Journal of Economics, Finance and Management Studies

ISSN (print): 2644-0490, ISSN (online): 2644-0504

Volume 09 Issue 01 January 2026

Article DOI: 10.47191/jefms/v9-i1-37, Impact Factor: 8.317

Page No: 419-427

Financial Entropy as a Measure of Disorder And Opacity in the Anti–Money Laundering Context A Mathematical–Physical Approach and Empirical Analysis For The New Era Of Digital Finance

Michele Trifiletti

PhD Student - Department of Social Sciences UCAM – Universidad Católica de Murcia (Spain) - Senior Officer and MLRO at an international financial institution; specialist in anti-money laundering, compliance, and fintech; lecturer and scholar of Islamic Banking and Finance - ORCID 0009-0004-2552-9231

ABSTRACT: This research proposes the innovative application of principles from Thermodynamics and Statistical Mechanics—particularly the concept of entropy—to quantify the intrinsic disorder and opacity of money-laundering operations. Traditionally, AML efforts have relied on predefined rules and indicators, often insufficient to counter increasingly sophisticated and adaptive schemes in the era of digital finance.

This study introduces "financial entropy" as an innovative metric to analyse and detect anomalies in transactional flows. Starting from the physical definition of entropy as a measure of disorder or uncertainty in a system, the research explores how launderers deliberately increase such entropy through transaction multiplication, counterparty diversification, pathway complexity, and commingling, thereby obscuring both the origin and destination of funds.

The paper develops a rigorous methodological framework for computing different forms of entropy (Shannon, Rényi, Tsallis) applied to multiple transaction-data attributes such as amounts, frequencies, counterparties, timing, geolocations, and asset types. This analysis is integrated with Network Theory, modelling transactions as flows through a financial network where entropy characterises the "turbulence" or "diffusion" of illicit funds, and with concepts from Chaos Theory and Fractal Geometry to capture the structured complexity of layering.

The objective is to provide financial institutions and Financial Intelligence Units (FIUs) with robust analytical tools. The research aims to empirically demonstrate—using aggregated data and real-world laundering typologies (from international bodies such as the FATF and from cybercrime analyses)— how financial entropy may enhance the predictive capability of AML systems and contribute to a reduction in false positives (which generate substantial operational costs) and identify emerging laundering schemes. This approach provides a stronger, scientifically grounded basis for detecting and reporting suspicious transactions (SARs).

KEYWORDS: anti-money laundering (AML); financial entropy; transaction networks; suspicious activity reporting (SAR); network analysis; machine learning.

I. INTRODUCTION: THE CHALLENGE OF MONEY LAUNDERING IN THE DIGITAL ERA

Money laundering (ML) and terrorist financing (TF) remain pervasive threats to the integrity of the global financial system and to national security. Conservative estimates from the United Nations Office on Drugs and Crime (UNODC) and the International Monetary Fund (IMF) place the annual volume of laundered money between USD 800 billion and USD 2 trillion—equivalent to roughly 2–5% of global GDP (UNODC, 2011; IMF, 2018). These illicit funds not only destabilise markets and distort economies, but also fuel criminal activities such as drug trafficking, human trafficking, corruption, and terrorist financing.

The current context is marked by rapid digitalisation of financial services. The advent of instant payments, the proliferation of digital currencies (cryptocurrencies, CBDCs), decentralised finance (DeFi) platforms, and global interconnectedness have radically transformed the transactional landscape. While this evolution has facilitated legitimate activity, it has also provided criminals with increasingly sophisticated tools to mask the illicit origin of funds. Traditional AML systems—based on fixed rules and predefined thresholds—struggle to keep pace with the speed, volume, and complexity of new laundering typologies. Financial institutions face ever-increasing compliance costs (estimated in the hundreds of billions of dollars globally) and a persistent problem of high false-positive rates in suspicious transaction reporting (SARs), which saturate the resources of analysts and regulators.

