Network Analysis for Criminal Investigators:
How effective is network analysis in detecting money laundering?

2401049
Joshua.A.J.McManus
The University of Buckingham
BA (Hons) Security, Intelligence, and Cyber.

Table of Contents

SECTION 1:

Main Body

Introduction

The global fight against money laundering (the process by which criminals disguise illicit money as legitimate)[1] has long been characterised by operational asymmetry. Regulatory compliance and financial intelligence (referred to outwith as Anti-Money Laundering Teams, AMLs) have historically relied upon static, rule-based monitoring systems that evaluate transactions in isolation. For example (in the US) a transfer exceeding $10,000 USD may trigger an automatic flag, while payments just below that threshold (such as $9,000 USD) historically have gone unnoticed. This process is known as structuring[2], and works on the basis of a misunderstanding of money laundering, which is never a single event. Money laundering requires the movement of value across multiple accounts, jurisdictions, and legal entities in order to obfuscate the link between target destination and criminal source.

This essay argues that network analysis is highly effective as a structural diagnostic capable of converting isolated transaction logs into macro-level geometries of suspicious behaviour, however its efficacy is not uniform. Network analysis is exceptionally precise at mapping the anomalies of the layering phase (the stage where launderers deliberately complicate transaction trails)[3] yet its power is severely restricted by the globalised nature of money laundering and the chasms of international legal jurisdiction. Effectiveness, therefore, is a function of visibility. Where data flows freely, networks reveal criminal architectures. And such, where borders interrupt data, those same architectures become invisible.

---

[1] Crown Prosecution Service (2024). Money Laundering Offences. [online] Cps.gov.uk. Available at: https://www.cps.gov.uk/prosecution-guidance/money-laundering-offences [Accessed 31 May 2026].

[2] Rahman, S. (2024). What is the difference between structuring and smurfing in money laundering? [online] www.rahmanravelli.co.uk. Available at: https://www.rahmanravelli.co.uk/expertise/anti-money-laundering-investigations/articles/what-is-the-difference-between-structuring-and-smurfing-in-money-laundering-/ [Accessed 31 May 2026].

[3] Central Bank of Ireland (2014). Anti-Money Laundering and Countering the Financing of Terrorism I Central Bank of Ireland | Central Bank of Ireland. [online] Centralbank.ie. Available at: https://www.centralbank.ie/regulation/anti-money-laundering-and-countering-the-financing-of-terrorism [Accessed 31 May 2026].

The Geometry of Laundering

To understand the uses of Network Analysis in AML, you must reconceptualise financial transactions from being discrete events into weighted graphs. If you take a graph of $\langle G = (V, E) \rangle$, where vertices $\langle V \rangle$ represent entities (i.e. bank accounts, shell companies, legal owners, and even individual transactors) and edges $\langle E \rangle$ represent the flow of value (typically weighted by transaction volume and frequency) you can represent money laundering as a map of connections but more importantly weak points. The layering phase of money laundering, which deliberately seeks to confuse auditors through multiple rapid transfers across numerous accounts, is uniquely vulnerable to this form of mathematical scrutiny.

A core technique in layering involves the use of circular loops, funds are routed through a sequence of accounts such that Account A pays B, B pays C, and C eventually returns value to A. In legitimate commerce, such closed-loop cycles are very rare and almost always deliberately artificial and designed to simulate the appearance of genuine business activity. Network analysis detects these cycles instantly through graph traversal algorithms[4] that identify strongly connected nodes and directed cycles across millions of transactions. Unlike threshold-based systems, which see only individual payments, graph-based detection perceives the entire circuit. A launderer moving £50,000 through fifteen accounts in ninety minutes produces a detectable 'ring' that simple monitors would miss entirely, since no single transfer exceeds a reporting threshold. However, this method falls short when dealing with transnational and crossborder financial transfers, especially in countries where secrecy is paramount[5].

This, however, is not the end point. Investigators, if given the resources of course, *could* apply sociological network theory to financial crime, particularly Ronald Burt's concept of structural holes[6]. In legitimate economic networks, a structural hole refers to a gap between two otherwise disconnected clusters of actors. A broker who bridges that hole creates value by facilitating information flow or trade that would not otherwise occur. In money laundering, however, criminal networks deliberately manufacture structural holes using shell companies and nominee directors[7]. This is done in order to control the only connection

[4] Truong, Q.D., Truong, Q.B. and Dkaki, T. (2016). Graph Methods for Social Network Analysis. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, [online] 168, pp.276–286. doi:https://doi.org/10.1007/978-3-319-46909-6_25.

