Bitcoin Network: The First Four Years". *Future Internet*.

Investopedia. (2024). "Ponzi Scheme: Definition, Examples, and Origins". https://www.investopedia.com/terms/p/ponzischeme.asp

Time. (2021). "Bernie Madoff, Financier Who Operated the Largest Ponzi Scheme in History, Dies". https://time.com/5788411/bernie-madoff-dies/

Stanford University. (2014). "Anomaly Detection in the Bitcoin System - A Network Perspective. https://snap.stanford.edu/class/cs224w-2014/projects2014/cs224w-20-final.pdf

LawSites. (2009). "The Madoff Social Network Map". https://www.lawnext.com/2009/11/madoff-social-network-map.html

Ideal-Investisseur. (2023). "Pyramide de Ponzi : explications de la fraude montée par Madoff". https://www.ideal-investisseur.fr/economie/comprendre-la-pyramide-de-ponzi-systeme-utilise-par-bernard-madoff-7561.html

Springer. (2023). "Blockchain Data Analytics from a Network Perspective". In *Blockchain and Distributed Ledger Technology Use Cases*. https://link.springer.com/chapter/10.1007/978-981-97-4430-5_1