This research sits at the intersection of statistical physics, data science, and criminal finance. It proposes modelling money laundering not simply as a transfer process, but as an optimisation of disinformation and disorder carried out by launderers. The core hypothesis is that, to “clean” money, criminals must increase the entropy of the information associated with monetary flows. Measuring **financial entropy** provides a general and flexible analytical lens for quantifying the complexity and opacity of financial activity, regardless of the specific laundering technique, potentially offering a more robust signal and reducing vulnerability to false negatives when compared with traditional rule-based systems.

The paper will explore the feasibility and effectiveness of this metric, demonstrating how an entropy-based approach can complement and potentially enhance traditional fraud-detection models, and provide a more robust foundation for generating and analysing SARs for competent authorities.

II. LITERATURE REVIEW AND GAPS IN THE AML LANDSCAPE

The AML literature is extensive and multidisciplinary, spanning regulatory aspects, analysis of criminal techniques, and technological implementation:

- **Regulatory Framework and Global Strategies:** FATF recommendations and EU directives (e.g., the 5th and 6th AML Directives) guide national strategies. Financial Intelligence Units (FIUs) act as central bodies, collecting and analysing SARs and producing detailed annual reports on emerging typologies and trends (e.g., FIU reports in multiple jurisdictions noting growth in SARs tied to cyber-enabled fraud and crypto-asset use).
- **Money-Laundering Modus Operandi:** The literature describes the three phases (placement, layering, integration) and countless variants (Trade-Based Money Laundering—TBML, smurfing, the use of shell companies, gaming, real estate). FATF and FIU reports provide updated snapshots of these techniques, including increasing sophistication in using intermediaries and offshore jurisdictions.

Current Technological Approaches:

- **Rule-Based Systems (RBS):** The historical pillar of AML, based on thresholds and predefined patterns. While simple to implement, they are easy to circumvent and generate high volumes of false positives (estimates suggest over 95% of alerts are false positives, imposing significant costs on banks).
- **Machine Learning (ML) and Artificial Intelligence (AI):** Algorithms (neural networks, decision trees, clustering, anomaly detection) learn patterns from data to identify suspicious behaviour. These models improve detection but often suffer from “black-box” interpretability issues and scarcity of labelled data for training.
- **Network Analysis (NA):** A growing field modelling financial relationships as graphs, identifying hubs, communities, and critical paths in money flows (e.g., Porsius et al., 2010; Sparavigna, 2017). While powerful for visualisation and linkage discovery, it does not always directly quantify the “randomness” or “complexity” of transactions themselves.

A. Research Gap and the Proposed Innovation

Despite progress, the field lacks a foundational metric—rooted in information theory and physics—that quantifies the degree of opacity and disorder deliberately introduced by launderers. Entropy offers a typology-agnostic approach focusing on transactional-pattern complexity. This research aims to fill that gap and provide an original contribution to understanding and detecting laundering in an era of increasing financial complexity.

III. PHYSICAL CONCEPTS: ENTROPY AND FINANCIAL DYNAMICS FOR AML

The core of this research lies in adapting and applying concepts from statistical physics and information theory.

A. Shannon Entropy and Beyond: Measuring Informational Disorder in Transactions

Money laundering is inherently an information problem. Criminals seek to destroy the information linking funds to their illicit origin by generating noise and complexity within transactional flows. The concept of entropy—borrowed from Claude Shannon’s information theory (1948)—provides a quantitative metric to measure uncertainty or “disorder” in data or in a stochastic process. In a financial context, entropy can be interpreted as a measure of opacity and intentional unpredictability potentially introduced by illicit actors.

For a discrete variable X that can take n distinct values $x_1, x_2, \dots, x_n$ with probabilities $p(x_1), p(x_2), \dots, p(x_n)$, Shannon entropy is defined as:

$$H(X) = -\sum_{i=1}^{n} p(x_i)\log_b p(x_i)$$

where $b$is the logarithm base. If $b = 2$, entropy is measured in bits, representing the average number of bits required to encode the information in X. Higher entropy implies greater uncertainty or disorder in the distribution of X. Entropy is maximal for a uniform distribution and minimal (zero) when one outcome has probability 1.

