“Blockchain network complexity and illicit transaction detection: Machine-learning evidence from the Elliptic Bitcoin benchmark”

AUTHORS	Ayman Mansour Khalaf Alkhazaleh
ARTICLE INFO	Ayman Mansour Khalaf Alkhazaleh (2026). Blockchain network complexity and illicit transaction detection: Machine-learning evidence from the Elliptic Bitcoin benchmark. *Investment Management and Financial Innovations*, *23*(3), 383–398. doi:10.21511/imfi.23(3).2026.27
DOI	http://dx.doi.org/10.21511/imfi.23(3).2026.27
RELEASED ON	Wednesday, 26 August 2026
RECEIVED ON	Saturday, 21 March 2026
ACCEPTED ON	Wednesday, 05 August 2026
LICENSE	This work is licensed under a Creative Commons Attribution 4.0 International License
JOURNAL	"Investment Management and Financial Innovations"
ISSN PRINT	1810-4967
ISSN ONLINE	1812-9358
PUBLISHER	LLC “Consulting Publishing Company “Business Perspectives”
FOUNDER	LLC “Consulting Publishing Company “Business Perspectives”

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
57	0	8

© The author(s) 2026. This publication is an open access article.

BUSINESS PERSPECTIVES

LLC "CPC "Business Perspectives"
Hryhorii Skovoroda lane, 10,
Sumy, 40022, Ukraine

www.businessperspectives.org

Ayman Mansour Khalaf Alkhazaleh (Jordan)

BLOCKCHAIN NETWORK COMPLEXITY AND ILLICIT TRANSACTION DETECTION: MACHINE-LEARNING EVIDENCE FROM THE ELLIPTIC BITCOIN BENCHMARK

Abstract

The blockchain financial system allows users to send money fast without any border restrictions. However, the same structure of the blockchain may be used as a means of laundering money. This paper assesses the relationship between the complexity of transaction networks and the likelihood of their illicit nature within the public Elliptic Bitcoin benchmark and examines whether anomaly detection using machine learning helps to interpret risks from an AML/CFT perspective. This empirical analysis assumes that Elliptic provides an anonymized transaction network in which nodes correspond to Bitcoin transactions, edges reflect directed transactions, and anonymized features facilitate licit/illicit classification of transactions. Furthermore, the dataset is not considered evidence of sender wallet addresses, receiver wallet addresses, transaction amount, timestamp, ownership of exchanges, user geography, and national AML/CFT effectiveness. Based on the labelled analytical dataset presented in the uploaded workbook (46,564 observations, including 42,019 licit transactions and 4,545 illicit transactions), a logit model found a significant positive correlation between illicit transactions and degree centrality (beta = 1.870, $p < 0.001$), clustering coefficient (beta = 0.940, $p < 0.001$), and flow entropy (beta = 0.680, $p < 0.001$). Isolation Forest and Autoencoder reached AUCs of 0.866 and 0.841, respectively. In turn, the coefficient measuring a country's regulatory capacity and its interaction term are not included in the estimation because there is no country-window marginal effect. Therefore, this paper does not test for the impact of regulatory capacity of the USA, Singapore, and UAE on transaction classification.

Keywords cryptocurrency, illicit, anonymity, centrality, clustering, entropy, compliance

JEL Classification G28, K42, O33

Type of the article: Research Article

Received on: 21st of March, 2026
Accepted on: 5th of August, 2026
Published on: 26th of August, 2026

© Ayman Mansour Khalaf Alkhazaleh, 2026

Ayman Mansour Khalaf Alkhazaleh, Associate Professor, Faculty of Business, Department of Accounting and Finance, Middle East University, Jordan.

This is an Open Access article, distributed under the terms of the Creative Commons Attribution 4.0 International license, which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

Conflict of interest statement:
Author(s) reported no conflict of interest

INTRODUCTION

The adoption of blockchain technology in finance has increased the efficiency, speed, and scope of global financial transactions. On the flip side, the same decentralization that makes global transactions possible has created new openings for illicit activities in the form of crypto-money laundering. The core scientific issue, therefore, is not just that transactions facilitated through blockchain can be used to carry out illicit financial activities but that the transparency provided by blockchain transactions co-exists with a lack of accountability among the entities involved in such transactions, creating an inherent contradiction of transparency-anonymity in the field of digital finance (Wronka, 2022; Bajra et al., 2024).

This poses serious problems for regulation and enforcement in the field. Blockchain transactions cannot be deleted or tampered with, making

them technically auditable, yet it is possible for parties involved in the transactions to retain their anonymity. Moreover, the high degree of mobility associated with digital platforms and fragmentation of institutions create opportunities to evade oversight and enforcement when supervisory regimes have divergent regulatory preparedness, investigative capabilities, and enforcement effectiveness. The situation gets even more complicated in transnational cases, where offenders resort to transferring their operations into locations with low coordination of regulation, poor compliance efforts, and slow supervision learning (Benson et al., 2024; Bensassi & Raz, 2025).

Adjacent research on digitally mediated information environments shows that platform-based information flows are shaped by media structures and user participation (Al-Muntasir, 2022). Research on professional communicators likewise indicates that social-media platforms can affect information-selection priorities (Ahmad et al., 2023). In organisational settings, remote communication can mediate the relationship between electronic management practices and organisational performance (Taqa, 2025). User-level evidence also shows that platform features, usage motives, and gratifications shape engagement with digital media environments (Oreqat, 2021). Collectively, this adjacent literature situates blockchain analytics within a wider digital-information environment in which platform design and communication processes shape observable information patterns.

Evidence from Jordanian banking similarly indicates that successful AI and FinTech adoption depends on regulatory alignment, infrastructure, and technological readiness (Othman, 2025).

While research regarding crypto-money laundering has proliferated in recent years, the problem remains inadequately solved. On the one hand, technical research focuses on anomaly detection, precision, and network analysis, whereas institutional approaches deal with the issues of compliance architecture, enforcement, and deterrence. However, a problem-centered approach, which could explain how transaction-network complexity can be assessed cautiously using benchmark data and provide insights into AML/CFT, remains largely underdeveloped. This is because crypto-money laundering not only raises technical problems related to tracking transactions but also institutional issues pertaining to the assessment of risks through anonymous benchmarks (Morshed & Khrais, 2025; Wronka, 2022).

