Insider Networks*

Selman Erol[†]

Michael Junho Lee[‡]

December 2023

Abstract

How do insiders respond to regulatory oversight on the use of insider information? History suggests that they form more sophisticated networks to circumvent regulation. We develop a theory of the formation and regulation of insider information networks. We show that agents with sufficiently complex networks bypass any given regulatory environment. In response, regulators employ broad regulatory boundaries to combat gaming. Tighter regulation induces agents to migrate activity from existing social networks to a core-periphery insider network. A small group of agents endogenously arise as intermediaries for the bulk of transmissions.

JEL classification: D85, G14, G20

Keywords: Network Formation, Transmission Networks, Insider Trading, Endogenous Intermediation

*The views expressed in this paper are those of the authors and do not necessarily reflect the position of the Federal Reserve Bank of New York or the Federal Reserve System. Ali Polat provided excellent research assistance. Authors thank Nicola Cetorelli, David Childers, Marco Cipriani, Andrea Galeotti, Co-Pierre Georg, Burton Hollifield, Wei Jiang, Gabriele La Spada, Amir Kermani, Marco Di Maggio, Mihai Manea, Emre Ozdenoren, Bryan Routledge, Omer Tamuz, Chris Telmer, and participants of talks at LBS, Oxford, NY Fed, CMU Tepper, 2019 Pennsylvania Economic Theory Conference, UCSB LAEF OTC Workshop, Vanderbilt Network Science and Economics Conference, and 2020 AFA Meetings for helpful comments. Selman Erol thanks PNC and CMU Tepper School for the PNC Research Assistantship Award.

[†]Carnegie Mellon University, Tepper School of Business. Email: erol@cmu.edu.

[‡]Federal Reserve Bank of New York. Email: michael.j.lee@ny.frb.org.

1 Introduction

From 1928 to 1932, Albert H. Wiggin, then president of the Chase National Bank, accumulated over $10,000,000 solely by trading Chase stock. $4,000,000 was made in the Crash of 1929, during which the stock market crashed, and with it, Chase as well. Wiggin had been shorting his own bank. Wiggin's trades were as legal as much as they were met with public outrage. In an effort to restore confidence in market integrity, the Securities Exchange Act of 1934 was passed which birthed the Security Exchange Commission (SEC). Section 16 of the act, also known as the "anti-Wiggin" proposal, was specifically included to root out abusive securities trading by people with insider information.[1]

In 2008, Mathew Martoma, portfolio manager at hedge fund SAC Capital Advisors, made a twenty minute phone call to owner Steven A. Cohen. Within a span of a week, Cohen reversed his long position in pharmaceutical firms Elan and Wyeth by nearly a billion dollars, which ultimately generated a profit of over $270,000,000. Martoma was later convicted of insider trading. Insider information was passed through a long chain of communication – from Elan to a doctor, to Martoma, who was introduced by an expert network firm. The conviction was the culmination of a painstaking six year investigation by the SEC.[2]

These two instances of insider trading, set apart by nearly a century, draw a striking contrast. In the first case, the insider legally traded directly with his information. In the latter, transmission was achieved through a complex network of connections that had adapted to greater regulatory sophistication. The sender and receiver were otherwise unrelated, with no overlapping social or professional networks, channels through which information typically diffuses. Instead, transmission was facilitated by an intermediary specializing in bringing together sources of information and those who seek it. While regulators have become increasingly sophisticated, so have those that are intent on escaping detection (whom we will conveniently refer to as "insiders"). This suggests that in understanding the cat and mouse game between regulators and insiders, a key consideration is the networks that agents form in order to circumvent regulation, and how regulators might cope with agents' tactics.

[1] http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=6444&context=penn_law_review
[2] http://www.newyorker.com/magazine/2014/10/13/empire-edge

We develop a model of endogenous network formation to study this dynamic between regulators, who set and enforce the regulatory environment, and agents, who form links to pass material non-public information to others to exploit for trading activity without getting caught. Agents can form costly links that enable them to transmit information. Traders that receive information through a shorter chain are able to generate greater trading profits, but agents may want to transmit through a long chain to circumvent regulation.

The regulator's objective is to detect and punish agents for sharing information, which imposes negative social externalities. In order to punish violations, the regulator must provide direct evidence that a trader suspected of insider trading did in fact obtain information from an insider. That is, the regulator must be able to map the entire path of transmission in order to punish the insiders. The regulator is limited in his capacity to observe transmissions, and must incur costs associated with enforcing insider trading cases, which increase with network distance between the insider and the trader.[3]

Our characterization of the regulatory costs holds literal resemblance to costs borne by regulators and prosecutors in an insider trading case. In the pivotal case of US v. Newman, the court ruled in favor of defendants because the traders were "three to four levels removed from the [insider]," adding that there had not been a single case in which "tippees as remote as [the defendants were] held criminally liable for insider trading."[4] More generally, regulatory agencies monitor financial markets for unusual or suspicious activities, especially around significant events that lead to predictable market movements. A successful investigation must meet two conditions: first, provide proof that the user of insider information knows it is so, and second, proof that the sender benefitted from sharing the information, in a form of quid pro quo. Investigators build a case by working backwards and investigating linked individuals to track down the provenance of inside information. As the distance between an individual and insider increases, more resources must be dedicated to unhash details about the subject's relationships, communications, and behavior offering (circumstantial) evidence of knowledge, as well as some form of mutualization of insider trading profits. This process involves costs associated with obtaining permits and

[3]In Section 6.1, we also explore legal boundaries arising from the conflict between enforcement and the violation of social liberties and privacy.

[4]See here for more details.

rights to analyze financial transaction records, private communications, and in some instances, even wiretapping. We view our modeling approach to be a direct analog of insider trading regulation. However, we also consider how other forms of costs may affect enforcement.

First, we show that regulatory ambiguity arises as an equilibrium phenomenon. For any given enforcement strategy potentially chosen by the regulator, agents with extensive networks can conceal their transmissions by using longer chains. Agents can game the system. Importantly, increasing the penalty from detection, or the search intensity of the regulatory environment does not generically hinder the use of insider information. This is reminiscent of Tsebelis (1989). As a result, in equilibrium, the regulator mixes between low and high intensities of enforcement, effectively employing regulatory ambiguity. Doing so induces agents to engage in riskier transmission behavior, allowing the regulator to successfully catch the agent with a positive probability.

Our analysis rationalizes a long standing position taken by regulatory institutions that advocate for flexible, broad guidelines on what constitutes insider trading. Regulatory institutions have been criticized for only loosely defining what constitutes illegal activity pertaining to the use of insider information. With broad rules governing insider trading, courts have been relied upon to ultimately determine illegality. We show that a precise regulatory framework necessarily allows for more gaming, as information networks quickly adapt to the regulatory environment.[5]

Second, we show that regulatory ambiguity impacts agents' network formation. In particular, we show that agents value being part of a network that enables flexible transmission of information, or which facilitates multiple paths of varying distance between agents. A flexible network provides agents with the option of transmitting information either through a risky, direct path, or a safer, longer path. In equilibrium, agents form a *tor-periphery network,* a type of core-periphery, where a small group of agents form the core and act as conduits of information on behalf of the network.[6] This structure embeds the flexibility function into a highly connected core. In doing

[5]The need for deliberately imprecise regulation to effectively combat gaming is a sentiment that extends beyond the context of insider trading regulation. For instance, Greenwood et al. (2017) argues that one of the key benefits of bank stress tests is its flexibility. The use of ambiguity arises more generally in other contexts (for example, see Glazer and Rubinstein (2014)).

[6]This provides a novel channel that may give rise to "law of the few," as discussed in Galeotti and Goyal (2010).

so, agents form a network that is scalable and flexible, and affords periphery members to transmit insider information through a wide set of transmission paths.

Our theory yields several testable empirical implications. In equilibrium, ambiguous regulatory boundaries induce insiders to share information through both short and long chains, with varying levels of risk of getting caught. Consequently, it predicts that the *observed* set of insider trading cases should involve shorter chains, which are also more profitable. Our characterization of insiders' transmission strategies map closely to those observed in recent insider trading cases. The bulk of observed cases involve shorter chains, supporting a tradeoff insiders face between path length and enforcement risk.[7] In the fewer observed cases involving sophisticated agents, a core of intermediaries were found to "shuffle" insider information through a chain of intermediaries on behalf of corporate insiders and hedge funds, requiring costly (and sometimes failed) attempts to prosecute by regulators.[8] Furthermore, empirical studies find that trade profitability declines with path length, for example when the trader is at the fourth or fifth link (Ahern, 2017).

Our theory also predicts that the *maximum* regulatory boundary plays a vital part in constraining the profitability of insider trading. Thus, a shock to regulatory costs or other limitations on the regulatory boundary directly benefit insiders, who can more aggressively transmit information by using shorter chains and increase profits. Pierce (2023) examines the performance of traders affected by insider court decisions that exogenously restricted the maximum regulatory boundary.[9] Consistent with our predictions, Pierce (2023) finds significant increases in the stock-picking ability of affected traders following restrictions, for example, around common insider trading events, such as earnings surprise announcements.

We extend our model to consider when agents are endowed with existing social networks. We show that when regulatory enforcement becomes sufficiently strong, agents' information sharing shifts away from their respective social networks and instead prompts the formation of more centralized and complex insider networks. In this context, the model generates an endogenous rise of intermediaries as a reaction to greater regulatory sophistication. Intermediaries in the core are responsible for

[7] Insider trading cases brought forth by the SEC can be found here.

[8] Analysis on the network of corporate insiders using reveal that insiders are tightly connected, and find evidence for information propagating through long chains within the network (Tamersoy et al., 2013).

[9] We consider a direct analog on how legal boundaries affect insider regulation in Section '6.1.

matching and transmitting information between a large mass of senders and receivers. Moreover, by extending its constituency, the core is able to adjust its flexibility to arbitrarily greater regulatory powers at a negligible cost. This suggests that in an environment where regulation becomes more stringent over time, the flexible core offers a dynamic form of flexibility as well.[10]

Our results imply that strengthened regulatory and legislative initiatives may trigger demand for, and therefore creation of, more sophisticated networks. As agents' typical channels through which to exploit inside information become too risky, intermediaries naturally arise to facilitate transmission between agents with greater flexibility and reach. In support of this, information intermediaries, such as expert network firms, have been, in the last decade, implicated directly and indirectly in a number of insider trading cases in the United States.[11] These firms are consulting agencies that specialize in connecting clients to experts spanning various sectors and fields. Indeed, legislative and regulatory actions have been claimed to be at least partly responsible for the growth of the expert network industry (Jeng (2013)), which according to some industry estimates, roughly doubled in size (by revenue) from 2012 to 2018. These firms have been found to offer discrete channel of information transmission and even insulate clients from legal trouble by obscuring whether clients know that information constitutes inside information.[12][13]

Finally, we explore how agents may achieve optimal transmission in a decentralized manner. We demonstrate that the optimal transmission strategy is implementable using simple rules, which replicate the transmission of insider information through paths of varying distance without any ex-post multilateral communication or coordination. Furthermore, we show that through decentralized transmission, insiders are

[10] In the US, enforcement indeed appears to have become stronger over time. For example, see Silvers (2016).