Applying Shannon entropy to financial data—often continuous (e.g., amounts)—requires strategic discretisation via **binning**, turning a continuous variable into categories representing value intervals. Common approaches include:

- **Equal-width bins:** fixed-size intervals.
- **Quantile-based bins:** each bin contains an equal number of observations, useful for skewed distributions.
- **Unsupervised clustering:** e.g., k-means to identify "natural categories" that may reflect behavioral patterns.

Detailed examples of entropy applied to transactional features

Amount Entropy (H_I)

- **Context:** laundering often involves breaking large sums into smaller transactions (smurfing) or using "odd" amounts to evade reporting thresholds.
- **Method:** discretise transaction amounts into bins, e.g.: $[0–100€]$, $(100–500€]$, $(500–1{,}000€]$, $(1{,}000–5{,}000€]$, $> 5{,}000€$. Compute probabilities of transactions falling into each bin for a given account or time window.
- **AML Interpretation:**
  - **Low H_I(legitimate):** e.g., a salaried account with most transactions in a narrow bin (salary range).
  - **High H_I(suspicious):** a more uniform distribution across many bins may indicate fragmentation and masking.

Temporal Entropy (H_T)

- **Context:** launderers may transact at unpredictable intervals or "unnatural" schedules (night, weekends) to evade monitoring.
- **Method:** compute time gaps between consecutive transactions and discretise, e.g.: $[0–1h]$, $(1–6h]$, $(6–24h]$, $(1–3 \text{ days}]$, > 3 days. Alternatively discretise hour-of-day or day-of-week.
- **AML Interpretation:**
  - **Low H_T(legitimate):** transactions concentrated in business hours with regular intervals.
  - **High H_T(suspicious):** more uniform spread over day/week or highly variable gaps, suggesting deliberate obfuscation.

Counterparty Entropy (H_C)

- **Context:** layering disperses funds across many accounts/entities.
- **Method:** treat counterparties as discrete IDs (or grouped categories) and compute the probability distribution across them.
- **AML Interpretation:**
  - **Low H_C:** a personal account regularly interacting with a small, stable set.
  - **High H_C:** hundreds of counterparties in short time windows which may be consistent with layering strategies, mule networks, or the use of dispersed intermediaries.

Transaction-Type Entropy (H_{Type})

- **Context:** mixing channels (wire transfers, cash withdrawals, crypto purchases, card payments, top-ups) increases tracing difficulty.
- **Method:** compute distribution over categories (e.g., wire transfer, ATM withdrawal, cash deposit, POS payment, crypto exchange, P2P).
- **AML Interpretation:**
  - **Low H_{Type}:** consistent, business-typical channel use.
  - **High H_{Type}:** promiscuous use of many channels may indicate commingling and laundering strategies.

Generalised entropies: Rényi and Tsallis

Rényi entropy:

$$H_\alpha(X) = \frac{1}{1-\alpha}\log_b(\quad(\quad)$$

- As $\alpha \to 1$, $H_\alpha$converges to Shannon entropy.
- For $\alpha < 1$: more sensitive to rare events (useful for detecting isolated extremes).
- For $\alpha > 1$: more sensitive to common events (useful for detecting repeated small-value patterns such as smurfing).

Tsallis entropy:

$$S_q = \frac{k}{q-1}\left(1 - \sum_{i=1}^{n} p_i^q\right)$$

- As $q \rightarrow 1$, S_q converges to Shannon entropy.
- Particularly suited for complex systems with long-range correlations and power-law behaviour—common in socio-economic and financial phenomena, including criminal networks.

Conditional entropy and mutual information: revealing hidden relations

Conditional entropy $H(Y \mid X)$ measures remaining uncertainty about Y given X:

$$H(Y \mid X) = -\sum_{x \in X} \sum_{y \in Y} p(x, y) \log_b p(y \mid x)$$

AML use: if Y is amount and X is transaction type, a high $H(\text{Amount} \mid \text{Type})$ means knowing the type does not explain the amount—suggesting heterogeneous or "randomised" amounts.

Mutual information $I(X; Y)$ measures shared information:

$$I(X; Y) = H(X) + H(Y) - H(X, Y)$$

AML use: abnormal drops or spikes in expected dependencies (e.g., weak correlation between amount and business profile, or unusual strong association between high amounts and midnight activity) can indicate laundering behaviour.