1. LITERATURE REVIEW AND HYPOTHESES

Despite the fast-growing number of publications in relation to blockchain finance and illicit finance, research can be separated into two groups: suspicious transaction studies and institutional studies concentrating on regulation and supervision. The difference between these categories of studies is important since crypto money laundering (CML) cannot be considered either as a purely technological problem or a legislative challenge; rather, the CML is the product of the interaction between transaction nature, platform features, regulatory capacity, and arbitrage opportunities. Thus, the current review is intended to link the principles of money laundering to the features of blockchain and the institutional context within which states try to regulate digital finance (Morshed & Khrais, 2025; Usman et al., 2025; Wronka, 2022).

The difference between CML and regular money laundering performed using financial intermediaries is that CML combines the features of auditability and anonymity. Though there are ledgers on the blockchain which allow recording all transactions, the identity and location of users are difficult to prove, and this creates the main conflict discussed in the literature under the title of the paradox of transparency and anonymity (Bajra et al., 2024; Wronka, 2022). Compared to traditional launderers, who require considerable reliance on banks and financial intermediaries, the development of decentralized finance decreases the necessity for gatekeeping and increases the variety of wallets, protocols, and exchanges through which value may be layered and moved. In this sense, the development of digital finance ecosystems has not only made money laundering easier and faster but has also provided new possibilities in this domain (Benson et al., 2024; Usman et al., 2025).

http://dx.doi.org/10.21511/imfi.23(3).2026.27

The regulatory challenge is further complicated by the fragmentary nature of CML governance regimes. For example, debates on FATF suggest that the lack of coordination of regulatory enforcement, inconsistencies produced by it, and jurisdiction shopping are the major problems in this domain (Bensassi & Raz, 2025; Cheng & Wen, 2025). At the same time, some research points to the fact that countries at an early stage of development should face the most complicated process of adaptation since they adopt new technologies faster than their institutions develop (Urooj, 2024; Wronka, 2023). Under conditions when the regulatory capacity varies, launderers not only benefit from pseudonymity but also use regulatory arbitrage, moving money across jurisdictions that operate under different norms. The outlined situation can be interpreted in the context of the political economy of secrecy, diversity of rules, and fragmented regulations examined in the literature devoted to international regulatory competition and cross-border secrecy (Bastiaens et al., 2025; Fröhlich, 2024; Meier et al., 2023).

On the other hand, existing evidence suggests that CML can be tracked through transactions. Research into forensic analysis in the field of blockchain and crypto finance suggests that laundering activities can be detected regardless of the measures used by launderers, including hop chains and tumblers, microtransactions, etc. (Agarwal et al., 2024; Pandurangan et al., 2024). Empirical work within the anti-financial crime realm suggests that anomalies may be detected even where laundering operations follow complex and sophisticated patterns of transactions; illegal communities may be identified via temporal centrality analysis (Asiri & Somasundaram, 2025; Kamuhanda et al., 2023; Phan, 2025; Vilella et al., 2025). The significance of this body of work lies in establishing that blockchain's inherent complexity need not stand in the way of its analytical utility.

Where transaction traces can be detected, the critical question is how law, policy, and enforcement make such patterns visible to authorities. In the context of AML/CFT governance, the examples of the United States, Singapore, and the UAE serve as different types of policy paradigms: a regime centered on enforcement, adaptive licensing, and cross-agency cooperation in Singapore, and financial crime reform efforts in the UAE (Fuda, 2025; Onufer, 2022; Sultan et al., 2024). These jurisdictions are used only as policy reference points in this article, as no partition of the Elliptic benchmark into US, Singaporean, or UAE transactions is available.

While differences in institutional settings may affect compliance and enforcement effectiveness, such differences cannot be established without a replicable tagging protocol and verified time-stamped country attribution of the addresses used in the transactions. The country-specific discussion below is therefore interpretative and conservative, focusing on AML/CFT capacity as a factor relevant to the dataset's policy relevance. No claims are made that the transactions in the Elliptic benchmark correspond to the country labels in any statistically meaningful way (Balaskas et al., 2024; Dote-Pardo & Severino-González, 2025; Y. Zhang & Q. Zhang, 2025).

In addition to the literature on institutional settings in which compliance occurs, the field of anti-money laundering has witnessed a methodological turn. Classical compliance approaches rely heavily on rule-based approaches, expert judgment, and anomaly detection. In doing so, they are frequently faulted for their high rates of false positive predictions (Akartuna et al., 2024). Survey and systems reviews show a strong shift towards machine learning and artificial intelligence in anti-money laundering applications (Ozkan-Okay et al., 2024; Parycek et al., 2024). Unsupervised methods of anomaly detection based on algorithms like Isolation Forest, autoencoders, One-Class SVM, and their combinations are highly popular in this domain owing to relatively low rates of suspicious transactions and difficulties of formulating precise detection rules a priori (Haque & Soliman, 2025; Maheswari et al., 2024). Concurrently, however, activity-based research highlights the importance of interpreting algorithm output with regard to opportunity structures (Lokanan, 2025).

An additional advantage of graph-based analytics is that blockchain transactions allow for representation as networks rather than isolated incidents, providing opportunities to assess degree centrality, local density of interactions, and variability of value flow. While contemporary methodological

literature recognizes the value of network measures in fraud and anomaly detection, there are also important implementation-related considerations. Estimation of centrality may vary with the choice of the filtering approach, normalization can have a substantial effect on comparability between time slices, and the use of interpretability measures such as SHAP values may be supplemented by other measures of variable importance (D. Frąszczak & T. Frąszczak, 2024; Lima & Souza, 2023; Wang et al., 2024). First of all, the general trend of AML governance research indicates the necessity to test the validity of interpretation of compliance indicators and risk scores as latent constructs especially in combination with institutional variables or indices (Hamed et al., 2024; Alkire et al., 2022; Frey & Tatum, 2022).