[11] See https://www.sec.gov/spotlight/insidertrading/cases.shtml for details on select cases involving expert networks.

[12] For example see SEC v. Longoria involving expert network firm, Primary Global Research (PGR). The complaint, which outlines how PGR employees "passed inside information" to clients, explains: "When soliciting consultants for PGR, [the employee] made clear that telephone conversations with PGR clients would not be monitored or recorded."

[13] In the monumental case of SAC Capital, the expert network firm had a compliance program put in place to insider trading, but was circumvented with ease. Per the SEC complaint: "Martoma and Gilman also took steps to conceal the true topic of their conversations from the expert network firm. For example, when Martoma scheduled a consultation with Gilman [...], Martoma reported to the expert network firm that the purpose of the call was 'Follow-up with Dr. Gilman: AAN Abstract Preview' even though [they] had discussed [insider information]."

able to further obfuscate information about the source of the tip, thereby increasing an investigation's burden of proof. When this translates into higher regulatory costs, it has the effect of constricting the regulatory boundary, enabling insiders to reap greater profits in equilibrium.

While our main application is in the context of insider trading networks, we believe that the model's insights apply to a broader set of applications. A pivotal feature of our model is that the regulator must map the path between the sender and the receiver in order to prosecute. We emphasize that this property crucially shapes agents' strategies for circumventing regulation. Long chains are essential and, furthermore, a cheap and effective method to increasing the cost incurred by regulators attempting to track transmissions. In this respect, our model is applicable to a broader set of economic problems on the regulation of transmission networks where regulatory actions require a high burden of proof, and also involve investigations that occur at the entity level. One application is money laundering and circumvention of capital controls. Money laundering operations commonly involve "layering" – a practice of transferring through numerous accounts – that obfuscates a fund's source from regulators.[14] The practice of layering is observed in other criminal networks (Jacopo, 2022). Similar challenges arise in the enforcement of capital controls. Notably, leaked documents referred to as the "Panama Papers," revealed an extensive network of off-shore financial intermediaries and shell companies that helped evade regulatory scrutiny dating back to the 1970s.[15] Our model also relates to the design of private transmission networks aiming to prevent external actors from unraveling messages. Our equilibrium network shows strong parallels to the operational design of tor networks, which use multiple intermediate nodes to obfuscate the link between end points of a transmission (Goldschlag et al., 1996; Dingledine et al., 2004).

2 Contribution and Related Literature

Our main application is on the regulation of insider trading ((DeMarzo et al., 1998; Acharya and Johnson, 2010)). This paper is the first to our knowledge to theoretically study the formation of insider networks. As in DeMarzo et al. (1998), our paper takes as given the objective of a regulator to detect and deter the sharing of insider information. We complement DeMarzo et al. (1998), which focuses on a regulator's

[14] See https://www.fincen.gov/history-anti-money-laundering-laws.
[15] See https://www.icij.org/investigations/panama-papers/.

choice of when to conduct an investigation, by studying the joint equilibrium determination of regulation, network formation, and information transmission. Importantly, in our setting, insiders are able to form sufficiently complex networks that allow them to circumvent regulation, albeit at a cost. Our theory makes two important departures from DeMarzo et al. (1998). First, DeMarzo et al. (1998) concludes that even if random investigation policy is allowed, a simple non-random enforcement policy is optimal. In our setting, enforcement policy is necessarily ambiguous (i.e. subject to randomness) due to the possibility of gaming by agents, which explains a long-standing policy stance of the SEC and other regulators. Second, regulators in DeMarzo et al. (1998) choose, in equilibrium, to "tolerate" smaller insider trading schemes and investigate those with larger profits, which maximizes its effect on curtailing insider trading volume while economizing on investigation costs. In contrast, in our model, regulation works by making the use of insider information via shorter chains costlier. Insiders face a tradeoff between transmitting through shorter chains, which is more likely to be prosecuted, and longer chains, which are safer but diminish profitability. Our results are consistent with empirical observations that a significant fraction of insider trading cases brought forth by the SEC involve short chains, and also sometimes accrue surprisingly small profits to insiders.

An extensive literature examines the diffusion of information through social networks in financial markets. Cohen et al. (2010) finds strong evidence of information diffusion through educational ties. Maggio et al. (2017) finds extensive evidence of information diffusion through broker networks. Ahern (2017) shows that a majority of prosecuted insider trading cases involve insider information being transferred through geographical, family, and social networks. An implication of our paper is that as regulatory pressures increase, insider trading activity migrates from existing networks to those that better insulate agents from detection and prosecution.

Our paper is related to the literature on information transmission in endogenous networks. Acemoglu et al. (2014) studies how information aggregation occurs through communication on endogenous social networks. Bloch and Dutta (2009) studies how communication networks with endogenous link strength bring rise to star networks. We make a unique contribution by studying the formation of information networks and its interaction with the regulatory environment.[16] We show that a core-periphery

[16] A few papers have studied the impact of regulation on networks in other contexts. For example, see Erol and Ordoñez (2017) and Erol (2017).

structure arises endogenously in insider networks, and furthermore show that a small number of agents act as intermediaries to facilitate information transmission. Our result also relates to bottlenecks and essential intermediaries which Manea (2018) takes as given.

Our insights are applicable to other settings in which agents use networks as a strategic tool for the transmission of information or goods in a game against an adversary. Agents committing money laundering may utilize a long chain of financial intermediaries in order to obfuscate the source and destination of money transfers. The model is relevant for studying networks for organized crime or terrorism in which agents form networks to conceal communication and money transfers. Our results are consistent with empirical studies that document the use of long intermediation chains in terrorist networks intended to conceal relationships and preserve secrecy (Krebs (2002)), as well as the emergence of core-periphery structures in transnational criminal networks (Williams (2001)). Finally, our paper contributes broadly to the literature on attack and defense in networks.[17]

3 Baseline Model of Network Formation

We begin by describing the baseline model with a discrete number of agents.

Agents. There are three distinct and finite sets of agents $A = S \cup I \cup R$: senders $s \in S$, receivers $r \in R$, and intermediaries $i \in I$. Senders are insiders who sometimes obtain inside information; receivers are traders with potentially the means to use inside information for profitable trading gains; intermediaries are agents who are able to form links with senders, receivers, and other intermediaries. In the baseline model, given our focus on the interplay between agents and the regulator, we assume that agents A are assumed to perfectly coordinate and make decisions as a single entity. [18]

Network formation and transmission. In the beginning of the model, A forms *links* $L \subset \{\{a, a'\} : a \in A \text{ and } a' \in I\}$ at cost $c(L)$, which are necessary for information transmission. A link between an intermediary and a non-intermediary costs η, and a link between any two intermediaries costs η'. The total cost $c(L)$ is additive

[17]For example, see Acemoglu et al. (2016), Dziubiński and Goyal (2017), Hoyer (2012), Haller (2016), and Hoyer and Jaegher (2016).

[18]This is akin to assuming that all costs and profits are shared equally between all agents in A. In Appendix B, we outline protocols that enable agents to transmit information and disseminate profits in a decentralized manner with limited communication and coordination.

over links. These links are assumed to represent trusted relationships between agents. After links are formed, each sender independently obtains distinct pieces of inside information with probability ζ. Let the subset of these senders be $\tilde{S} \subset S$. Nature also determines a receiver $r_s \in R$ for each $s \in \tilde{S}$, who is able to exploit s's information to implement profitable trading strategies. Hence, gains from inside information arise only if s is able to relay the information to r_s. For each $s \in \tilde{S}$, transmission is feasible along all paths in L that connect s and r_s through intermediaries, where a path for s is denoted $p_s = (s, i_1, i_2, ..., i_{\Delta_s}, r_s)$ and the set of transmission paths across $s \in \tilde{S}$ as p. We call Δ_s, the number of intermediaries between s and r, as the depth (or distance) of path p_s. For each $s \in \tilde{S}$, A chooses whether to transmit or not, and if so, the path p_s through which information is transmitted. Upon successful transmission, r_s uses the inside information to generate $\beta(\Delta_s)$ in trading profit, and a social externality cost of $\beta'(\Delta_s)$, where β and β' strictly decrease in Δ_s. We assume that $\beta(\Delta_s) - \beta'(\Delta_s) < 0$ for all Δ_s, such that insider trading is net costly. In Appendix A, we extend the model to allow for insiders to explicitly trade on financial markets.

Regulation and Enforcement. Insider trading imposes a negative social externality. There is a regulator G whose objective is to minimize social costs that arise from the exploitation of inside information. In the event that a receiver r_s trades using inside information, an investigation starts. For each investigation involving r_s, the regulator G sets a *regulatory bound* m_s, which determines the *maximum depth* of an investigation, and results in a cost $\kappa(m_s)$, where $\kappa(\underline{m}) = 0$ for some $\underline{m} \geq 1$, and κ is strictly increasing for all $m_s \geq \underline{m}$.[19] For simplicity, we assume that G's action set is restricted to $m_s \geq \underline{m}$. With slight abuse of notation, we use m to denote the set of m_s.

Investigations operate at the agent level. Specifically, an investigation begins with r_s and investigates the case sequentially along p_s, up to a maximum of m_s intermediaries on the path.[20] If $m_s \geq \Delta_s$, an investigation is said to be successful in revealing the entire path of transmission. If investigation succeeds, the regulator imposes a punishment $\gamma(\Delta_s)$ on A, and recovers $\gamma'(\Delta_s)$, where γ, γ' strictly decrease

[19]In effect, we also abstract from the decision of whether or not to investigate a trade, since simple investigations are not costly. Several past studies explore this as key component (e.g. DeMarzo et al. (1998)).

[20]Investigations typically triggered when regulators monitoring financial markets detect suspicious trading activity. Hence, we consider investigations that begin with r_s for expositional purposes. Technically, we could also allow for investigations to start with s, or also work from both ends of a path p_s. In either case, it is sufficient that the regulator is able to identify either the r_s or s.

in Δ_s. Illustrative examples of successful and failed investigations are in Figures 1 and 2.