[5] Weeks-Brown, R. (2018). Straight Talk: Cleaning Up. [online] IMF. Available at: https://www.imf.org/en/Publications/fandd/issues/2018/12/imf-anti-money-laundering-and-economic-stability-straight [Accessed 31 May 2026].

[6] Burt, R.S. (1992). Structural Holes: The Social Structure of Competition. [online] JSTOR. Harvard University Press. Available at: https://www.jstor.org/stable/j.ctv1kz4h78 [Accessed 31 May 2026].

[7] Financial Action Task Force (2014). Transparency and Beneficial Ownership. [online] Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-transparency-beneficial-ownership.pdf.coredownload.pdf [Accessed 31 May 2026].

between a cluster of cash-generating activities (such as small-scale drug dealing) and a separate cluster of mainstream financial institutions where funds are ultimately integrated.

This could be exposed by utilising the betweenness centrality of nodes. For target node ⟨ x ⟩, if you define ⟨ σ_{st} ⟩ as the total number of shortest paths (in measure of 'hops') between nodes ⟨ s ⟩ and ⟨ t ⟩ and define ⟨ $\sigma_{st}(x)$ ⟩ as the number of these paths that pass through target node ⟨ x ⟩, you can map betweenness centrality as ⟨ $C_B(x) = \sum_{s \neq x \neq t} \frac{\sigma_{st}(x)}{\sigma_{st}}$ ⟩. In a laundering network, a shell company registered to a nominee director will display disproportionately high betweenness metrics because it serves as the sole bottleneck linking an upstream illicit cash network to a downstream integration network. Legitimate entities exhibit more distributed connectivity, as no single company should monopolise pathways between entire functional clusters of the economy. Studies of suspicious activity reports (SARs) have demonstrated that accounts flagged for high betweenness centrality are statistically far more likely to be involved in layering than those identified by transaction-volume thresholds alone[8]. Network analysis can thus convert an abstract corporate evasion tactic into a directly calculable red flag.

While betweenness centrality isolates the critical bottlenecks of the layering phase, another layer of scrutiny lies in eigenvector centrality. To showcase its utility, let ⟨ $A = (a_{i,j})$ ⟩ be the adjacency matrix, a square matrix where ⟨ $a_{i,j}$ ⟩ represents the value transferred from node ⟨ i ⟩ to node ⟨ j ⟩ (or 1 if any transfer exists, 0 otherwise), of a financial transaction network. The eigenvector centrality ⟨ x_i ⟩ of a node ⟨ i ⟩ is defined as proportional to the sum of the centralities of its adjacent neighbours, expressed as: ⟨ $x_i = \frac{1}{\lambda}\sum_{j \in M(i)}(a_{i,j}x_j)$ ⟩ (where ⟨ $M(i)$ ⟩ denotes the set of nodes connected to ⟨ i ⟩, and ⟨ λ ⟩ is the principal eigenvalue (the largest solution to the characteristic equation ⟨ $det(A - \lambda I) = 0$ ⟩, which by the Perron-Frobenius theorem[9] is positive and associated with a unique eigenvector whose entries are all non-negative), satisfying the matrix equation ⟨ $Ax = \lambda x$ ⟩. Eigenvector centrality implies that an entity's strategic importance is a function not just its direct transactional volume (degree), but also the 'prestige' of the nodes it interacts with. In legitimate networks, high eigenvector scores accurately capture high influence transactions such as major clearing houses, institutional hubs, or dominant payment gateways.

[8] Baigabyl, R., Nugumanova, A. and Sodnomova, M. (2025). Using Graph Centrality Metric for Detection of Suspicious Transactions. Scientific Journal of Astana IT University, [online] 22, pp.134–152. doi:https://doi.org/10.37943/22ZSKI6025.

[9] Lemmens, B. and Nussbaum, R.D. (2012). Nonlinear Perron-Frobenius theory. [online] Cambridge ; New York: Cambridge University Press. Available at: https://assets.cambridge.org/97805218/98812/excerpt/9780521898812_excerpt.pdf [Accessed 1 Jun. 2026].

However, sophisticated criminal networks are engineered precisely with this in mind. In layered networks, ultimate beneficial owners (UBOs) deliberately insulate themselves from the graph's high-prestige components to evade detection. This structural evasion was evident in the multi billion “Troika Laundromat”[10] scandal. The infrastructure of this network relied on a decentralised web of at least 70 interconnected offshore shell companies operating across various jurisdictions. Had AMLs relied solely on eigenvector centrality, the principal nodes directing the scheme may have remained invisible. Because the laundering core transacted through a highly isolated sub-net of newly fabricated nominee accounts rather than established, high-prestige entities, their $\langle x_i \rangle$ metrics trended towards zero. The network's true operational architecture was instead uncovered by tracking the high betweenness centrality of specific transactional bridges linking these low-prestige shell clusters back to commercial European banking endpoints. Relying heavily on global eigenvector metrics can introduce significant blind spots, as it assumes a natural distribution of network prestige that deceptive laundering schemes actively seek to fracture. Consequently, network analysis is highly effective only when investigators match the chosen centrality algorithm to the specific architectural subversion employed by the criminal network.