Second, the literature indicates that the nodes participating in transactions close to the center of the illicit network or located in dense transaction clusters tend to be more associated with suspicious behavior. Community detection and centrality research highlights the need to take into account transaction topology to detect laundering opportunities that can not be detected using only transaction label (Andrei & Veltri, 2025; Kamuhanda et al., 2023; Vilella et al., 2025). However, as was mentioned above, the discussed research tends to be institutionally thin – either ignoring the institutional environment or treating it as exogenous. At the same time, the literature on laundering and compliance pays little attention to opportunities emerging from the transaction structure. Fintech regulation studies tend to bridge this gap investigating the effect of financial regulation on laundering exposure, but there is very limited transaction-level evidence available (Li et al., 2021; Parycek et al., 2024; Usman et al., 2025).

Here the Routine Activity Theory becomes relevant. This theory states that crime occurs at the intersection of motivated offenders, suitable target, and weak guardianship. Blockchain technology increases the number of the first two factors while decreasing the latter. Thus, centrality, clustering, and entropy can be viewed as proxies for opportunity structures (Ofori & Appiah, 2025; Zhon & Asiama, 2022). The critics of the theory argue that opportunity alone can not explain the effect of identical technological conditions in different countries due to institutional and political differences (Dávid-Barrett, 2024; Lokanan, 2025).

The Institutional Theory provides an additional framework, focusing on the coercive, normative, and mimetic forces shaping the higher/lower level of compliance of organizations and markets with the regulation. In the realm of AML/CFT, the existence of effective institutions creates the expectations of supervision, reporting, coordination, and sanctions increasing guardianship in the technologically flexible environment. The application of the theory to the sphere of AI and compliance has been confirmed in the adjacent literature (DiMaggio & Powell, 1983; Li et al., 2021). Similarly, FATF standards and recommendations are studied for the effects of institutions on AML/CFT governance practices in emerging and transitional countries (Cheng & Wen, 2025; Nanyun & Nasiri, 2021; Urooj, 2024).

Lastly, Risk-Based Regulation provides a theoretical framework for reconciling institutional and behavioral perspectives by pointing out the need for prioritization of scarce attention to risky cases. Instead of applying one-size-fits-all approach to entities and transactions, risk-based frameworks emphasize the need to adapt dynamically to changing risks. In the context of blockchain, this requires building a system of surveillance able to conduct analytics and detect structurally suspicious nodes, flows, and clusters. Studies in risk-based governance illustrate the significance of such alignment (Gavira-Durón et al., 2022; Paul, 2024). From the point of view of policy theory, it implies that such alignment would yield better results: improved risk-based detection, reporting, prioritization of supervision, and proportionate intervention. The more developed an institutional capacity of a country in AML/CFT governance is, the lower is the probability of suspicious transactions. But this paper does not try to measure such relationship (Balaskas et al., 2024; Saggese et al., 2024).

Overall, three aspects can be identified in the literature. Firstly, the network of blockchain transactions contains measurable structural signals allowing to detect suspicious behavior. Secondly, machine learning models are able to transform

http://dx.doi.org/10.21511/imfi.23(3).2026.27

such signals into valuable evidence of anomaly and classification as long as the graph construction is clear. Finally, regulatory capacity is significant for interpretation and policy relevance, but statistical relationship to transaction-level benchmark labels must be avoided until the layers of regulation, time and exchanges are reproducibly aligned. This study therefore evaluates transaction-network complexity in the Elliptic Bitcoin benchmark and discusses comparative AML/CFT governance implications without treating the benchmark as direct evidence of national incidence or user geography. Study hypotheses are as follows:

H1: Higher transaction centrality, clustering, and flow entropy are positively associated with the probability of illicit blockchain activity in the labelled benchmark.

H2: Unsupervised anomaly scores are positively aligned with labelled illicit classification in the benchmark validation stage.

H3: Network-complexity indicators contribute materially to model interpretability and illicit-transaction classification performance.

2. METHODOLOGY

This study uses a quantitative, benchmark-based, and data-driven design to test whether transaction-network complexity is associated with illicit classification in an anonymized Bitcoin transaction graph. The empirical procedure follows four steps:

1) document and preprocess the public Elliptic transaction graph according to its benchmark structure;

2) compute complexity metrics such as centrality, clustering, and flow entropy from the transaction-node graph;

3) generate anomaly scores using unsupervised detection models and benchmark those signals on the labelled subset; and

4) estimate a logit-based inferential model using the labelled illicit outcome.

The US, Singapore, and the UAE are kept as contextual AML/CFT examples only, and not as actual partitioning of the Elliptic benchmark.

Public benchmarks and publicly available regulatory datasets are incorporated into this study; however, their functions differ in the new model design. The calibration dataset involves the use of Elliptic Data, which is a graph of anonymized Bitcoin transactions with licit, illicit, and unknown labels (Weber et al., 2019). For benchmarking purposes, publicly available regulatory indicators for 2018–2024 are applied only to describe the AML/CFT regulatory environment. When speaking of the Basel AML Index, it should be noted that in such cases it is treated as initially intended, that is, a jurisdiction-level score reflecting ML/TF risk, and not AML/CFT capacity. (Basel Institute on Governance, 2024). This distinction is important because the regulatory layer supplies contextual interpretation, whereas the Elliptic benchmark supplies the transaction-level calibration base for model estimation and validation.

The Elliptic benchmark is not treated as transparent wallet-level sender-receiver data. In the revised design, each observation is an anonymized transaction node, edges represent directed payment flows, and the feature set is used only in its anonymized benchmark form. The public benchmark contains 203,769 transaction nodes, 234,355 directed payment-flow edges, 166 anonymized node features, and 49 temporal steps. The labelled analytical subset used for supervised and inferential estimation contains 46,564 transaction-node observations, comprising 42,019 licit and 4,545 illicit observations. Unknown-class observations are excluded from supervised and inferential licit/illicit models and are not coded as licit cases. Preprocessing therefore focuses on class handling, feature standardization, graph consistency, and duplicate-record checks rather than on unverified wallet-address, transaction-hash, transaction-amount, exchange, timestamp, or national-attribution filtering.