Figure 1: Successful search by the regulator

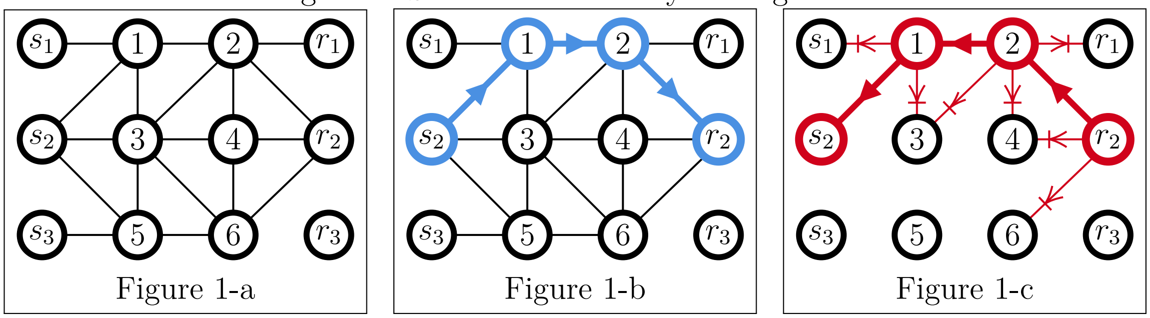


Figure 1 illustrates the game. The network available is shown in Figure 1-a. There are many paths that the agents can utilize. For example, $s \to 3 \to 4 \to r$ is a path of length 3; $s \to 3 \to 5 \to 6 \to 4 \to 2 \to r$ is a path of length 6. Figure 1-b illustrates the strategy of choosing the path $s \to 1 \to 2 \to r$. Figure 1-c illustrates the strategy of the regulator choosing some $m \geq 3$. Given m, the regulator can hold investigations for m steps until evidence is found. In the first round, r and all of its incoming links are inspected: $2 \to r$, $4 \to r$, and $6 \to r$. Upon the investigation, the regulator finds that the information has been sent by 2. In the second round, the regulator investigates 2 and all of its incoming links, $1 \to 2$, $3 \to 2$, and $4 \to 2$. The regulator discovers that information has been sent by 1. In the third round, the regulator inspects 1 and all of its incoming links: $s \to 1$ and $3 \to r$. The regulator finds definitive evidence that information was transmitted from s to r, and can inflict a punishment.

Timing and payoffs. The game is between A, who forms a network consisting of links L and picks transmission paths p, and the regulator G, who chooses regulatory bounds m. A and G do not observe each others' actions.[21] Denote $S^* \subset \tilde{S}$ the set of senders whose information A chooses to transmit, and ι_s the indicator for $m_s \geq \Delta_s$. The payoff functions in the corresponding game are

$$V_A(L,p,m) = -c(L) + \mathbb{E}_{\tilde{S}}\Big[\sum_{s\in S^*}(\beta(\Delta_s) - \iota_s\gamma(\Delta_s))\Big]$$

$$V_G(L,p,m) = -\sum_{s\in S}\kappa(m_s) + \mathbb{E}_{\tilde{S}}\Big[\sum_{s\in S^*}(-\beta'(\Delta_s) + \iota_s\gamma'(\Delta_s))\Big].$$

Notice G's largest possible gain from an investigation that succeeds upon reaching depth m_s is $\gamma'(m_s) - \kappa(m_s)$. This is a strictly decreasing function of m_s and positive at zero. Define

$$\overline{m} = \sup\{m_s \in \mathbb{N} : \gamma'(m_s) - \kappa(m_s) \geq 0\}$$

[21] Thus the game is strategically equivalent to a simultaneous move game where actions are (L,p) and (m).

Figure 2: Failed search by the regulator

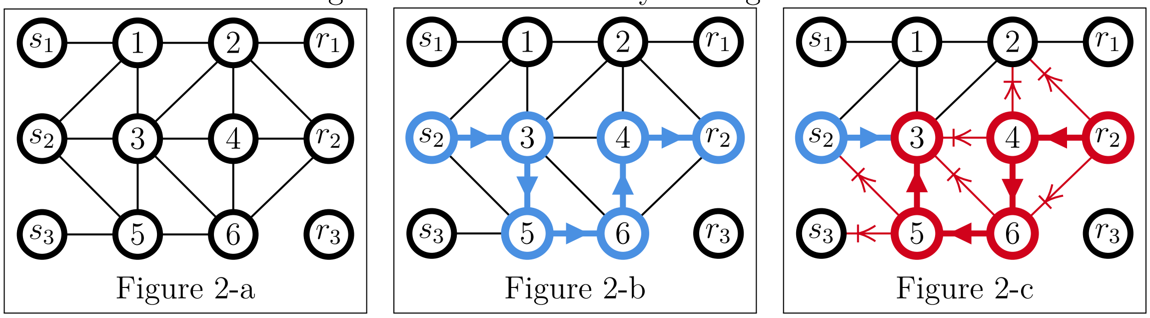


Figure 2 illustrates the game with failed search. Figure 2-a is the network. Figure 2-b illustrates the transmission strategy employed by the agents: $s \to 3 \to 5 \to 6 \to 4 \to r$. This is a path of length 5. Figure 2-c illustrates the search upon the regulator choosing $m = 4$, the maximum number of rounds for search. First, r and all of its incoming links are inspected: $2 \to r$, $4 \to r$, and $6 \to r$. Upon the investigation, the regulator finds that the information has been sent by 4. Then 4 and all of its incoming links are inspected: $3 \to 4$ and $6 \to 4$. Upon the investigation, the regulator finds that the information has been sent by 6. The search goes on this way. In the last round, upon the inspection of 5 and all of its links $r \to 5$ and $3 \to 5$, the regulator finds that the information has been relayed by 3. However, the search fails to identify the entire transmission path, and insiders are not prosecuted.

Note $m_s > \overline{m}$ is strictly dominated by $m_s - 1$ so regulator never uses an depth $m_s > \overline{m}$.

Our focus is Nash equilibria wherein the choice of the network is a pure strategy, which we shortly call *equilibria*. We assume $\overline{m} < \infty$ and $\zeta\beta(\overline{m}+1) - \eta > 0$ so that pure strategy Nash equilibrium networks exist.

4 Equilibrium Analysis

4.1 The Virtue of Regulatory Ambiguity

As the network is a pure strategy, we can lay out necessary conditions for regulation and transmission strategies as partial equilibrium properties for a given network. Let the set of paths between s and r_s in L be denoted

$$P(s, r_s, L).$$

We show that the regulator employs a form of regulatory ambiguity in equilibrium:

Theorem 1. ***(Regulatory Ambiguity)*** *Let L be the network, and suppose that $s \in \tilde{S}$. Consider the equilibrium transmission and regulation strategies regarding s. If s and r_s are connected by at least one path of distance at least $\overline{m}+1$ and one path of distance between $\underline{m}+1$ and $\overline{m}$, then the regulator plays a mixed strategy. In* *particular, the support of G's strategy is*

$$\{\Delta(p) : p \in P(s, r_s, L),\ \underline{m} \leq \Delta(p) \leq \overline{m}\}$$

The distances of paths in the support of A's strategy is

$$\{\Delta(p) : p \in P(s, r_s, L),\ \underline{m} + 1 \leq \Delta(p) \leq \overline{m}\} \cup \{\overline{\Delta}(s, r_s, L)\},$$

where $\overline{\Delta}(s, r_s, L) := \min\{\Delta(p) : p \in P(s, r_s, L),\ \overline{m} + 1 \leq \Delta(p)\}\}$.

The above theorem formalizes the potential need for the regulator to employ regulatory ambiguity, in the form of a mixed strategy in regulatory bound. For any fixed investigation depth m, A best-responds to G with a path of higher distance than G's investigation depth. In turn, G best-responds to A by matching the distance of A's transmission path. This goes up to $\overline{m}$, at which point G best-responds with a low depth $\underline{m}$. The best response cycle ensures that the equilibrium must be in mixed strategies and all of the depths in the range are played with positive probability.[22][23]

Incurring a high enforcement cost is only justified conditional on detecting transmission or deterrence. When agents can anticipate high regulatory oversight, information is transmitted at long distances to circumvent investigations. At the same time, low regulatory oversight is justified if regulation is too costly. In the latter case, however, agents send and receive information at short distance, which could be detected with high oversight. As a consequence, the regulator must employ a mixed strategy with respect to the enforcement intensity in equilibrium. This formalizes the regulator's need to employ ambiguity in the form of a mixed enforcement strategy. Regulatory ambiguity arises when agents, in equilibrium, acquire access to a network that is able to successfully match senders to receivers through multiple paths of differing lengths.

This rationalizes a common strategy implemented and advocated by regulators to maintain vagueness in what constitutes illegal insider trading activity. For instance,

[22]Our result on regulatory ambiguity is robust to incomplete information in the following sense. Suppose that the regulator has two types, a high and low maximum regulatory bound, $\overline{m}^h, \overline{m}^l$. If the likelihood of the high type is sufficiently high, then, for any fixed strategy m^h chosen by the high type regulator, agents best-respond with a transmission path of $m^h + 1$, since this would always circumvent regulation. Following the provided argument, a best-response cycle would again arise.

[23]If insider profits could be scaled by sharing with multiple receivers, the optimal transmission strategy would entail a multi-path transmission strategy that extracted maximal information rents from trade. Without spillovers between investigations (that is, progress in one investigation facilitating others with involving duplicate nodes), then the strategy across path lengths for a given sender would not be consequential. However, if spillovers arise, then synchronizing the strategy for a given sender may arise.

legal boundaries of insider trading in the US are ambiguous and often criticized for being unclear. As a consequence, insider trading prosecution cases ultimately depend on courts to determine whether the nature of the shared information is in fact insider information, i.e. material and non-public, and whether the transfer of information is illegal, e.g. a violation of fiduciary duty. This flexibility in what constitutes illegal insider information is often argued by enforcement officers of the SEC as what allows for successful prosecution and even deterrence. A quote by Arthur Levitt, former chairman of the SEC, captures this sentiment:

> If the SEC had an option as to whether they wanted to have greater specificity and the Justice Department as well, they'd say 'Absolutely not' because greater specificity would give the legal fraternity various ways of getting around those specifics. They want these laws purposely vague to see to it they have the maximum leverage in terms of bringing cases.

It is worth noting that agents always transmit information as a consequence of $\overline{m} < \infty$. Marginal improvements to the regulator's competitive advantage, such as reducing its costs κ or increasing punishment γ does not fundamentally deter agents from transmitting information. Instead, these marginally improve the regulator's ability to operate investigations, thereby reducing social costs as agents are induced to transmit through longer paths.

4.2 The Formation of Insider Networks

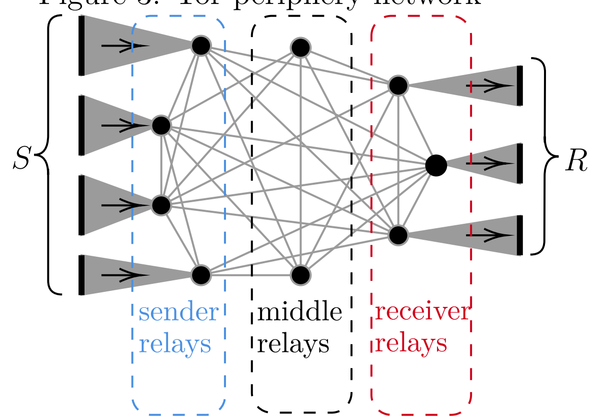
With the characterization of the optimal transmission strategy for a given network, we consider agents' network formation problem. We begin by noting several observations that help determine desirable properties of the equilibrium network. First, recall that the realizations of a sender and receiver pair occur after the formation of the network. This implies that if link costs are not prohibitively high, agents A prefer a network in which there exists a path between any $s \in S$ and $r \in R$, in order to ensure that inside information can be exploited.