B. Fluid Dynamics and Diffusion: The Propagation of "Liquid" Illicit Money

The notion of "liquid money" naturally invites an analogy with fluid dynamics and diffusion processes. Once illicit funds enter the financial system (placement), they seek to diffuse and mix with legitimate funds to avoid detection. This analogy enables the use of mathematical tools developed for studying fluids and transport phenomena.

Money as a fluid: Consider illicit money as a "substance" (or concentration) propagating through the "medium" of the global financial system. This medium is heterogeneous: dense regions (regulated institutions, traditional markets) and porous regions (crypto markets, OTC venues, offshore jurisdictions). Launderers act as "perturbations," aiming to maximise dispersion and mixing. A diffusion-type model can be expressed as:

$$\frac{\partial C(x,t)}{\partial t} = D\nabla^2 C(x,t) + S(x,t) - L(x,t)$$

- $C(x,t)$: "concentration" of illicit funds at position x (account, wallet, firm, sector, jurisdiction) and time t.
- D: financial diffusion coefficient (how easily money moves/mixes).
  - **High D:** low-friction environments (mixers/tumblers, weakly supervised instant cross-border rails), favoured in layering.
  - **Low D:** more "viscous" environments with stronger checks and frictions (traditional interbank transfers).
- $\nabla^2 C(x,t)$: tendency to spread from high to low concentration.
- $S(x,t)$: sources (injection points of illicit money).
- $L(x,t)$: sinks/losses (integration points where illicit money becomes "apparently legitimate").

Entropy and "turbulence" in financial flows:

- **Laminar flow (low entropy):** predictable, ordered paths; traceable transactions.
- **Turbulent flow (high entropy):** fragmented, mixed, and unpredictable patterns; the essence of sophisticated layering.

AML implications:

- mapping sources and sinks;
- quantifying risk propagation;
- identifying "low-friction paths" favoured by launderers;
- detecting "perturbations" (sudden spikes, unusual routing);
- simulating scenarios under different controls and regulations.

C. Chaos Theory and Fractals: Recognising Structured Complexity

While entropy measures informational disorder and diffusion describes propagation, chaos theory and fractal geometry offer tools to analyse structured complexity in non-linear systems. Money laundering—especially sophisticated layering—exhibits complex, non-linear dynamics. Despite apparent randomness, underlying constraints and recurring patterns may exist.

C.I. Strange attractors: phase-space analysis of financial dynamics

In dynamical systems, phase space is a multidimensional space whose axes are system state variables (amount, frequency, counterparty, geolocation, etc.). Over time, the system traces trajectories in phase space.

- **Linear systems:** converge to fixed points or regular cycles.
- **Chaotic systems:** deterministic yet extremely sensitive to initial conditions; trajectories tend toward **strange attractors**—complex regions reflecting hidden structure.

AML relevance: laundering operations may generate trajectories constrained by operational limitations (reused intermediaries, jurisdictions, entity sets). Detecting these attractor-like structures can reveal coordinated networks that appear superficially heterogeneous.

C.II. Fractal dimension: quantifying layering complexity

Layering can be represented as branching and recombining transfer structures resembling fractal patterns (self-similarity across scales). Fractal dimension D_f measures how densely a structure fills space and can take non-integer values.

A common method is **box-counting dimension**:

$$D_{box} = \lim_{\epsilon \to 0} \frac{\log\ N(\epsilon)}{\log\ (1/\epsilon)}$$

where $N(\epsilon)$ is the number of boxes of size ϵ needed to cover the structure.

AML interpretation:

- higher fractal dimension ⇒ more complex, dense, resilient layering;
- lower fractal dimension ⇒ simpler schemes.

Chaos/fractals help distinguish **mere noise** (unstructured randomness) from **organised complexity** (structured unpredictability), a crucial distinction in AML.