Data construction and reproducibility. The labelled analytical subset uses anonymized/internal transaction-node keys only; these keys are not wallet addresses, original transaction hashes, user identifiers, exchange identifiers, or jurisdic-

tional markers. The uploaded analytical workbook contains 46,564 model-ready labelled rows, 42,019 licit cases and 4,545 illicit cases, with no missing analytical cells in the variables used for the reported models. It also contains feature-block summaries, model-score variables, diagnostic sheets, and a 5,000-row directed edge map used only as a transparent graph-consistency extract. The reported benchmark structure refers to the full Elliptic graph; therefore, audit-level replication of the graph variables should be conducted from the original Elliptic classes, features, and edge list rather than from the check extract alone. The workbook uses internal analytical identifiers and provenance-warning fields; therefore, it documents the reported analysis and consistency checks, but it is not a substitute for audit-level replication from the original Elliptic source files. No row is assigned to the United States, Singapore, or the UAE. Consequently, the manuscript does not estimate exchange-centered national windows, does not infer user residence, and does not treat GraphSense or BigQuery as unreproduced sources of country-specific labelled outcomes.

The network metrics account for the transactional complexity present in the benchmark graph. Degree centrality is used to determine the direct connectivity of a transaction node in the flow graph. The clustering coefficient metric determines the density of the neighborhood present in the graph, which can be linked with coordinated transfers. Flow entropy refers to the variation in the distribution of the directed flow between connected nodes. The anomalies were detected using unsupervised machine learning approaches such as Isolation Forest and Autoencoder methods. The binary dependent variable is equal to one when the labelled benchmark is identified as illegal and zero for legal transactions; unlabeled benchmarks are excluded from negative cases.

The blockchain data are represented as a directed transaction graph in which anonymized transactions form the nodes and directed payment flows form the edges. The study does not partition the global blockchain into separate national blockchains, and it does not infer user residence from transaction structure. GraphSense and BigQuery are therefore described only as possible contextual or auxiliary blockchain-analytics resources for future extensions; the revised statistical model does not depend on unreproduced exchange-anchored national windows, country tags, or jurisdictional labels.

To assess predictive quality on the labelled portion of the benchmark, Random Forest and XGBoost classifiers were used as supervised validation models. Thus, the unsupervised stage produces exploratory suspiciousness scores, the supervised stage checks whether the same features discriminate the labelled illicit class, and the inferential model tests the association between network-complexity variables and the labelled illicit outcome. Model performance was evaluated using ROC-AUC together with threshold-dependent precision, recall, and F1-score. Ten-fold cross-validation was used to assess stability where model settings allowed it, and SHAP analysis supported interpretability by ranking the contribution of each feature to illicit classification.

In order to determine whether there is a correlation between transaction complexity and being classified as illicit, a generalized logit model was fitted using the analytical sample. The new regression model utilizes the three workbook measures of transaction complexity: degree centrality, clustering coefficient, and flow entropy. Jurisdiction-level regulatory variables were omitted from the analysis due to the absence of transaction synchronization for the Elliptic benchmark against the country-year AML/CFT scores.

$$\begin{aligned} &\log it\left[P\left(y\_i = 1\right)\right] = \beta 0 \\ &+\beta 1 Centrality\_i + \beta 2 Clustering\_i \\ &+\beta 3 Entropy\_i + \varepsilon\_i, \end{aligned} \tag{1}$$

where i indexes labelled benchmark observations; y represents a node representing illicit transactions and 0 otherwise; Centrality, Clustering, and Entropy represent standardized network complexity metrics as detailed in the uploaded analytical workbook; and ε_i represents the error term. Thus, this is a benchmark-level classification model, not a national window or exchange-level model.

The combination of anomaly detection with inference allows for the mapping of transaction-level signal behavior to classification-level graphical

http://dx.doi.org/10.21511/imfi.23(3).2026.27

evidence. By linking computational metrics with realistic governance interpretation, this design avoids problems with relevance without confusing contextual regulatory differences for transaction-level causal effects.

Various tests for robustness and diagnostic purposes were performed to examine whether there was internal stability within the benchmark relationship being estimated. This included tests such as stratified subsample re-estimation, intercorrelations between different anomaly score measures, multicollinearity checks, Hosmer-Lemeshow goodness-of-fit test, and holdout predictive AUC calculations. Other checks for class handling issues ensured that observations not known to be either illicit or legitimate were not considered legitimate by default. All of these are seen as benchmark-level internal diagnostics, not as external tests about country or exchange-level effects.

In sum, this methodology aims to marry computational analysis with institutional realities. Using an open benchmark enhances replicability, but working with anonymized publicly available data means that no wallet, exchange, timestamp, dollar value, or jurisdictional level information can be attributed to each observation. For reporting purposes, the source data of this study is available in Appendix A, and the analytical boundary between benchmark-level estimation and the regulation context is clearly delineated. The combination of machine learning and statistical models can be done in a fully transparent fashion when studying proxy-based regulatory signals in the digital economy.

3. RESULTS

Descriptive analysis starts by establishing the empirical structure of the labeled Bitcoin benchmark. Since the Elliptic data is anonymized, the descriptive baseline is based on the function of the transaction node, the directed edge, the anonymized features, the temporal step, and the labels, but not the unverifiable information on senders' and receivers' wallets or the national windowed exchanges. This is summarized in Table 1.

Table 1 clarifies that the empirical approach is focused on transaction nodes, directed flow-of-payment edges, anonymized features, benchmarked time windows, and licit/illicit/unknown categories. This correction is necessary to avoid the implication that the Elliptic benchmark contains any identifiable information about the sending wallet, receiving wallet, amount, timestamp, exchange ownership, or nationality of the user.

In this sense, then, the descriptive benchmark is supportive of graph-based anomaly detection and classification, but it is neither informative regarding national incidence nor the enforcement/regulatory implications of exchanges. It also does not reveal the structure of jurisdictional networks.

It is at this point in the project that the use of Table 1 can be seen primarily as a means to clarify the methodological framework, rather than as a demonstration of causal influence, or as a means to establish information about user-location, national-incidence rates, or jurisdictional networks.