Furthermore, it is important to note that neither metric is fully objective pieces of evidence. For example, a legitimate payment processor or a currency exchange bureau may exhibit high betweenness centrality, and low eigenvector scores because its business model is precisely to bridge otherwise disconnected low-profile parties. The effectiveness of network analysis at this stage is diagnostic rather than conclusive. It generates a ranked list of structural outliers requiring further investigation, but it cannot distinguish between a criminal shell company and a legitimate intermediary alone. Nonetheless, as a tool for AMLs processing millions of transxactions, the ability to reduce the search space from all accounts to a handful of anomalous nodes represents an effective tool over traditional method.

[10] OCCRP (2019). The Troika Laundromat. [online] Organised Crime and Corruption Reporting Project. Available at: https://www.occrp.org/en/project/the-troika-laundromat [Accessed 1 Jun. 2026].

The Data Integration Problem

Fundamentally, Network analysis is only as effective as the underlying data. Financial intelligence is often never delivered in a formatted relational database (RDBs)[11]. Instead, it is usually given in fractured and sometimes (deliberately) corrupted datasets. To build a true network, analysts must link vastly different data formats: SWIFT and SEPA transaction logs (which provide IBANs, timestamps, and amounts)[12], corporate filings from registries such as Companies House (which list directors, shareholders, and registered addresses)[13], and Suspicious Activity Reports (SARs) filed by compliance officers, which contain narrative text and named entities. Each source uses different identifiers, different naming conventions, and different levels of data quality. The challenge is, how does one know that two records refer to the same real-world entity? This problem, known as entity resolution or record linkage[14], has two main approaches. Deterministic resolution requires perfect (or near-perfect) agreement on identifiers, such as the same tax identification number, the exact legal name, or an identical address string. Probabilistic resolution assigns a matching probability based on multiple fuzzy attributes (similar names, partial address matches, shared phone numbers) and links records when the probability exceeds a threshold. Both approaches introduce vulnerabilities that launderers actively exploit.

The specific countermeasure is obfuscation. A criminal network may register a shell company as “J. Smith” with one offshore registry, as “John Smyth” with a second, and as “Jonathan Smithe” with a third, using slightly varying post office boxes or service addresses each time. If the entity-resolution threshold is set too rigid (requiring exact string matches), the graph fragments into disconnected components, each representing a different apparent “J. Smith” who is in fact the same beneficial owner. The laundering infrastructure becomes invisible to network detection algorithms because the algorithm never recognises that the nodes are connected. Conversely, if the threshold is set too loosely, the algorithm produces false positives, merging distinct individuals who happen to share common surnames or partial addresses. This vulnerability is furthered in cross-border scenarios where different jurisdictions use incompatible identifier systems.

---

[11] Databricks Inc. (2025). Financial Data Intelligence: How to Transform Raw Data into Actionable Insights. [online] Databricks. Available at: https://www.databricks.com/blog/financial-data-intelligence-how-transform-raw-data-actionable-insights [Accessed 1 Jun. 2026].

[12] Maroulis, N. (2026). SWIFT MX camt.053 in SEPA - A Detailed Analysis of Its Broad Use. doi:https://doi.org/10.2139/ssrn.6132206.

[13] HM Government (2017). Company Accounts Guidance. [online] GOV.UK. Available at: https://www.gov.uk/government/publications/life-of-a-company-annual-requirements/life-of-a-company-part-1-accounts [Accessed 1 Jun. 2026].

[14] Financial Action Task Force (2022). Partnering in the Fight against Financial Crime. [online] Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf [Accessed 1 Jun. 2026].