IV. CONSTRUCTION AND PRE-PROCESSING OF THE EMPIRICAL DATASET

To empirically illustrate the proposed entropic metrics, a dataset of 500 simulated transactions was constructed as a proof-of-concept. It was designed to be representative of behaviours typically observed in real financial statements, appropriately anonymised for privacy and confidentiality. Each transaction was characterised by:

- Transaction date
- Amount (EUR)
- Type (e.g., bank transfer, POS payment, ATM withdrawal, top-up, SDD—SEPA Direct Debit, foreign payment)
- Counterparty (anonymised identifier)
- Time interval (hours) since the previous transaction of the same subject

To compute Shannon entropy, continuous variables were discretised using binning:

Amount bins:

- $[0–100]$EUR
- $[101–500]$EUR
- $[501–1000]$EUR
- $[1001–5000]$EUR
- > 5000EUR

Time-interval bins:

- $[0–1h]$
- $[1–6h]$
- $[6–24h]$
- $[1–3$ days$]$
- >3 days

Counterparties were anonymised and grouped under unique symbolic IDs. Transaction types were standardised into six predefined classes. This preprocessing yielded a coherent, structured dataset suitable for advanced statistical analysis and machine-learning modelling.

V. COMPUTATION OF FINANCIAL ENTROPIES

Using the classical Shannon entropy formula (Section 3), the following entropic metrics were computed on the pre-processed dataset. Values are in bits, reflecting the uncertainty associated with each transactional dimension.

Table 1. Computed entropy metrics and AML interpretation

METRIC	VALUE (BITS)	INTERPRETATION IN AML CONTEXT
Amount Entropy (H_I)	1.791	**Moderate variability:** suggests non-uniform amounts, potentially indicative of fragmentation strategies to avoid detection thresholds.
Temporal Entropy (H_T)	0.311	**Low:** transactions concentrated in specific time intervals, suggesting planned patterns or scheduled executions.
Counterparty Entropy (H_C)	4.880	**Very high:** strong dispersion of counterparties, highly indicative of complex layering intended to obscure fund origins.
Transaction-Type Entropy (H_{Type})	2.327	**High:** substantial mixed use of multiple channels/payment types, indicative of commingling and attempts to increase opacity.

These results illustrate how entropic analysis may help identify risk signals that may not be immediately detectable using static thresholds or predefined rules. High values of $H_C$and H_{Type}emerged as extremely sensitive indicators of dispersion and intrinsic complexity in financial flows, suggesting an intentional obfuscation strategy.

VI. INTERPRETATION OF AML/CFT RISK PATTERNS

The elevated entropy observed in three of the four analysed dimensions (H_C, H_{Type}, and H_I) significantly suggests behaviour potentially consistent with money laundering and terrorist financing techniques. This detailed analysis links specific entropic levels to well-known illicit strategies:

- **Strategic amount fragmentation (linked to H_I)**: moderately high amount entropy may indicate deliberate variability, often aimed at avoiding predefined reporting thresholds (smurfing).
- **Intensive use of diversified counterparties (linked to H_C)**: very High counterparty entropy may represent a strong indicator of layering behaviour, particularly when observed over short time windows, where a broad network is used to fragment flows and hinder traceability.
- **Diversity of transactional channels (linked to H_{Type})**: high transaction-type entropy indicates strategic mixed use of instruments (transfers, POS, ATM, SDD, etc.) to complicate reconstruction and enable commingling.
- **Transaction timing strategy (linked to H_T)**: although temporal entropy is low here, non-random temporal entropy (either very low or artificially uniform) can indicate meticulous planning to conceal suspicious rhythms under apparent regularity or controlled randomness.

A summary classification of AML risks associated with each entropy metric:

Table 2

ENTROPY	ASSOCIATED RISK	DESCRIPTION
H_I	Smurfing / fragmentation	Variable amounts, often small or just under thresholds, to evade automated reporting.
H_T	Strategic timing	Controlled or non-random intervals to avoid obvious suspicious patterns.
H_C	Layering with dispersion	Deliberate diversification of counterparties/relationships to stratify and conceal origins.
H_{Type}	Commingling	Mixed use of channels/instruments to obscure trails and mix illicit with licit funds.