Workbook-derived anomaly scores show good discriminatory power within the labelled transaction graph. This evidence is consistent with recent blockchain anomaly-detection work that models spatial and temporal dependencies among transaction nodes (Chen et al., 2025). The Isolation Forest and Autoencoder scores diverged from normal feature distributions and returned high AUC values. Precision, recall, and F1-score were more moderate when the threshold was set to the top

Table 1. Corrected benchmark structure and analytical role

Component	Benchmark structure	Use	Boundary
Nodes	203,769 anonymized transactions	Graph unit	No wallets, users, or countries
Edges	234,355 benchmark flows; workbook check map: 5,000 rows	Connectivity; limited graph check	No sender-receiver or country-window reconstruction
Features	166 anonymized features; workbook feature blocks	Model inputs	Not raw amount or timestamp
Labels	Licit, illicit, and unknown	46,564 labelled observations	Unknown excluded, not recoded as licit
Time steps	49 steps	Ordering	Not aligned with policy scores

4,545 ranked transactions, corresponding to the number of illicit observations. Anomaly results should therefore be interpreted as exploratory screening evidence rather than operational classification rates.

Table 2 reports workbook-computed quantitative results, including algorithmic performance measures and SHAP feature weights. The SHAP weights are used only as model-specific explanatory evidence, consistent with recent work treating SHAP as a feature-importance tool rather than a standalone validity test (Wang et al., 2024). Country-window anomaly averages are not reported because they would require an exchange-attribution layer that cannot be derived from the Elliptic benchmark itself. The reported threshold metrics are conservative.

While Isolation Forest was marginally better than Autoencoder in terms of AUC score (0.866 against 0.841), both methods' precision, recall, and F1-score were relatively moderate. Graph-based classification can be interpreted in the context of recent studies on fraud detection in the Bitcoin ecosystem, which reveal that graph-based learning methods can uncover fraud and anomalies based on the structure of transactions within Bitcoin networks (Asiri & Somasundaram, 2025). As shown by SHAP analysis, degree centrality is the most important predictor group, followed by clustering coefficient and anonymized benchmark features. In practice, more connected and clustered transactions are anomalies in the labelled benchmark data, but additional threshold setting is required before using classification algorithms.

The results in Table 2 support H2 because the anomaly rankings generated by the unsupervised machine-learning methods align with the labelled illicit classification, as indicated by the reported AUC values. This interpretation is consistent with recent evidence that temporal graph-based algorithms can improve illicit Bitcoin transaction classification (Lin et al., 2026). The feature-importance results in Table 2 also support H3 because network-complexity variables remain material contributors to the modelled anomaly rankings and classification interpretation.

These findings therefore indicate that the ranking of anomalies generated by the two methods is in line with the labelled benchmark data.

To determine the relationship between illicit transactions and network complexity, the logit model has been estimated using illicit as the dependent variable. Therefore, the new logit equation includes the degree centrality, clustering coefficient, and flow entropy variables but excludes the regulation and regulatory interactions variables.

The results in Table 3 support H1. The positive and statistically significant coefficients for degree centrality, clustering coefficient, and flow entropy show that greater transaction-network complexity is positively associated with illicit classification probability within the labelled benchmark. The findings on centrality support recent research on illicit financial flows showing that centrality-based anomaly measures are capable of distinguishing structurally anomalous nodes in time-varying financial networks (Vilella et

Table 2. Quantitative performance and feature importance metrics

Metric	Isolation Forest	Autoencoder	Interpretation
AUC	0.866	0.841	Strong AUC discrimination
Precision	0.469	0.420	Moderate; threshold-dependent
Recall	0.469	0.420	Moderate; threshold-dependent
F1-score	0.469	0.420	Moderate; threshold-dependent
SHAP: degree centrality	0.41	0.38	Strongest feature group
SHAP: clustering coefficient	0.33	0.27	Material graph-density contribution
SHAP: anonymized feature block	0.17	0.22	Benchmark features, not raw amount
SHAP: flow entropy	0.09	0.13	Moderate irregularity contribution

Notes: AUCs and threshold metrics have been recalculated based on the labelled analytical workbook uploaded. The threshold metrics refer to the top 4,545 score ranks being classified as illicit in keeping with the total number of illicitly labelled rows; thus, they are screening measures, not operational classification rates. SHAP weights reflect normalized feature importance values calculated for the workbook. No country-level average anomalies are presented since the updated empirical framework no longer relies on the inference of national exchange windows from the benchmark.

http://dx.doi.org/10.21511/imfi.23(3).2026.27

Table 3. Revised logit results: Determinants of illicit transaction probability

Variable	Coefficient (beta)	Std. Error	z-Value	p-Value
Intercept	–4.023	0.041	–98.48	< 0.001
Degree Centrality	1.870	0.029	65.46	< 0.001
Clustering Coefficient	0.940	0.023	40.70	< 0.001
Flow Entropy	0.680	0.022	31.57	< 0.001
Labelled observations	46,564	–	–	–
Log-likelihood	–8,658.83	–	–	–
LR chi-square	12,464.15	–	–	< 0.001
McFadden pseudo-R2	0.419	–	–	–
Regulatory Index	Removed from inferential model	–	–	–
Centrality x Regulatory Index	Removed from inferential model	–	–	–

Note: The standard errors and p-values are recalculated from the uploaded labelled analytical workbook. All independent variables are measured using z-score standardization. The regulatory capacity coefficient and country/window-specific marginal effects are not calculated.

al., 2025). The exclusion of the regulatory capacity coefficient and the regulation-transaction interaction effect makes it impossible to treat the benchmark level estimates as evidence of jurisdictional effects which cannot be proven by transaction-level anonymity.

Therefore, it seems reasonable to consider the model as the benchmarking model for classification of illicit transactions rather than as a proof of causality between national AML/CFT capacity and probability of transaction-level money laundering. It is consistent with typological AML research emphasizing the role of metrics and evidentiary scope in FIU operations (Akartuna et al., 2024). Because the regulatory layer is not synchronized with the transaction-level benchmark, the revised results do not report marginal effects of regulatory strength across U.S.-, Singapore-, or UAE-anchored windows. Instead, Table 4 states the interpretive boundary conditions used to retain the governance discussion without presenting unsupported national probability estimates, regulatory-capacity coefficients, or regulatory interaction effects.