As a starting point, consider the structure of a network that can efficiently propagate information between senders and receivers with the fewest number of links. A strong candidate is a *hub-spoke* network, which takes the form of a star-shaped network with a single hub node that is linked directly to all spoke nodes. This network emerges more generally, in the context of communication networks due to its scalability.

Agents must also anticipate the threat of regulation. As shown in Theorem 1, agents' optimal transmission strategy requires paths of varying degrees of depth. Notably, in the case of the hub-spoke network, all transmissions would be caught in investigations, as $\Delta_s = 1$. Thus, a desirable feature of the network is one that offers both sufficient obfuscation, i.e. paths with high depth, and flexibility in the available transmission paths between senders and receivers.

Consider a *core-periphery* network, which is similar to hub-spoke, but consists of a group of nodes (the "core") in place of the hub, and nodes (the "periphery") connected to the core in place of spokes. In addition to inheriting desirable features of a hub-spoke, a core-periphery may also extend the distance of paths within the core, thereby facilitating greater obfuscation. The need for flexibility in the amount of obfuscation inside the core necessitates a specific type of core. Consider a *tor-periphery* network topology, illustrated in Figure 3, and defined below:[24]

Figure 3: Tor-periphery network



Definition. For any $k \geq \overline{m} + 1$, *a k-tor-periphery* network is defined as follows.

- There is k number of agents called the *tor*, denoted $T \subset A$.
  - Agents in the tor are called *relays*. There are three types of relays:
    - Sender relays: every link of each sender relay is with S or T
    - Receiver relays: every link of each receiver relay is with R or T
    - Middle relays: every link of each middle relay is with T

[24] The name comes its close resemblance to The Onion Router (Tor) architecture, which is designed to solve related issues with regard to internet privacy.

  - Tor provides *flexible obfuscation*: for every sender and receiver relay pair, there are paths of all distances[25] from $\underline{m}-1$ to $\overline{m}-1$ inside T that connect the pair.

- Every sender and receiver outside the tor is in the *periphery*.

  - Each sender in the periphery has exactly one link a sender relay
  - Each receiver in the periphery has exactly one link with a receiver relay

- Every link includes at least one relay.

We formally show that tor-periphery networks describe approximate equilibrium networks. Call a strategy $\left(L^*, \sigma_p^*, \sigma_m^*\right)$ an ϵ*-equilibrium* if for all L, p, m,

$$
\begin{aligned}
V_A(L^*, \sigma_p^*, \sigma_m^*) &\geq V_A(L, p, \sigma_m^*) - \epsilon|A| \\
V_A(L^*, \sigma_p^*, \sigma_m^*) &\geq V_A(L^*, p, \sigma_m^*) \\
V_G(L^*, \sigma_p^*, \sigma_m^*) &\geq V_G(L^*, \sigma_p^*, m).
\end{aligned}
$$

The first condition states that the average payoff of agents can not be improved by more than ϵ by deviating from the network and the transmission strategy. The second condition, however, states that a deviation from the transmission strategy alone can not improve agents' payoffs at all. Therefore, there is a sense in which the ϵ term in the first condition is due to the cost of links.

Theorem 2. *For any $k > \overline{m}$ and $\epsilon > 0$, there exists $n_{k,\epsilon}^*$ such that if $|S|, |R| > n_{k,\epsilon}^*$ then any k-tor-periphery network wherein $T \subset I$ is an ϵ-equilibrium network.*

Theorem 2 highlights that a small number of intermediaries can take on the role of intermediation on behalf of a disproportionately larger economy. In addition to retaining some properties of a hub-spoke to offer economies of scale in transmission, tor-periphery provides the necessary depth and flexibility for obfuscation to face regulatory ambiguity outlined in Theorem 1. Moreover, these costs become vanishingly small relative cost of forming links as the number of senders and receivers increase. We explore this crucial feature of the network in the next section.

[25]In general, a path in a simple network is defined as an ordered sequence of distinct nodes wherein each consecutive pair of nodes in the sequence is linked in the network. The distance of a path is defined as the number of nodes on it, other than the first and the last node.

5 The Emergence of Intermediaries

5.1 The Case for a Continuum Economy

A key interest is to consider equilibrium dynamics with a large number of agents. In this section, we map the discrete environment to a setting with a continuum of agents. Before doing so, we briefly discuss several dimensions to consider as we move to the continuum case.

In our discrete model, the strategies employed by agents A and regulator G are exact best replies. We are able to characterize an equilibrium network by making use of the ϵ error-term in Theorem 2. Pinning down the exact optimal topology of links *inside the core* of the network is a non-trivial problem, but in important respects are inconsequential in a "macro-economic" sense. In particular, *the* striking feature of the ϵ-equilibrium network is outsized role that the set of intermediaries in the core plays to facilitate insider trading, relative to the cost of facilitating information transmission. This arises because the optimal $\overline{m}$, which determines the regulatory bound for any individual case, is invariant with respect to the number of agents. As the number of agents increase, the costs of forming the core make up a vanishing part of the total link cost. An implication is that the size of I can be kept bounded as the sizes S and R grow unboundedly.

A valid question is on the sensitivity of this feature to assumptions that might offer the network with scalability. For one, transmitting information is costless, and this allows agents to freely scale the number of transmissions. If transmitting information is instead assumed to be costly, costs associated transmission would magnify with the number of agents. This is, however, without loss of generality – incorporating transmission costs would amount to reducing the per-transmission gain $\beta(\Delta_s)$ by an additional factor of distance Δ_s. Second, link costs are assumed to be linear and additive, which allows an individual agent to form a large number of links. If intermediaries instead face convex costs with respect to links, it could become too expensive a highly connected intermediary to take on more links. In this case, I would also needs to grow unboundedly, but this would still be at a rate smaller than S and R. In this sense, the additive cost of links is conducive to scalability, but is also not crucial.[26]

[26] A similar argument holds for convexity in transmission costs.

Thus, we view this feature, in which the number of intermediaries per sender and per receiver that can enable sufficient obfuscation to become vanishingly small in large populations, as a defining and robust insight. We build on this aspect foreshadowed in Theorem 2 by modifying the model to a continuum economy. As will be shown, the continuum approach offers tractability and starkly illuminates the outsized role that a select group of agents play to facilitate insider trading.

5.2 Continuum Baseline Model

We make several modifications in order to extrapolate Theorem 2 to a setting with infinite A. We first expand the set of senders and receivers. In particular, there is $\mu_S = \lambda(S)$ mass of senders and $\mu_R = \lambda(R)$ mass of receivers, in Lebesgue measure λ. The costs and benefits of A and G, other than the link cost, scale with population size as ζ fraction of S receive inside information, and payoffs V_A, V_G remain the same after replacing sums with integrals.

The main non-trivial aspect to modify is the cost of links. Proper accounting of the cost of links in a network on a continuum population needs significant care. In particular, uncountable zero-measure sets, such as Cantor sets, can potentially be exploited to lower network formation costs that are incongruent with the limit of any discrete case. For this reason, we impose that there is a finite *number* of intermediaries in I. With finite I and no links between non-intermediaries, we are able to account for each link accurately and once by indexing them with intermediaries. This assumed disproportion between the size of intermediaries and size of non-intermediaries is proven to be innocuous by Theorem 2.

An (undirected) *network* L is now defined as a (symmetric) measurable subset of A^2. Let $\mu_i = \lambda(L_i)$ be Lebesgue measure of $L_i = \{a : \{a, i\} \in L\}$, agents linked to $i \in I$. These cost $\eta\mu_i$. The costs of links within intermediaries is zero as the set I^2 is finite. Hence, the total cost of the network is given by

$$c(L) = \eta \sum_{i \in I} \mu_i.$$

This reflects what we observe in Theorem 2. The cost of links inside the core have vanishing relevance in a growing population.

We modify the definition of a *tor-periphery* network by changing each instance of "every" in the definition into "almost every," with respect to Lebesque measure λ. By virtue of the continuum, we obtain a characterization result for the (exact) equilibrium in Theorem 3 as opposed to the sufficient condition for approximate equilibrium in Theorem 2.

Theorem 3. ***(Characterization of equilibrium networks)*** *A network is an equilibrium network if and only if it is a k-tor-periphery network with $T \subset I$.*

Admittedly, the equilibrium in continuum case does not put much discipline on the inner structure of the core, beyond flexibility for obfuscation. As such, it is possible, if not probable, that the continuum case does not describe the limit of the *exact* structure of connections inside the core of a discrete equilibrium. We view this as a *strength*, not a weakness. Our results show that the exact structure of links inside the core bears little consequence for aggregate outcomes, as long as it facilitates flexible obfuscation – an insight that is harder to appreciate when trying to identify "who should link who" in the (intractable) discrete case. For the remainder of the paper, we continue with the continuum model, which allows us to sharply characterize the dynamics between the agents A and regulator G. We acknowledge that this comes at the cost of abstracting over potentially interesting features that may emerge in the exact network structure of the core in a discrete environment.

5.3 Emergence of intermediaries out of non-intermediaries

So far, we considered an environment in which a set of intermediaries play a vital role in forming links and transmitting information between senders and receivers. However, a distinct feature in the context of insider trading is the emergence of intermediaries who specialize in helping insiders exploit inside information outside of regulatory oversight. To consider the endogenous rise of intermediation, we now extend the continuum baseline by (i) allowing links to be formed among all agents, and (ii) dropping intermediaries from the environment, i.e. setting $I = \emptyset$.

In the continuum baseline, I is assumed to be finite in order to rule out the possibility of zero measure uncountable sets from making up the core. In order to maintain an analog assumption, we assume sparseness. Formally, a network L is called *sparse* if only a finite number of agents have an infinite *number* of nodes, in counting measure. In sparse networks, there is a natural non-abusive method to count the cost of links. Let F^* be the finite set of agents with infinite degree, η denote the cost of each link, and $d[a, Z, L]$ denote the number of links that $a \in A \backslash F^*$ has with members with $Z \subset A$ in network L. Then the cost of links is

$$c(L) = \int_{A \backslash F^*} \left(\frac{1}{2} d[a, A \backslash F^*, L] + d[a, F^*, L] \right) \eta \mathtt{d} a$$

That is, each link within $A \backslash F^*$ is counted twice, hence divided by 2. Each link between $A \backslash F^*$ and F^* is counted one. Links inside the zero measure set F^* have 0 cost. We obtain the following result:

Theorem 4. ***(Endogenous intermediaries)*** *Tor-periphery networks are equilibrium networks.*

A small set of agents endogenously specialize in providing flexible channels of information transmission and ultimately intermediate almost every (in λ) information transmission between the set of senders and receivers. This is, agents provide intermediation for other agents beyond the purpose of "scratching each other's back." Middlemen are necessary to tunnel and obfuscate transmission, and to avoid punishment.