The Financial Friction

The most severe constraint on network analysis is geographical. Network analysis requires a (near-) complete view of the transaction graph to identify structural holes, cycles, and high-betweenness nodes. International money laundering is fundamentally designed to exploit sovereign borders precisely because borders fragment visibility. If laundering network routes funds from London to the British Virgin Islands (BVI) and then to Panama and finally returns to a European account, the complete graph exists only in principle as no single financial intelligence unit possesses all the data. UK authorities can see the London to BVI leg, BVI authorities can see the incoming and outgoing transfers, Panamanian authorities see the middle leg. This is purely a legal issue as the technology to map a global financial graph exists and real-time data sharing between national financial intelligence units is architecturally feasible[15]. Data protection laws restrict the transfer of personal financial data across borders without explicit legal justification. Banking secrecy acts in jurisdictions such as Switzerland, Singapore, and the Cayman Islands hinder the full disclosure of client information to foreign authorities. Even where legal channels for information sharing exist (such as the Egmont Group of Financial Intelligence Units[16]), the processes are multilateral, slow, and subject to mutual legal assistance treaties that can take months or years to execute. By the time permission is granted to access foreign transaction records, the laundering network has long since dissolved and re-formed elsewhere. Network analysis applied to a fragmented dataset yields a fragmented picture, and a fragmented picture is, for the launderer, as good as no picture at all.

The recent shift towards decentralised finance (DeFi) and cryptocurrency presents a paradox. Public blockchains (such as those used in Bitcoin, Ethereum, and their analogues) provide an open, immutable, and global ledger perfectly suited to graph analysis, as every transaction between wallet addresses is visible to every participant[17]. Network analysis on blockchain data has indeed been used successfully to trace ransomware payments and sanction evasion but launderers have developed countermeasures designed explicitly to fragment blockchain graphs. The most effective of these is chain-hopping, the use of cross-chain bridges to move value from one blockchain to another. A launderer might convert Bitcoin to Ethereum via a decentralised bridge, then Ethereum to Solana, then back to Bitcoin through a different bridge. Each bridge crossing breaks the edge-lineage of the graph because

[15] Financial Action Task Force (2012). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. [online] Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf?nocache=true [Accessed 1 Jun. 2026].

[16] Egmont Group (2025). Principles for Information Exchange between Financial Intelligence Units (FIUs). [online] Available at: https://egmontgroup.org/wp-content/uploads/2022/07/EG-Principles-for-Information-Exchange-Revised-July-2025.pdf [Accessed 1 Jun. 2026].

[17] Shukla, A., Jirli, P., Mishra, A. and Singh, A.K. (2024). An overview of blockchain research and future agenda: Insights from structural topic modeling. Journal of Innovation & Knowledge, [online] 9(4), p.100605. doi:https://doi.org/10.1016/j.jik.2024.100605.

the transaction output on the destination chain is a new wallet address with no direct on-chain link to the source address. While heuristics can sometimes reconstruct these hops by analysing timing and volume patterns, the process is probabilistic rather than deterministic. Moreover, privacy-preserving technologies such as zero-knowledge proofs and dedicated privacy coins (Monero, Zcash, etc)[18] are explicitly designed to defeat graph analysis entirely, rendering transaction flows untraceable by cryptographic design. The cryptocurrency shift represents an arms race, as graph analysis becomes more powerful, laundering techniques evolve to reintroduce the fragmentation that borders previously provided.

[18] Lee, J., Choi, G., Han, J. and Park, J. (2025). Advanced Monero wallet forensics: Demystifying off-chain artifacts to trace privacy-preserving cryptocurrency transactions. Forensic Science International: Digital Investigation, [online] 54, p.301988. doi:https://doi.org/10.1016/j.fsidi.2025.301988.

Conclusion

The effectiveness of network analysis in detecting money laundering is not a static attribute of the technology, but a variable contingent upon the topological integrity of the data. As this essay has demonstrated, graph-theoretic approaches offer a revolutionary shift from the 'point-in-time' failures of threshold-based monitoring to a systemic 'relational' paradigm. By identifying structural holes and utilising betweenness centrality, investigators can unmask the layering architectures that define modern financial crime. However, the move toward decentralised finance and the persistent reality of jurisdictional silos represent a 're-fragmentation' of the financial graph.

While the mathematics of cycle detection and path-finding are computationally absolute, they are epistemologically limited by the quality of entity resolution and the legal friction of sovereign borders. Ultimately, network analysis serves as a powerful diagnostic for identifying where the law should look, but its efficacy remains tethered to the visibility of the global financial commons. Effectiveness, therefore, is a function of visibility. Where data flows freely, networks reveal criminal architectures. Where borders interrupt data, those same architectures become invisible.

THE END.

SECTION 2:

Accreditation.