As seen from Table 4, the Elliptic benchmark is consistent with transaction graph-based classification, whereas Basel AML indicators and country-level AML/CFT data are limited in their utility to governance context interpretation only. The boundary is also consistent with DeFi AML research warning that enhanced regulation is needed, but that policy claims require careful links between use cases, data, and regulatory evidence (Benson et al., 2024). Hence, the Basel AML Index is not converted into a regulatory capacity variable for causal inference in the updated inferential model and is treated as an indicator of higher or lower ML/TF risk based on a given context. As such, there is no longer an issue of inconsistency between regulatory coefficient values and marginal effects, or any inference that benchmark labels identify user location.

Such boundary conditions do not impair the technical contribution. Instead, they strengthen the contribution by distinguishing the capabilities of the benchmark in relation to the interpretive potential of regulatory sources.

Table 4. Regulatory context and interpretive boundary conditions

Layer	Role	Source basis	Period	Supports	Does not support
Elliptic benchmark	Estimation	Anonymized graph	Benchmark	ML/logit classification	National incidence or geography
GraphSense / BigQuery	Future extension only	Public tags/raw-chain resources	Source-specific	Only future reproducible windows	Current country outcomes
Basel AML Index	Governance context	Jurisdiction ML/TF risk score	2018–2024	Regulatory-risk context	Transaction-level coefficient

Note: The regulatory context is utilized for interpretive purposes only and is not part of the updated inferential predictive model.

A number of diagnostics were undertaken to evaluate the reliability and consistency of results. This included analysis of stratified sample estimates, algorithmic score comparison, assessment of collinearity, model fit, and external validation via holdout sample prediction. Diagnostic statistics from the labelled analytical file are presented in Table 5. The table reflects model diagnostics at the benchmark level and should not be interpreted as independent evidence of regulatory effects.

Based on the diagnostic outputs, there is a relatively stable benchmark model, given the labelled analytical sample and the observed pre-processing conditions. There is a maximum centrality coefficient parameter change of 0.023 across ten re-estimated samples, each representing 80 percent of the original sample. Comparing algorithmic scores shows a moderate to strong correlation between Isolation Forest and the two alternative anomaly scores, r = 0.722 with One-Class SVM, and r = 0.710 with LOF. Diagnostic tests, by definition, only represent internal consistency tests and cannot be interpreted as external validation tests.

The low mean VIF (1.09) and the non-significant Hosmer-Lemeshow statistic (chi-square = 10.07, p = 0.260) imply that collinearity and lack of fit are minor problems in the benchmark model specification. The mean holdout AUC of the logit specification is 0.919, while the mean absolute prediction error stands at 0.110. These figures imply satisfactory internal predictive stability of the benchmark model in the labelled dataset. This cautious use of machine-learning output is consistent with AML compliance research that links suspicious activity detection to routine-activity opportunity conditions while retaining interpretive limits (Lokanan, 2025).

Taken together, the diagnostics in Table 5 indicate that the empirical findings form an internally stable pattern within the labelled benchmark sample. This stability concerns benchmark-level classification and prediction; it does not provide evidence that national AML/CFT capacity causes changes in transaction-level laundering probability.

The hypothesis-specific evidence is summarized in Table 6. H1 is supported: Table 3 reports positive and statistically significant coefficients for degree centrality (beta = 1.870, $p < 0.001$), clustering coefficient (beta = 0.940, $p < 0.001$), and flow entropy (beta = 0.680, $p < 0.001$), indicating that greater transaction-network complexity is associated with a higher probability of illicit classification. H2 is supported: Table 2 reports AUC values of 0.866 for Isolation Forest and 0.841 for the Autoencoder, demonstrating satisfactory alignment between unsupervised anomaly scores and labelled illicit classification in the validation stage. H3 is supported: the SHAP evidence in Table 2 assigns substantive importance to degree centrality, clustering coefficient, and flow entropy, indicat-

Table 5. Internal robustness and diagnostic checks

Validation Test	Statistic / Metric	Benchmark	Observed Value	Interpretation
Labelled-row completeness	Rows / missing analytical cells	No missing model cells	46,564 rows; 0 missing	Complete analytical file
Class distribution	Illicit / licit	Unknown excluded	4,545 / 42,019	Consistent labelled subset
Subset stability	Max |Delta beta|, centrality	Low change	0.023	Stable across stratified resampling
Isolation Forest vs One-Class SVM	Score correlation r	Positive convergence	0.722	Moderate-to-strong convergence
Isolation Forest vs LOF	Score correlation r	Positive convergence	0.710	Moderate-to-strong convergence
Variance Inflation Factor	Mean VIF	< 3	1.09	No collinearity concern
Hosmer-Lemeshow Goodness of Fit	chi-square; p	p > 0.05	10.07; p = 0.260	Acceptable fit
Holdout predictive AUC	Mean of five stratified 80/20 splits	> 0.80	0.919	High internal prediction
Mean Absolute Prediction Error	MAE	Lower is better	0.110	Moderate prediction error
Log-likelihood ratio	LR chi-square	> 0	12,464.15; p < 0.001	Model improvement significant

http://dx.doi.org/10.21511/imfi.23(3).2026.27

Table 6. Hypothesis testing summary

Hypothesis	Empirical evidence	Relevant table(s)	Decision
H1	Degree centrality (beta = 1.870), clustering coefficient (beta = 0.940), and flow entropy (beta = 0.680) are all positive and statistically significant ($p < 0.001$).	Table 3	Supported
H2	Isolation Forest and Autoencoder achieve AUC values of 0.866 and 0.841, respectively, showing satisfactory discrimination of the labelled illicit class at the validation stage.	Table 2	Supported
H3	SHAP feature importance identifies degree centrality, clustering coefficient, and flow entropy as material contributors to model interpretation; the logit estimates also confirm their classification relevance.	Tables 2 and 3	Supported

Note: Table 5 provides internal robustness and diagnostic evidence for the benchmark results but is not a separate hypothesis test.

ing that network-complexity measures materially contribute to model interpretation and illicit-classification performance.