5.4 The rise of intermediaries against social networks

Interestingly, the emergence of information intermediaries draws striking parallel to the rise of consultancy firms that have played an outsized role in recent years. While information intermediaries are legal, these consultancy firms have been implicated in a number of insider trading cases in the past decade. A large fraction of these firms is commonly referred to as expert network firms, which specialize in connecting clients to experts in various fields ranging from technology, medicine, healthcare, energy, and even economics.[27] What triggers the rise of such intermediaries?

Suppose that the agents are endowed with pre-existing social networks. Transmission over social networks is often uncoordinated and casual. There is no legal risk, but information is not kept confidential and diffuses to the market. This does not help to beat the market. Alternatively, social networks among close connections can be used for coordinated transmission but only across short distances. Coordinating long chains with secrecy and trust is not possible on casual social networks. On the other hand, transmission over short distances is easy to document by prosecutors after a short search. The legal risk boils down primarily to detection risk.

[27] https://www.bloomberg.com/news/articles/2018-02-28/investors-are-paying-1-300-per-hour-for-expert-chats

We extend the baseline as follows. Each sender s has a given corresponding "friend and family" $f_s \in T$. Each pair (s, f_s) share their payoffs equally. The pair can choose ex-ante to use their social network connection to gain $\beta(0)$ by direct transmission, should the opportunity arise. If they choose so, they commit to each other, and are excluded from the insider network. Alternatively, they can join an insider network and commit to equal sharing across all insiders, as in baseline. In either case, there is δ probability of an ex-post investigation where $\delta\beta' - \beta > 0$.

We show that there exists a threshold δ^*, above which agents migrate their insider activity to a tor-periphery insider network:

Theorem 5. ***(Social and professional networks)*** *There exists δ^* such that if $\delta < \delta^*$, all agents use social networks. If $\delta > \delta^*$, all agents switch to an insider networks.*

Theorem 5 forms the basis for the potential link between tightening regulation and the rise of information intermediaries. Major shifts in the regulatory framework in the early 2000s developed through Regulation Fair Disclosure (Reg FD), which was promoted by the SEC in 2000, and the Global Analyst Research Settlements, which was an enforcement agreement reached between the SEC, other regulatory agencies, and the ten largest investment firms in the US. Together, regulation focused on tightening governance on information disclosure by public companies, and imposing controls on the leakage of material non-public information through financial intermediaries, such as research analysts and broker-dealers. What followed was dramatic growth in the expert network industry.

This relation between tighter regulatory control and the rise of information intermediation is also observed in the official sector. In 2012, the US Congress passed the Stock Trading on Congressional Knowledge Act (STOCK Act). The general intent of the law was to prevent government officials and employees from exploiting privileged access to non-public information that could potentially be used for financial gains. Following the passage of the STOCK Act, information intermediaries emerged in the form of political intelligence firms, which specialize in connecting clients to experts in areas of policy, law, and regulation.

A key takeaway from our model is that while these actions may succeed at displacing existing channels of information diffusion, they may prompt the formation of networks that undermine the main objective to improve market integrity. Furthermore, by providing a discrete channel of information transmission, these firms can also insulate clients from legal trouble, as the current regulatory framework requires proof of knowledge that the information constitutes inside information. A particularly eye-opening case is USA v. Blaszczak, in which defendants were convicted of selling and trading on political intelligence. In a divisive decision, courts ruled in favor of the defendants. The dissenting judge expressed concern over the impact of the ruling on its impact on insider trading:[28]

> The majority opinion effectively permits sophisticated insiders to leverage their access to confidential government information and sell it to the highest bidders – in this case, hedge funds that used the confidential information to make millions shorting the stocks of public companies affected by CMS's regulations.

5.5 Evolution of intermediaries in face of changing regulation

Theorem 5 highlights how tightening regulation can prompt the formation of insider networks in which bulk of information is intermediated by a small core. Once an insider network is established, how does it adjust to further tightening of the regulatory environment? Our model presents one more stark insight. As a corollary of Theorems 2 and 3 , the tor can adapt to rising regulation by adding more intermediaries. New members are assigned to be middle relays, and need at most $\overline{m}+1$ number of links to pre-existing relays in order to provide additional flexibility to the entire ecosystem of insiders. As new relays do not need to be sender or receiver relays, the bulk of the network cost is already paid up.

Improving the extent of potential obfuscation in face of tightening regulation (maximal depth $\overline{m}$ or detection δ) needs vanishingly small cost, relative to regulators' costs. In this sense, there is no level of regulation that the agents can not adjust to, as long as $\overline{m} < \infty$ and $\zeta\beta(\overline{m}+1) - \eta > 0$. If the first is reversed by a downward shift in costs κ, Theorem 1 no longer holds. The "winner" of the war-of-attrition shifts from A to G. If the first condition holds but the second fails, even though Theorem 1 holds, the network cost does not support the continuation payoffs. In either case, regulation becomes more *effective*: there is a positive probability of not transmitting information.

[28]Court ruling can be found here.

6 Extensions and Robustness

6.1 Legal Boundaries

It is worthwhile highlighting how our setting also offers a foundation for laws that may be deliberately set broadly so as to avoid gaming by agents. In our main setting, the regulator is able to punish agents as long as an investigation maps the transmission path between the sender and the receiver. Alternatively, suppose prior to information transmission, lawmakers select a boundary strategy b, which determines the maximum path length between a sender and receiver that constitutes illegal insider information if used for financial gains. For instance, if $\Delta_s \leq b$, transmission may be regarded as a deliberate transfer of information intended for illegal profits; if $\Delta_s > b$, the communication between the sender and receiver may be deemed too distant to constitute illegal activity.

Correspondingly, suppose that any given b is associated with a cost $\beta(b)$, where $\beta(b)$ is a strictly increasing function associated with the social cost of violating of investors' civil liberties and privacy. This reflects the idea that the legal boundary b confines the regulator's ability to explore whether illegal insider trading occurred. For example, a regulator may require authorization from a judge to search, confiscate, and analyze evidence. The scope of any particular investigation would then be limited to the legal boundary b. For simplicity, we suppose that $\kappa(m) = 0$ for any m, but the set of feasible m is bounded above by b. Accordingly, the regulator would set m to equal b.

It is straightforward to see how the arguments underpinning Theorem 1 may carry forward. As long as agents have sufficiently complex networks that facilitate long transmission paths, lawmakers' equilibrium boundary strategy must be a mixed strategy over a set $[\underline{b}, \overline{b}]$, for some thresholds $\underline{b}, \overline{b}$, where $\beta(\underline{b}) = 0$, and $\beta(\overline{b}) \leq B < \beta(\overline{b} + 1)$.

Given this interpretation, Theorem 1 rationalizes a common practice of maintaining vagueness in what constitutes illegal insider trading activity, and instead rely on the judgment of courts on a case-by-case basis. A corollary is that any shock to the legal framework, which increases the costs associated with prosecuting insiders using longer chains necessarily raises the profitability of insider trading. As a direct test of this prediction, Pierce (2023) finds decisive evidence of this – following New York Second Circuit ruling on US v. Newman, which raised the burden of proof for punishing traders with "remote" links to the source, the trading performance of traders in the Second Circuit of *Second Circuit firms* significantly improved.

6.2 Link-costs of investigations

Throughout the paper, the primary cost of regulation arose from expanding the perimeter of an investigation at the node level. In principle, this would require an investigation to comb through all interactions of a subject to identify the transmission of information. Naturally, doing so could result in costs proportional to the number of links of the subject. We briefly discuss how our framework can accommodate these other forms of costs.

Consider the interpretation in which $\kappa(m)$ represents an upfront "infrastructure" cost for that bounds the maximum depth/distance of an investigation. One can think of node-level cost as arising from various issues, including political or legal costs. For example, the regulator may face non-pecuniary costs arising from requiring greater societal tolerance of privacy intrusion. In the presence of link-level costs, a similar upfront cost could be imposed, which determines the maximum mass of links m' that can be investigated. Link-level costs could represent logistical costs with allocating resources to an investigation. We can extend the baseline to introduce this cost, $\kappa'(m')$. The total upfront cost is now $\kappa(m)$, which represents the node cost, and $\kappa'(m')$, which represents the link cost. The investigation fails if either budget is spent before the investigation reaches the sender with surety. So given the transmission path

$$(r_s, i_1, i_2, ..., i_{\Delta_s}, s)$$

the investigation is successful if and only if $m_s \geq \Delta_s$ and

$$m'_s \geq \sum_{k=1}^{\Delta_s} \lambda(L_{i_k})$$

Similar to $\overline{m}$, define $\overline{m}'$

$$\overline{m}' = \sup\{m \in \mathbb{N} : \gamma'(m) - \kappa\,(m) - \kappa'(\mu_S + \mu_R) \geq 0\}$$

Under $\overline{m}' < \infty$ and $\zeta\beta(\overline{m}' + 1) - \eta > 0$ all $(\overline{m}' + 1)$-tor-periphery networks with $T \subset I$ are equilibrium networks.

As a final note, we can use this framework to consider an alternative environment, in which for any given r_s, there are multiple other receivers $r \in R$ who are indistinguishable from r_s. In this case, the regulator's cost would be modified such that the upfront costs would increase by a scalar representing the number of receivers suspected of irregular trading.

6.3 Direction of investigation

Our preferred narrative is that investigations start with either a sender or receiver, who is suspected of illegal activity. However, our setting allows for investigations to start at either end of a transmission path, depending on the monitoring technologies deployed. We outline how our results carry over with a modification.

Suppose only traders are observed. Then A can use pure strategies for transmission at any pair, as long as the combined probabilities on path distances conditional on any given trader correspond to probabilities in the baseline equilibrium mixed strategy. This is, flexibility is now needed only at each trader, not at each pair. Consequently, almost every pair must be connected with one path that has distance among $\underline{m}+1$ to $\overline{m}+1$. Conditional on any trader, the measure of senders with each corresponding path depth must be selected in accordance so as to add up to the baseline equilibrium probability for each path distance. Furthermore, the equilibrium network is still given by tor-periphery, with an appropriately modified flexible obfuscation condition.

7 Conclusion

In this paper, we study a model of endogenous formation of networks over which agents transmit information under regulation. In equilibrium, the regulator implements regulatory ambiguity that induces agents to take greater risks in information transmission. Agents adapt to regulation by forming a flexible network with a core-periphery structure, which endows agents with the option to transmit information through various paths of differing length.