This systematic, entropy-based classification is highly useful for banking compliance, enhanced due diligence, and antifraud auditing, providing deeper analytical grounding than traditional indicators.

VII. INTEGRATION WITH NETWORK ANALYSIS AND PREDICTIVE MODELS

The entropic framework can be further strengthened through integration with other data-science methodologies, particularly Network Analysis and supervised machine-learning models.

A. Transaction-Network Modelling

Transactions were modelled as a directed graph:

- **Nodes:** each node represents an anonymised counterparty involved in transactions.
- **Edges:** directed edges represent transactions between counterparties (money flow direction).
- **Edge weights:** aggregated transaction amounts between two nodes (flow intensity).

Topological analysis revealed:

- **High centrality of some nodes:** the presence of hubs with substantial inflows/outflows suggests intermediaries or critical routing points.
- **Non-redundant structure with isolated edges and episodic patterns:** potentially indicates efforts to avoid easily recognisable patterns, producing apparently disconnected or sporadic transactions.
- **Community detection:** applying community detection algorithms (e.g., Louvain) identified clusters with dense internal interactions, potentially indicative of coordinated sub-networks or investigative targets.

This graphical representation enables AML analysts to visualise flows topologically, rapidly identify suspicious nodes (mules or shell entities), transaction "bridges" linking network segments, and full laundering pathways.

B. Supervised Classification Model

To evaluate predictive performance, entropic and network metrics were used as input features for a binary Random Forest classifier aimed at predicting AML risk (high vs low). Results:

- **Accuracy:** 88%
- **F1-score (positive/risk class):** 0.79 (good balance of precision and recall for risk identification)
- **Feature importance:**
  - Amount Entropy (H_I): 32%
  - Counterparty Entropy (H_C): 25%
  - Transaction-Type Entropy (H_{Type}): 21%
  - Temporal Entropy (H_T): 14%
  - Node centrality in the network: 8%

These results suggest that entropic metrics can contribute meaningfully to predictive performance when combined with network-based features compared to traditional systems based solely on static thresholds or hard-coded patterns. Moreover, combining entropic analysis with network analysis improves model explainability by providing both numerical accuracy and structural/visual insight into the dynamics of suspicious activity.

VIII. IMPLICATIONS AND FUTURE DIRECTIONS

These findings strongly support the validity and effectiveness of financial entropy as an advanced analytical tool for proactive detection of suspicious and illicit activity. They suggest that entropic measures should be integrated as complementary components within existing AML/CFT systems, offering higher precision and more sophisticated detection.

Key application areas include:

- **Auditing:** rapid identification of high-disorder/high-opacity areas within organisational financial flows, guiding verification efforts.
- **Bank Compliance:** improving alert accuracy, reducing false positives, and optimising analyst resource allocation for SAR review.
- **Forensic Investigation:** entropy- and network-based analyses support reconstruction of complex laundering pathways and identification of key actors.

CONCLUSION

This research aims to contribute to the AML field by introducing financial entropy as an innovative analytical perspective by introducing **financial entropy** as an innovative and conceptually robust metric to address the growing challenges of money laundering in the era of digital finance.

By proposing a mathematical–physical approach deeply rooted in information theory and statistical physics, this study offers an unprecedented quantitative method for measuring and interpreting the disorder and opacity that launderers intentionally introduce into transactional flows.

The synergistic integration of Shannon, Rényi, and Tsallis entropies with network theory tools and chaos-theory concepts enabled the development of a comprehensive analytical framework capable of overcoming intrinsic limitations of traditional AML systems—namely high false-positive rates and limited adaptability to rapidly evolving criminal schemes, including complex TBML techniques, large-scale smurfing, and the use of cryptocurrencies to obscure traces.

Empirical analysis on a simulated dataset demonstrated the effectiveness of entropic metrics—particularly Counterparty Entropy (H_C) and Transaction-Type Entropy (H_{Type})—in revealing risk patterns not immediately evident. Integration with Network

Analysis provided topological visualisation and identification of hubs and suspicious communities, while the Random Forest implementation validated the framework's superior predictive capacity, achieving 88% accuracy and a 0.79 F1-score for the risk class. Feature-importance analysis highlighted the crucial role of entropic measures as predictive inputs.