Accordingly, the hypothesis-specific evidence in Tables 2 and 3 supports *H1*, *H2*, and *H3*, while the diagnostics in Table 5 reinforce the internal stability of these findings. Tables 1 and 4 serve descriptive and interpretive-boundary functions, respectively, rather than hypothesis testing. The results therefore support a benchmark-specific, association-based conclusion that labelled illicit outcomes are systematically related to transaction-network complexity and anomaly signals. They should not be extrapolated to national windows, user geography, exchange headquarters, or separate national chains.

4. DISCUSSION

Based on the results, greater blockchain transaction-network complexity is associated with a higher likelihood of illicit classification within the labelled Bitcoin benchmark, thereby supporting *H1*. Specifically, higher degree centrality, local clustering, and flow entropy are each positively associated with illicit classification, suggesting that illicit-labelled transactions tend to occupy network positions with greater connectivity, density, and flow irregularity. As mentioned above, the present findings can be interpreted in light of the existing literature, which reports that illegal groups, abnormal temporal nodes, and fraudulent patterns are more likely to occur where transactions have a complex structure involving high connectivity and density (Andrei & Veltri, 2025; Kamuhanda et al., 2023; Vilella et al., 2025). Moreover, the findings are consistent with a routine-activity perspective in which opportunities for illegal activity in digital environments are related to transaction structure rather than individual transaction attributes (Lokanan, 2025; Ofori & Appiah, 2025).

It should be noted that the discussion of the regulatory coefficient does not imply that any country has a lower money laundering risk than another. The point here is to explain why technical transaction detection capacity is critical to effective AML/CFT management. The existing institutional approaches still demonstrate the importance of credibility, coordinated efforts, and analytics to mitigate laundering risks within the mediated financial environments (Cheng & Wen, 2025; Nanyun & Nasiri, 2021; Tuhirirwe & Alexander, 2025). The United States, Singapore, and the UAE therefore remain useful contextual reference points for discussing different AML/CFT governance trajectories, but not as statistically estimated national partitions of the Elliptic benchmark (Fuda, 2025; Onufer, 2022; Sultan et al., 2024).

Support for H2 and H3 is important because it shows that anomaly detection and graph explainability add value beyond descriptive discussion. Prior studies often report predictive accuracy without explaining which behavioral structures drive classification (Akartuna et al., 2024; Benson et al., 2024; Popik-Mazur, 2025). Here, the highest explanatory contributions come from network-complexity indicators, which is consistent with risk-based regulation and institutional-theory arguments that effective guardianship depends on the ability to identify structurally risky nodes and flows before enforcement resources are allocated (DiMaggio & Powell, 1983; Paul, 2024).

CONCLUSION

This study evaluated how transaction-network complexity is associated with the probability of illicit blockchain activity in the public Elliptic Bitcoin benchmark, while using AML/CFT governance material only as contextual interpretation.

The results show that higher degree centrality, clustering coefficient, and flow entropy are associated with higher illicit probability. Isolation Forest and Autoencoder models also generate anomaly signals that align with labelled illicit classification, and SHAP evidence indicates that network-complexity indicators are central to model interpretation. Thus, these results suggest that the importance of blockchain analysis is not limited to visible trails but also entails transparency in graph generation and a measured approach in terms of what anonymized benchmarks allow.

Consequently, the key learning point from this study is that effective implementation of regulations for AML/CFT in digital finance requires proficiency in analysis and capable regulatory agencies. In terms of practical application, this means that importance should be placed on data management, coordination between various agencies, and regulations targeting dense areas of transactions, dense graph neighborhoods, and abnormal flows of money. Future research could build on this approach by applying exchange tagging schemes, expanding the number of blockchains, adding address attribution, and coordinating regulatory action temporally before examining the impact of reforms on risks of criminal activity.

AUTHOR CONTRIBUTIONS

Conceptualization: Ayman Mansour Khalaf Alkhazaleh.
Formal analysis: Ayman Mansour Khalaf Alkhazaleh.
Funding acquisition: Ayman Mansour Khalaf Alkhazaleh.
Investigation: Ayman Mansour Khalaf Alkhazaleh.
Methodology: Ayman Mansour Khalaf Alkhazaleh.
Resources: Ayman Mansour Khalaf Alkhazaleh.
Software: Ayman Mansour Khalaf Alkhazaleh.
Validation: Ayman Mansour Khalaf Alkhazaleh.
Visualization: Ayman Mansour Khalaf Alkhazaleh.
Writing – original draft: Ayman Mansour Khalaf Alkhazaleh.
Writing – review & editing: Ayman Mansour Khalaf Alkhazaleh.

REFERENCES

1. Ahmad, A. K., Nahar, H. M., & Manajreh, M. M. N. (2023). Effect of social media on shaping the agenda of the communicator in the Jordanian TV channels. *Middle East Journal of Communication Studies, 3*(2), 1-40. https://doi.org/10.71220/2585-003-002-003
2. Agarwal, U., Rishiwal, V., Tanwar, S., & Yadav, M. (2024). Blockchain and crypto forensics: Investigating crypto frauds. *International Journal of Network Management, 34*(2), Article e2255. https://doi.org/10.1002/nem.2255
3. Akartuna, E. A., Johnson, S. D., & Thornton, A. (2024). Motivating a standardised approach to financial intelligence: A typological scoping review of money laundering methods and trends. *Journal of Experimental Criminology, 21,* 1367-1413. https://doi.org/10.1007/s11292-024-09623-y
4. Al-Muntasir, M. (2022). The phenomenon of information flow from traditional and new media about the Corona pandemic from the perspective of newly graduated media professionals in Yemen. *Middle East Journal of Communication Studies, 2*(2), 7-25. https://doi.org/10.71220/2585-002-002-005
5. Alkire, S., Kanagaratnam, U., Nogales, R., & Suppa, N. (2022). Revising the global multidimensional poverty index: Empirical insights and robustness. *Review of Income and Wealth, 68*(S2), 347-384. https://doi.org/10.1111/roiw.12573
6. Andrei, F., & Veltri, G. A. (2025). Status spill-over in

http://dx.doi.org/10.21511/imfi.23(3).2026.27

cryptomarket for illegal goods. *Social Science Computer Review, 43*(3), 626-648. https://doi.org/10.1177/08944393241286339