We show how the core represents the endogenous rise of information intermediaries. A small set of agents that form the core of the network intermediate information between potential senders, i.e. insiders, and receivers, i.e. those that seek to exploit information. In an extension, we show that tightening regulation can trigger agents to migrate transmission activity from social networks to an insider network. We draw parallels to the recent growth of the expert network and political intelligence industry following stricter regulation regarding disclosure and insider trading. The surge of information intermediaries suggest that rather than curtailing insider trading, market participants may have adapted by developing alternative and more complex channels through which insider information is shared and exploited.

As a final note, we believe that our setting is applicable to a broader set of problems. In particular, the model can be used to understand network design problems, in which agents want to transmit messages or goods, but must combat a strategic actor (as in our case) or exogenous risks. Many networks involving communication or information sharing require achieving a sufficient level of security and privacy. An efficient network entails safeguarding the anonymity of messages from a malicious attacker while economizing on the cost of building and using the network. The model can be extended to study trading networks, in which agents prefer trading in proximity, but face counterparty risk. In particular, we highlight potential benefits of having a core-periphery structure that allows for intermediaries to flexibly re-direct flow between counterparties. We leave these applications for future research.

References

Acemoglu, Daron, Azarakhsh Malekian, and Asu Ozdaglar, "Network security and contagion," *Journal of Economic Theory*, 2016, *166*, 536–585.

_ **, Kostas Bimpikis, and Asuman Ozdaglar**, "Dynamics of information exchange in endogenous social networks," *Theoretical Economics*, 2014, *9* (1), 41–97.

Acharya, Viral V and Timothy C Johnson, "More insiders, more insider trading: Evidence from private-equity buyouts," *Journal of Financial Economics*, 2010, *98* (3), 500–523.

Ahern, Kenneth R, "Information networks: Evidence from illegal insider trading tips," *Journal of Financial Economics*, 2017, *125* (1), 26–47.

Bloch, Francis and Bhaskar Dutta, "Communication networks with endogenous link strength," *Games and Economic Behavior*, 2009, *66* (1), 39–56.

Cohen, Lauren, Andrea Frazzini, and Christopher Malloy, "Sell-side school ties," *The Journal of Finance*, 2010, *65* (4), 1409–1437.

DeMarzo, Peter M, Michael J Fishman, and Kathleen M Hagerty, "The optimal enforcement of insider trading regulations," *Journal of Political Economy*, 1998, *106* (3), 602–632.

Dingledine, Roger, Nick Mathewson, Paul F Syverson et al., "Tor: The second-generation onion router.," in "USENIX security symposium," Vol. 4 2004, pp. 303–320.

Dziubiński, Marcin and Sanjeev Goyal, "How do you defend a network?," *Theoretical Economics*, 2017, *12* (1), 331–376.

Erol, Selman, "Network hazard and bailouts," 2017.

_ **and Guillermo Ordoñez**, "Network reactions to banking regulations," *Journal of Monetary Economics*, 2017, *89*, 51–67.

Galeotti, Andrea and Sanjeev Goyal, "The law of the few," *American Economic Review*, 2010, *100* (4), 1468–92.

Glazer, Jacob and Ariel Rubinstein, "Complex questionnaires," *Econometrica*, 2014, *82* (4), 1529–1541.

Gofman, Michael, "A network-based analysis of over-the-counter markets," in "AFA 2012 Chicago meetings paper" 2011.

Goldschlag, David M, Michael G Reed, and Paul F Syverson, "Hiding routing information," in "International workshop on information hiding" Springer 1996, pp. 137–150.

Greenwood, Robin, Jeremy C Stein, Samuel G Hanson, and Adi Sunderam, "Strengthening and streamlining bank capital regulation," *Brookings Papers on Economic Activity*, 2017, *2017* (2), 479–565.

Haller, Hans, "Network vulnerability: a designer-disruptor game," 2016.

Hoyer, Britta, "Network disruption and the common enemy effect," *Discussion Paper Series/Tjalling C. Koopmans Research Institute*, 2012, *12* (06).

_ **and Kris De Jaegher**, "Strategic network disruption and defense," *Journal of Public Economic Theory*, 2016, *18* (5), 802–830.

Jacopo, Costa, "The nexus between corruption and money laundering: deconstructing the Toledo-Odebrecht network in Peru," *Trends in Organized Crime*, 2022, pp. 1–22.

Jeng, Daniel, "Expert networks and insider trading: An introduction and recommendation," *Review of Banking and Financial Law*, 2013, *32* (2), 245–264.

Krebs, Valdis, "Uncloaking terrorist networks," *First Monday*, 2002, *7* (4).

Maggio, Marco Di, Francesco Franzoni, Amir Kermani, and Carlo Sommavilla, "The relevance of broker networks for information diffusion in the stock market," 2017.

Manea, Mihai, "Bottleneck links, essential intermediaries, and competing paths of diffusion in networks," 2018.

Pierce, Andrew T, "Capital-market effects of tipper-tippee insider trading law: Evidence from the Newman ruling," *Journal of Accounting and Economics*, 2023, p. 101639.

Silvers, Roger, "The valuation impact of SEC enforcement actions on nontarget foreign firms," *Journal of Accounting Research*, 2016, *54* (1), 187–234.

Tamersoy, Acar, Bo Xie, Stephen L Lenkey, Bryan R Routledge, Duen Horng Chau, and Shamkant B Navathe, "Inside insider trading: Patterns & discoveries from a large scale exploratory analysis," 2013, pp. 797–804.

Tsebelis, George, "The abuse of probability in political analysis: The Robinson Crusoe fallacy," *American Political Science Review*, 1989, *83* (1), 77–91.

Williams, Phil, "Transnational criminal networks," *Networks and netwars: The future of terror, crime, and militancy*, 2001, *1382*, 61.

A Insider Trading in Financial Markets

In this section, we extend the model to allow for insiders to trade directly in financial markets, in effect endogenizing $\beta(\Delta_s)$ and $\gamma(\Delta_s)$.

Insider Information and Transmission. There is a financial market where agents can trade an asset with some fundamental value θ, where θ takes a value 1 or 0 with equal probability. Let the sender s be perfectly informed about θ. Suppose that the sender s transmits information regarding θ to the receiver r_s along a path of depth Δ_s. We assume that longer transmission poses a higher risk that s's information becomes public, i.e. nonmaterial, before trading is executed. One interpretation is that information is more likely to leak along the transmission path as information is passed through more agents. Alternatively, transferring information may take time, and a longer path increases the likelihood that transmission does not occur in time for profitable opportunities. Then, the likelihood that transmission provides r with an informational advantage is given by $\rho(\Delta_s)$, where $\rho(\cdot) \in [0,1]$ and $\rho(\cdot)$ decreases in Δ_s. With $1 - \rho(\Delta_s)$ probability, then θ becomes common knowledge, i.e. the market-maker becomes informed.

Financial Market. The market is populated with the receiver, a market-maker, and noise traders. If the receiver gains an informational advantage, the receiver makes a market order $x \in \{1, -1\}$. Noise traders' demand is stochastically determined $\tilde{y}$ drawn from uniform distribution $U[-y, y]$, where $y > 1$. The market-maker observes total demand $X = x + \tilde{y}$, where $x = 0$ if the receiver chooses not to trade. The market-maker sets price $P = E[\theta|X]$. Given price P, the payoff from trade for the receiver is given by $x(\theta - P)$. Finally, the regulator is assumed to observe individual order flow, i.e. x. This implies that as long as $x \neq 0$, the regulator initiates search. If the regulator initiates a search and catches agents, a punishment γ is imposed.

The solution to the trading game is characterized below:

Proposition 1. *In the trading game equilibrium, the expected profits from transmitting on a path of depth Δ_s are given by $\beta(\Delta_s) = \rho(\Delta_s) \cdot \frac{y-1}{2y}$.*

Proof. We conjecture and verify that if if informed makes order $x = 1$ if $\theta = 1$, and $x = -1$ otherwise. Given this, the market-maker observes total order flow $X = 1 + \tilde{y}$ if $\theta = 1$ or $X = -1 + \tilde{y}$ if $\theta = 0$ if transmission successfully occurs. Given this, prices are given by:

$$E[\theta|X] = \begin{cases} 1 & \text{if } X > -1 + y \\ \frac{1}{2} & \text{if } X \in [1 - y, -1 + y) \\ 0 & \text{if } X < 1 - y \end{cases}$$

The profits of the receiver if informed is $\frac{y-1}{2y}$. It is straightforward to see that deviating is not profitable. Given a transmission over a path of length l, the receiver's expected payoff is given by $\Pi(\Delta_s) = \rho(\Delta_s) \cdot \frac{y-1}{2y}$, and the expected social externality cost of $\rho(\Delta_s)\gamma(\Delta_s)$. □

The trading game provides a microfoundation for how insider trading profits are inversely related to the length of the transmission path. In equilibrium, the market-maker is less informed than the receiver with probability $\rho(\Delta_s)$. This in turn affects the ex-ante expected payoff from transmitting through a path of depth Δ_s. Embedding this result in the rest of the model, we can see that the core intuition from the main model follows. The sender and receiver face a tradeoff between transmitting information with higher expected value and the higher likelihood of prosecution (i.e. $Prob(m \geq \Delta_s)$ decreases in Δ_s).

B Decentralized Protocols

B.1 Decentralized Transmission and the Burden of Proof

So far, we assumed that insiders chose the optimal transmission path to exploit inside information. Implicitly, this assumes that insiders, including the sender and receiver, are coordinating, either through instructions or communication, on the transmission path for inside information. By knowing the source of the information, intermediaries along the chain demonstrate implicit knowledge that the transmission constitutes inside information. In the context of the model, this considerably simplifies the burden of proof for the regulator. First, verifying the transmission path connecting the sender and the receiver is sufficient for the regulator to prove that all agents, including the receiver and intermediaries, knowingly shared inside information for the trading purposes. Second, it also provides tangible link between the sender and receiver, thereby rendering any transfers to the sender enough to meet the condition of "quid pro quo". As such, the two parts to the burden of proof, namely, knowledge that the information traded on constitutes non-public material information, and benefits shared between those along the insider chain. In practice, however, inside information is often shared across the network in a decentralized manner (without explicit instructions on how to transmit information), and without explicit knowledge that the tip entails inside information.

In this section, we take as given a tor-periphery network, and consider an explicit implementation of optimal transmission strategy that could be employed by agents in a decentralized manner, and explore its implications on regulatory enforcement. At a high level, agents individually decide on who to pass information to, and use a message that contains only limited information about the providence of information. We demonstrate that insiders are able to replicate complex transmission strategies with only limited information, and explore how its strain regulators' ability to meet the burden of proof, further limiting enforcement intensity in equilibrium.