Sources Used

1. Baigabyl, R., Nugumanova, A. and Sodnomova, M. (2025). Using Graph Centrality Metric for Detection of Suspicious Transactions. *Scientific Journal of Astana IT University*, [online] 22, pp.134–152. doi:https://doi.org/10.37943/22ZSKI6025.
2. Burt, R.S. (1992). *Structural Holes: The Social Structure of Competition*. [online] *JSTOR*. Harvard University Press. Available at: https://www.jstor.org/stable/j.ctv1kz4h78 [Accessed 31 May 2026].
3. Central Bank of Ireland (2014). *Anti-Money Laundering and Countering the Financing of Terrorism I Central Bank of Ireland | Central Bank of Ireland*. [online] Centralbank.ie. Available at: https://www.centralbank.ie/regulation/anti-money-laundering-and-countering-the-financing-of-terrorism [Accessed 31 May 2026].
4. Crown Prosecution Service (2024). *Money Laundering Offences*. [online] Cps.gov.uk. Available at: https://www.cps.gov.uk/prosecution-guidance/money-laundering-offences [Accessed 31 May 2026].
5. Databricks Inc. (2025). *Financial Data Intelligence: How to Transform Raw Data into Actionable Insights*. [online] Databricks. Available at: https://www.databricks.com/blog/financial-data-intelligence-how-transform-raw-data-actionable-insights [Accessed 1 Jun. 2026].
6. Egmont Group (2025). *Principles for Information Exchange between Financial Intelligence Units (FIUs)*. [online] Available at: https://egmontgroup.org/wp-content/uploads/2022/07/EG-Principles-for-Information-Exchange-Revised-July-2025.pdf [Accessed 1 Jun. 2026].
7. Financial Action Task Force (2012). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation.* [online] Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf?nocache=true [Accessed 1 Jun. 2026].
8. Financial Action Task Force (2014). *Transparency and Beneficial Ownership*. [online] Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-transparency-beneficial-ownership.pdf.coredownload.pdf [Accessed 31 May 2026].
9. Financial Action Task Force (2022). *Partnering in the Fight against Financial Crime*. [online] Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Partnering-int-the-fight-against-financial-crime.pdf [Accessed 1 Jun. 2026].

10. HM Government (2017). *Company Accounts Guidance*. [online] GOV.UK. Available at: https://www.gov.uk/government/publications/life-of-a-company-annual-requirements/life-of-a-company-part-1-accounts [Accessed 1 Jun. 2026].
11. Lee, J., Choi, G., Han, J. and Park, J. (2025). Advanced Monero wallet forensics: Demystifying off-chain artifacts to trace privacy-preserving cryptocurrency transactions. *Forensic Science International: Digital Investigation*, [online] 54, p.301988. doi:https://doi.org/10.1016/j.fsidi.2025.301988.
12. Lemmens, B. and Nussbaum, R.D. (2012). *Nonlinear Perron-Frobenius theory*. [online] Cambridge ; New York: Cambridge University Press. Available at: https://assets.cambridge.org/97805218/98812/excerpt/9780521898812_excerpt.pdf [Accessed 1 Jun. 2026].
13. Maroulis, N. (2026). SWIFT MX camt.053 in SEPA - A Detailed Analysis of Its Broad Use. doi:https://doi.org/10.2139/ssrn.6132206.
14. OCCRP (2019). *The Troika Laundromat*. [online] Organised Crime and Corruption Reporting Project. Available at: https://www.occrp.org/en/project/the-troika-laundromat [Accessed 1 Jun. 2026].
15. Rahman, S. (2024). *What is the difference between structuring and smurfing in money laundering?* [online] www.rahmanravelli.co.uk. Available at: https://www.rahmanravelli.co.uk/expertise/anti-money-laundering-investigations/articles/what-is-the-difference-between-structuring-and-smurfing-in-money-laundering-/ [Accessed 31 May 2026].
16. Shukla, A., Jirli, P., Mishra, A. and Singh, A.K. (2024). An overview of blockchain research and future agenda: Insights from structural topic modeling. *Journal of Innovation & Knowledge*, [online] 9(4), p.100605. doi:https://doi.org/10.1016/j.jik.2024.100605.
17. Truong, Q.D., Truong, Q.B. and Dkaki, T. (2016). Graph Methods for Social Network Analysis. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, [online] 168, pp.276–286. doi:https://doi.org/10.1007/978-3-319-46909-6_25.
18. Weeks-Brown, R. (2018). *Straight Talk: Cleaning Up*. [online] IMF. Available at: https://www.imf.org/en/Publications/fandd/issues/2018/12/imf-anti-money-laundering-and-economic-stability-straight [Accessed 31 May 2026].

THANK YOU

Network Analysis for Criminal Investigators:

How effective is network analysis in detecting money laundering?

2401049

Joshua.A.J.McManus

The University of Buckingham

BA (Hons) Security, Intelligence, and Cyber.