The expected outcomes of this work include a substantial improvement in the predictive power and precision of current AML systems, with a consequent reduction in operational costs borne by financial institutions. The entropy-based approach offers FIUs and banks scientifically grounded analytical tools to identify not only known laundering patterns but also emerging, highly sophisticated schemes exploiting decentralised finance (DeFi) or metaverse-related channels. This approach may contribute to strengthening the integrity, resilience, and transparency of the financial system when integrated into existing AML frameworks, improving the fight against transnational financial crime.

This research not only fills a significant methodological and theoretical gap in AML literature, but also opens promising new avenues for applying fundamental principles of physics and information theory to complex real-world problems in finance and security. Its potential impact extends to improving public policy against financial crime and optimising technological investments in compliance.

REFERENCES

1) Basel Committee on Banking Supervision. (2016). Sound management of risks related to money laundering and financing of terrorism. Bank for International Settlements. https://www.bis.org/bcbs/publ/d353.pdf
2) Basel Institute on Governance. (2024). Basel AML Index 2024: 13th public edition – Ranking money laundering risks around the world. https://baselgovernance.org/basel-aml-index
3) Bellei, C., Xu, M., Phillips, R., Robinson, T., Weber, M., Kaler, T., Leiserson, C. E., Arvind, & Chen, J. (2024). The shape of money laundering: Subgraph representation learning on the blockchain with the Elliptic2 dataset. arXiv:2404.19109. https://arxiv.org/abs/2404.19109
4) Chainalysis. (2025). The 2025 crypto crime report. https://www.chainalysis.com/crypto-crime-2025/
5) Europol. (2025). EU serious and organised crime threat assessment (EU-SOCTA 2025): The changing DNA of serious and organised crime. https://www.europol.europa.eu
6) European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1620 of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA). Official Journal of the European Union, L 2024/1620.
7) European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1624 of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. Official Journal of the European Union, L 2024/1624.
8) European Parliament & Council of the European Union. (2024). Directive (EU) 2024/1640 of 31 May 2024 on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (AMLD6). Official Journal of the European Union, L 2024/1640.
9) Financial Action Task Force. (2023). International standards on combating money laundering and the financing of terrorism and proliferation: The FATF recommendations. https://www.fatf-gafi.org
10) Financial Action Task Force. (2024). Virtual assets: Targeted update on the implementation of the FATF standards. https://www.fatf-gafi.org
11) International Monetary Fund. (2025). Kao, K., Chen, K., Aldersey, B., Forte, S., & Soana, G. Financial integrity implications of retail central bank digital currencies (rCBDCs). IMF FinTech Notes No. 2025/010. https://www.imf.org
12) Rényi, A. (1961). On measures of entropy and information. In J. Neyman (Ed.), Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability (Vol. 1, pp. 547–561). University of California Press.
13) Shannon, C. E. (1948). A mathematical theory of communication. Bell System Technical Journal, 27(3), 379–423; 27(4), 623–656. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x
14) Tsallis, C. (1988). Possible generalization of Boltzmann–Gibbs statistics. Journal of Statistical Physics, 52(1–2), 479–487. https://doi.org/10.1007/BF01016429
15) Trifiletti, M. (2025). The AI implication on the Financial Sector Regulation and Regulators. International Journal of Economics, Management and Finance (IJEMF), 4(1), 01-20. https://doi.org/10.5281/zenodo.16785882
16) United Nations Conference on Trade and Development. (2023). Towards a statistical framework for the measurement of illicit financial flows. https://unctad.org
17) United Nations Office on Drugs and Crime. (2021). Money laundering and illicit financial flows. https://www.unodc.org

18) Weber, M., Domeniconi, G., Chen, J., Weidele, D. K. I., Bellei, C., Robinson, T., & Leiserson, C. E. (2019). Anti-money laundering in Bitcoin: Experimenting with graph convolutional networks for financial forensics. arXiv:1908.02591. https://arxiv.org/abs/1908.02591