Decentralized Transmission. Instead of selecting path p_s, we assume that at the transmission stage, each agent chooses who and how to send information. Specifically, at the transmission stage, suppose that agents can transmit information only using a *tip* $\omega(\theta_s, a, \tau)$, which contains the inside information θ_s of sender s, the recipient $a \in A$, and the context τ, which explicitly conveys information about the nature of θ. The set of τ can be arbitrarily large. We will consider the simplest case where $\tau \in \{\star, \varnothing\}$,where $\tau = \star$ indicates that the original source is from S, and otherwise $\tau = \varnothing$, which also offers an economic interpretation of whether the recipient has demonstrable knowledge that θ_s constitutes inside information.

In our baseline model, agents select some path $p_s(s, i_1, i_2, ..., i_{\Delta_s}, r)$, which equivalent to a sequence of tips $\omega(\theta, i_k, \star)$ for $k = 1, 2, ..., \Delta_s$ and $\omega(\theta, r, \star)$. With decentralized transmission, agents lose several pieces of potentially vital information. First, aside from the first intermediary i_1 who receives a tip directly from s, intermediaries who receive tips are no longer have direct information regarding the providence of the inside information (i.e. the identity of s). Second, intermediaries no longer have direct information regarding their exact position within a transmission chain. Instead, they only know the identity of the agent who sends the tip to them, who we refer to as the *tipper.*

We first want to show that agents are able to achieve the optimal transmission strategy with decentralized transmission. Recall, in equilibrium, agents mix between a set of paths that span depths from $\underline{m} + 1$ to $\overline{m} + 1$. For expositional purposes, let us focus on when $\kappa(\cdot)$ is such that $\underline{m} = 1$ and $\overline{m} = 4$.[29] In order to implement the optimal transmission strategy, there must exist a rule that allows a sequence of agents to choose tips that can replicate the mixing strategies on paths of varying distances. We prove by example in the following proposition:

Proposition 2. *Consider the following rule:*

1. s sends $\omega(\theta, i_k, \star)$

2. If tipper is from S, i_k sends $\omega(\theta, i_{\Delta_s}, \varnothing)$ with probability p_3^1; $\omega(\theta, i_k, \varnothing)$ with probability p_4^1; and $\omega(\theta, i_{k'}, \star)$ with probability p_5^1 where $k \neq \Delta_s$

[29] First, this path length coincides with those empirically observed in some of the most sophisticated insider trading cases to date (Ahern, 2017). However, we provide a discussion at the end on how a richer set of ι would be operative in practice and support much larger transmission strategy sets.

3. If tipper is a sender relay, i_k sends $\omega(\theta, i_{\Delta_s}, \varnothing)$ if she receives $\omega(\theta, i_k, \varnothing)$. Instead, if she receives $\omega(\theta, i_k, \star)$, she sends $\omega(\theta, i_{k'}, \varnothing)$ with probability p_5^2; and $\omega(\theta, i_{k'}, \star)$ with probability p_6^2, where $k' \neq \Delta_s$ and not hub.

4. If tipper is not in S and not a sender relay, i_k sends $\omega(\theta, i_{\Delta_s}, \varnothing)$ if she receives $\omega(\theta, i_k, \varnothing)$; and $\omega(\theta, i_{k'}, \varnothing)$ if she receives $\omega(\theta, i_k, \star)$, where $k' \neq \Delta_s$ and not hub.

5. i_{Δ_s} sends $\omega(\theta, r, \varnothing)$.

Using this rule, agents can implement the equilibrium transmission strategy.

Proof. **(Proposition 2)** The implied probabilities of all path lengths are given by p_3^1 for $l = 3$, p_4^1 for $l = 4$, $(1 - p_3^1 - p_4^1)p_5^2$ for $l = 5$, and $(1 - p_3^1 - p_4^1)(1 - p_5^2)$ for $l = 6$. Hence, for any mixing strategy with $p_1, p_2, p_3, (1 - p_1 - p_2, -p_3)$ corresponding to transmission paths with depth $l = 3, 4, 5, 6$, the rule can match probabilities by setting $p_3^1 = p_1$, $p_4^1 = p_2$, and $p_5^2 = \frac{p_3}{(1-p_3^1-p_4^1)}$. □

The rule outlined in Proposition 2 shows that tips, combined with information about the identity of the tipper and network, is sufficient for agents to replicate any equilibrium transmission strategy.

There are several notable observations of Proposition 2. Appending the context of insider information to a tip, i.e. tips with $\tau = \star$, informs the tippee that θ_s should be passed along further. Doing so enables intermediaries to achieve transmission paths of varying lengths ex-post with fairly simple rule. Interestingly, in last several tips along *any* path, agents avoid communicating the context. In doing so, with decentralized transmission, omitting the providence of θ in a tip acts as a signal that tip should be used for trading. Whenever an intermediary receives a tip with $\tau = \varnothing$, the intermediary tips the intermediary directly linked to a trader who can exploit the information.

Additionally, the simple rule not only facilitates optimal transmission, but achieves a deeper purpose in the context of insider trading because the regulator faces the burden of proving the trader's knowledge of insider information. The practice of sharing information whilst deliberately avoiding details on its insider nature is documented in real-world practices in insider trading. In the pivotal case of United States v. Newman, the Southern District of New York convicted a group of portfolio managers, analysts, and corporate insiders, who were accused of exploiting insider information. Despite clear evidence on the path of information transmission, the defendants successfully appealed their case based, among several issues, on the fact that [30]:

> [The] Government presented no evidence that Newman and Chiasson knew that they were trading on information obtained from insiders in violation of those insiders' fiduciary duties.

In other words, without explicit proof that a tippee communicates the insider nature of the tip, the ultimate beneficiary of insider information can credibly argue that they knowingly traded on nonpublic, material information.

To appreciate the impact of this on equilibrium outcomes, consider the following extension. Let agents follow the rule in Proposition 2, and suppose that whenever information is transmitted without sharing its fidelity (i.e. $\tau = \varnothing$), regulators incur an additional cost $\overline{\kappa}$. That is, absent direct proof that a tippee knows the original source of the tip, the regulator may need to devote greater resources to build a case around circumstantial evidence. The expected cost of enforcing $\overline{m}$ rises by more than $\overline{\kappa}$, since all paths involve at least one tip with $\tau = \varnothing$. When the cost function $\kappa(m)$ shifts upward sufficiently high, the regulator is forced to lower $\overline{m}$. In effect, the average transmission path decreases, and insider profits increase in equilibrium.

B.2 Alternative Decentralized Transmission Mechanisms

Proposition 2 outlines an implementation of decentralized transmission in the context of tor-periphery networks. In this section, we further consider a more general decentralized transmission protocol that could achieve discreet communication over trusted links.

As a precursor, links in L represent trust that is formed at cost in the past. Embedding trust in links is key for the machinations of insider networks along several dimensions. In practice, it helps to mitigate regulatory risk by maintaining the confidentiality of information transmission and discouraging whistleblowing and/or cooperating with authorities. It also facilitates efficient exploitation of insider gains by ensuring the reliability and accuracy of information, and avoiding diversion for private gains.

Consider the following protocol among trusted agents. Agents agree on a modus operandi M to facilitate inside information transmission. $M : A \times A \times \Theta \to A \cup \{\emptyset\}$

[30] See here for more details.

is a codex describes local 'next steps' during transmission. If nature gives a receiver $r \in R$ an opportunity in θ, making $r = r_\theta$, then r knows that r should

Given L, the search and transmission of information is facilitated via a *modus operandi* M, described as follows. We start by considering a scenario, in which $r_s \in R$ seeks inside information. If r_s wants an "opinion" on some matter θ, r knows that r_s should

- Ask a trusted intermediary $M(r; r, \theta) \in L_r$: "What is your opinion on θ?"
- If $M(r; r, \theta) = \emptyset$, do not ask anyone.

When $a \in A$ is asked "What is your opinion on θ?" by a trusted agent $a' \in L$, then a knows that a should

- Not ask a' why opinions on θ is needed,
- Ask trusted agents described by the codex $M(a'; a, \theta) \in L_a$, "What is your opinion on θ?"
- Report the opinion back to a' once it is provided by $M(a'; a, \theta)$.[31]
- Not share the opinion with anyone else.

When $s \in S$ is asked for an opinion on θ by a trusted agent $a \in L$, then s knows that s should

- Not ask a why an opinion on s is needed,
- Provide an honest opinion if s knows θ.

The modus operandi M is a codex to that describes instructions for mutually trusting counterparties in L. It is an ex-ante communicated methodology on how to communicate ex-post. In this particular scenario, requests for information held by s flows from r_s to s along the chosen path. Then information flows back along the same path once obtained from s.

A similar methodology can be used in an alternative scenario in which an expert s initiates the chain. When s_θ receives the inside information, s knows that s should ask a trusted intermediary $M(s; s, \theta) \in L$: "Do you want my opinion on θ?" When $a \in A$ is asked "Do you want my opinion on θ?" by a trusted agent $a' \in L$, then a knows that a should hear the opinion and ask a trusted agent described by the codex $M(a'; a; \theta) \in L$, "Do you want my opinion on θ?" When $r_s \in R$ is asked "Do you

[31]Alternatively, the codex can describe who to refer to next.

want my opinion on θ?" by a trusted agent in L, r_s should hear the opinion and trade on the information.

Mixtures of the two scenarios also work. Asking for information can start from r_s and offering information can start from s. Ultimately, any execution boils down specifying a path of transmission. That is, choosing codex M is equivalent to picking, for each case θ, either not to transmit, or to pick a transmission trail r_s and s in L

$p_\theta = (r_s, i_1, i_2, ..., i_\Delta, s) =$

$\Big(r_s, i_1 = M(r_\theta; r_\theta, \theta), i_2 = M(r_\theta; i_1, \theta), ..., i_{k+1} = M(i_{k-1}; i_k, \theta)), ..., s = M(i_{\Delta-1}; i_\Delta, \theta)).$

Note that M in and of itself does not rule out trails that overlap with itself. For example, it is possible that $i_1 = i_3$. But this only makes the required investigation shorter. So it is without loss that M that leads to a non-path trail would never be picked. Furthermore, any randomization needed for path lengths is handled by randomizing M.

B.3 Decentralized Compensation Schemes

In the baseline model, we assume that agents A shared the costs and benefits from insider information. In reality, redistribution of payoffs, particularly in the form of payments, poses a significant risk to agents due to traceability. As such, in practice, insiders may dynamically exchange tips instead, sharing information to the network in anticipation of receiving tips in the future (Tamersoy et al., 2013). In a dynamic version of our setting, this could arise if agents alternate between being senders and receivers over time. In other contexts, however, traders may explicitly seek to pay for access to inside information. For example, in the cases involving expert network firms, hedge funds sought contact with corporate and legislative insiders to extract material non-public information, which was relayed by intermediaries at a price.[32] Motivated by this, we outline a simple protocol that achieves both decentralized transmission and compensation scheme.

Specifically, consider the following scenario in which inside information is actively sought out by a trader. suppose that each sender and intermediary are simply paid a fixed amount in exchange for their 'expert opinion.' There is no implicit distribution and sharing of private gains of traders. Instead, there is an implicitly agreed upon 'market rate' q_0 for information origination and q_1 for information relay. Consider

[32]In the context of compensation, networks in which intermediaries form a coalition at the core may have additional benefits arising from allocative efficiency (Gofman, 2011).

the following scheme:

- The trader seeking information from a path of distance Δ, offers to any linked intermediary to pay for 'advice' at price $q_0 + \Delta q_1$, such that price maps to the intended path length: $\frac{(q_0+\Delta q_1)-q_0}{q_1}$.
- The intermediary picks any random intermediary and offers to pay $q_0+(\Delta - 1)\, q_1$ for 'advice.' Note, i_1 pockets q_1.
- A random sequence of questions continues until an intermediary is offered $q_0 + 2q_1$.
- This intermediary asks someone who is linked to the expert of the topic and offers $q_0 + q_1$, pockets q_1. The final intermediary, upon observing that he is offered $q_0 + q_1$, asks the expert, offers q_0 and pockets q_1.
- The expert accepts, provides its 'opinion,' which flows back along the path as agreed upon in the trade. Note that if an intermediary has been asked and has received payment before, he is trusted to refuse additional offers. When an offer is refused, the offering intermediary asks another intermediary at random until it finds one who accepts.

This protocol requires that links in L represent trusted relations, (ii) prices q_0 and q_1 are determined ex-ante, and (iii) for each $s \in S$ and $i \in I$, there is $j \in I$ such that $\{i, j\}, \{j, s\} \in L$ and i knows that $\{j, s\} \in L$, the last of which is satisfied if and only if the network is a tor-periphery.

C Proofs

Proof of Theorem 1

Consider choosing m. If A sends with Δ, then A gets $u_A = \beta(\Delta) - \iota_{m\geq\Delta}\gamma(\Delta)$ and G gets $u_G = -\kappa(m) + \iota_{m\geq\Delta}\gamma'(\Delta) - \beta'(\Delta)$. If A does not send, A gets 0 and G gets $-\kappa(m)$. G never plays $m < \underline{m}$ as $\underline{m}$ is free. In fact we assumed $m < \underline{m}$ away from the action set. G never plays $\overline{m} + 1$ or more, because $\overline{m}$ strictly dominates these.

Let the set of available path lengths between $\underline{m} + 1$ and $\overline{\Delta}$ be D, and enumerate its elements $\Delta_1 < \Delta_2 < ... < \Delta_{|D|} = \overline{\Delta}$. Denote $\underline{m} = \Delta_0$.

Consider an equilibrium. Note the two lemmas:

(a) For any k between 0 and $|D| - 1$, if $m = \Delta_k$ has 0 probability, then $\Delta = \Delta_{k+1}$ has 0 probability because A would shift the probability down to increase benefits without reducing the cost.

(b) For any k between 1 and $|D|-1$, if $\Delta = \Delta_k$ has 0 probability, then $m = \Delta_k$ has 0 probability because G would shift the probability down to reduce costs without reducing benefit.

(c) By induction using (a) and (b), $m = \Delta_0$ has positive probability.

(d) $\Delta = \Delta_{|D|}$ guarantees positive u_A. So not sending has 0 probability. Then $m = \underline{m}$ gives $u_G = -\beta'$.

(e) If $\Delta = \Delta_{|D|}$ has 0 probability, then $m = \Delta_{|D|-1}$ gives $u_G > -\beta'$.

By (c),(d),(e), $\Delta = \Delta_{|D|}$ has positive probability. Then by (a), (b), and induction, all $m = \Delta_0$ to $\Delta_{|D|-1}$ and all $\Delta = \Delta_1$ to $\Delta_{|D|}$ have positive probability. A puts positive probability on $\Delta = \Delta_{|D|}$ which is larger than all m. So by indifference conditions, $u_A = \beta(\Delta_{|D|}) = \beta(\overline{\Delta})$ and $u_G = -\beta'$.

Proof of Theorem 2 A tor-periphery offers all distances from $\underline{m}+1$ to $\overline{m}+1$ for every $s-r$ pair. Along the lines of Theorem 1, (σ_p^*, σ_m^*) is characterized by the A's indifference between $\underline{m}+1$ to $\overline{m}+1$ and G's indifference between $\underline{m}$ to $\overline{m}$. This yields 0 payoff to G and $\beta(\overline{m}+1)$ interim payoff to A because A puts positive probability on $\overline{m}+1$ and G can not match $\overline{m}+1$. Then

$$V_A(L^*, \sigma_p^*, \sigma_m^*) = \zeta|S|\beta(\overline{m}+1) - \eta\left(|S|+|R|\right) - c(T)$$

The only task is prove that $V_A(L^*, \sigma_p^*, \sigma_m^*) \geq V_A(L, p, \sigma_m^*) - \epsilon|A|$ condition holds.

Take any L. Conditional on a pair, regardless of distances available in L, the highest payoff with any p against σ_m^* is $\beta(\overline{m}+1)$. This follows from the fact that σ_p^* is a best response against σ_m^* when all rationalizable path distances are available to pick.

Let S' and R' be the non-isolated senders and receivers. Others can not take part in transmission. Take any $n^*_{k,\epsilon} > \frac{\eta'}{4\epsilon}k^2$. Then

$$\begin{aligned}
V_A(L,p,\sigma^*_m) &\le \zeta|S'|\frac{|R'|}{|R|}\beta(\overline{m}+1) - c(L) \\
&\le \zeta|S'|\frac{|R'|}{|R|}\beta(\overline{m}+1) - \eta\left(|S'|+|R'|\right) \\
&\le \zeta|S|\frac{|R|}{|R|}\beta(\overline{m}+1) - \eta\left(|S|+|R|\right) \\
&= V_A(L^*,\sigma^*_p,\sigma^*_m) + c(T) \\
&< V_A(L^*,\sigma^*_p,\sigma^*_m) + \eta'\frac{1}{2}|T|^2 \\
&< V_A(L^*,\sigma^*_p,\sigma^*_m) + \epsilon|A|
\end{aligned}$$

Proof of Theorem 3 We can follow the logic in the proof of the discrete case for sufficiency. Consider any tor-periphery network L^*. Along the lines of Theorem 1, (σ^*_p,σ^*_m) is characterized by A's indifference between $\underline{m}+1$ to $\overline{m}+1$ and G's indifference between $\underline{m}$ to $\overline{m}$ (for almost every pair in Lebesgue measure, not every pair). This yields 0 payoff to G and $\beta(\overline{m}+1)$ payoff to A. Then

$$V_A(L^*,\sigma^*_p,\sigma^*_m) = V^* := \zeta\mu_S\beta(\overline{m}+1) - \eta\left(\mu_S+\mu_R\right)$$

Take any L and p. Conditional on a pair, regardless of distances available in L, the highest payoff with any p against σ^*_m is $\beta(\overline{m}+1)$. This follows from the fact that σ^*_p is a best response against σ^*_m when all rationalizable path distances are available to pick.

Let μ'_S and μ'_R be the non-isolated senders and receivers. Others can not take part in transmission. Then

$$\begin{aligned}
V_A(L,p,\sigma^*_m) &\le \zeta\mu_S\frac{\mu'_R}{\mu_R}\beta(\overline{m}+1) - c(L) \\
&\le \zeta\mu_S\frac{\mu'_R}{\mu_R}\beta(\overline{m}+1) - \eta\left(\mu'_S+\mu'_R\right) = V^*
\end{aligned}$$

So all tor-periphery networks are equilibria networks.

For necessity, notice that A can always deviate to forming a tor-periphery and choosing $\overline{m}+1$ path-distance at each pair. This yields V^* payoff with certainty since G can not win against $\overline{m}+1$. So A gets at least V^* payoff in any equilibrium.

Consider any equilibrium (L',σ'_p,σ'_m). The conditional interim payoff of A on (s,r_s) such that (s,r_s) does not have a path of distance at least $\overline{m}+1$ is 0 since A needs to mix with not sending information. For the remaining (s,r_s), the conditional interim payoff is $\beta\left(\overline{\Delta}(s, r_s, L)\right)$. Thus

$$
\begin{aligned}
V_A(L', \sigma_p', \sigma_m') &\leq \zeta\mu_S\frac{\mu_R'}{\mu_R}\beta(\overline{m}+1) - c(L) \\
&\leq \zeta\mu_S\frac{\mu_R'}{\mu_R}\beta(\overline{m}+1) - \eta\left(\mu_S' + \mu_R'\right) = V^*
\end{aligned}
$$

So in any equilibrium A has at most V^*. Therefore, in any equilibrium A has exactly V^* payoff. So the equality in $V_A(L', \sigma_p', \sigma_m') \leq V^*$ holds. The equalities in all previous inequalities hold only if and only if (i) $\mu_S = \mu_S^{'}$, $\mu_R = \mu_R^{'}$, (ii) for a.e. (s, r_s), there exists a path of distance $\overline{m}+1$ between s and r_s, (iii) $c(L') = \eta\left(\mu_S + \mu_R\right)$. These make up a necessary condition for equilibrium.

There is one more necessary condition. Notice that L^* also costs V^*. So A can deviate from its transmission strategy to any other transmission strategy by doubly deviating to L^*. So the best response cycle and the proof of Theorem 1 applies. A must have positive probability on all path lengths $\underline{m}+1$ to $\overline{m}+1$ for almost every (s, r) pair. This yields the additional necessary condition: (iv) between almost every pair (s, r) there are paths of all distances $\underline{m}+1$ to $\overline{m}+1$ in L.

The final step is to show that (i), (ii), (iii), (iv) necessitate tor-periphery networks. Recall that each link must have at least one intermediary by assumption. So $A \backslash I$ can not have links among each other. Also I is finite. So $c(L)$ accrues solely from links in $I \times (A \backslash I)$. By (iii)

$$
\sum_{i \in I}\mu_i = \frac{c(L')}{\eta} = \mu_S + \mu_R
$$

Then by finiteness of I and (i), almost every I has has exactly one link.

Consider an intermediary i s.t. $\mu_i > 0$. If i is linked to a positive measure of senders and positive measure receivers, almost every one who is linked only to i, then these pairs of senders and receivers immediately get caught when they transmit information (because $\underline{m} \geq 1$). So either i's a.e. linked agents are senders or i's a.e. linked agents are receivers. Depending on which, assign i either as a sender relay or receiver relay. Assign the remaining intermediaries as middle relays. By (iv), a.e. sender relay-receiver relay pair must be connected with paths of distance $\underline{m}-1, ..., \overline{m}-1$. This concludes the proof that L' is a tor-periphery, with $T \subset I$.

Proof of Theorem 4 The proof is identical to the sufficiency part of the proof of Theorem 3.

Proof of Theorem 5 Follows fairly easily by complementarities in joining the insider network.