7. Asiri, A., & Somasundaram, K. (2025). Graph convolution network for fraud detection in bitcoin transactions. *Scientific Reports, 15,* Article 11076. https://doi.org/10.1038/s41598-025-95672-w

8. Bajra, U. Q., Rogova, E., & Avdiaj, S. (2024). Cryptocurrency blockchain and its carbon footprint: Anticipating future challenges. *Technology in Society, 77,* Article 102571. https://doi.org/10.1016/j.techsoc.2024.102571

9. Balaskas, S., Nikolopoulos, T., Koutroumani, M., & Rigou, M. (2024). Determinants of tax avoidance intentions in tourism SMEs: The mediating role of coercive power, digital transformation, and the moderating effect of CSR. *Sustainability, 16*(21), Article 9322. https://doi.org/10.3390/su16219322

10. Basel Institute on Governance. (2024). *Basel AML Index 2024*: 13th Public Edition. Basel Institute on Governance. Retrieved from https://baselgovernance.org/publications/basel-aml-index-2024

11. Bastiaens, I., Lechner, L., & Postnikov, E. (2025). Non-trade issues in preferential trade agreements and global value chains. *Review of International Political Economy, 32*(2), 353-380. https://doi.org/10.1080/09692290.2024.2427308

12. Bensassi, S., & Raz, A. F. (2025). Combating trade-related fraud: Do the Financial Action Task Force recommendations bite? *Economica, 92*(365), 322-347. https://doi.org/10.1111/ecca.12561

13. Benson, V., Turksen, U., & Adamyk, B. (2024). Dark side of decentralised finance: A call for enhanced AML regulation based on use cases of illicit activities. *Journal of Financial Regulation and Compliance, 32*(1), 80-97. https://doi.org/10.1108/JFRC-04-2023-0065

14. Chen, S., Liu, Y., Zhang, Q., Shao, Z., & Wang, Z. (2025). Multi-distance spatial-temporal graph neural network for anomaly detection in blockchain transactions. *Advanced Intelligent Systems, 7*(8), 2400898. https://doi.org/10.1002/aisy.202400898

15. Cheng, G., & Wen, B. (2025). On the performance-based legitimacy of Financial Action Task Force: A quantitative exploration. *Regulation & Governance.* https://doi.org/10.1111/rego.70088

16. Dávid-Barrett, E. (2024). Measuring grand corruption. In R. I. Rotberg & F. O. Hampson (Eds.), *Grand corruption: Curbing kleptocracy globally* (pp. 37-48). Routledge. https://doi.org/10.4324/9781032719344-4

17. DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147-160. https://doi.org/10.2307/2095101

18. Dote-Pardo, J. S., & Severino-González, P. (2025). Money laundering in emerging countries: Patterns, trends, and knowledge gaps from a systematic review. *Journal of Money Laundering Control, 28*(2), 341-358. https://doi.org/10.1108/JMLC-01-2025-0002

19. Frąszczak, D., & Frąszczak, E. (2024). NetCenLib: A comprehensive Python library for network centrality analysis and evaluation. *SoftwareX, 26*, Article 101699. https://doi.org/10.1016/j.softx.2024.101699

20. Frey, T. K., & Tatum, N. T. (2022). Instructor strictness: Instrument development and validation. *Communication Education, 71*(4), 327-354. https://doi.org/10.1080/03634523.2022.2096246

21. Fröhlich, M. (2024). The EU model for international competition cooperation: Fighting international competition restrictions beyond the extraterritorial application of the EU competition law regime. In *European Yearbook of International Economic Law 2023* (pp. 201-232). Springer. https://doi.org/10.1007/8165_2023_116

22. Fuda, K. (2025). The evolution of financial regulation and the role of the Monetary Authority of Singapore: A historical analysis based on organizational knowledge creation theory. *Management & Organizational History, 20*(1), 130-152. https://doi.org/10.1080/17449359.2024.2441925

23. Gavira-Durón, N., Mayorga-Serna, D., & Bagatella-Osorio, A. (2022). The financial impact of the implementation of Solvency II on the Mexican insurance sector. *The Geneva Papers on Risk and Insurance - Issues and Practice, 47*(2), 349-374. https://doi.org/10.1057/s41288-020-00196-1

24. Hamed, R. S., Al-Shattarat, W. K., Al-Shattarat, B. K., & Mejri, M. (2024). Exploring the linkages between anti-money laundering guidelines and earnings manipulation techniques. *Humanities and Social Sciences Communications, 11,* Article 1572. https://doi.org/10.1057/s41599-024-04114-x

25. Haque, A., & Soliman, H. (2025). A transformer-based autoencoder with isolation forest and XGBoost for malfunction and intrusion detection in wireless sensor networks for forest fire prediction. *Future Internet, 17*(4), 164. https://doi.org/10.3390/fi17040164

26. Kamuhanda, D., Cui, M., & Tessone, C. J. (2023). Illegal community detection in bitcoin transaction networks. *Entropy, 25*(7), Article 1069. https://doi.org/10.3390/e25071069

27. Li, J., Zhou, Y., Yao, J., & Liu, X. (2021). An empirical investigation of trust in AI in a Chinese petrochemical enterprise based on institutional theory. *Scientific Reports, 11*(1), 13564. https://doi.org/10.1038/s41598-021-92904-7

28. Lima, F. T., & Souza, V. M. (2023). A large comparison of normalization methods on time series. *Big Data Research, 34,* Article 100407. https://doi.org/10.1016/j.bdr.2023.100407

29. Lin, Z., Luo, Q., Wu, D., Shen, J., Li, L., Nong, X., & Qin, Z. (2026). Detecting illicit transactions in bitcoin: A wavelet-temporal graph transformer approach for anti-money laundering. *Scientific Reports, 16,* Article 1548. https://doi.org/10.1038/s41598-025-23901-3

30. Lokanan, M. E. (2025). Enhancing AML compliance: A machine learning approach to suspicious activity detection through routine activity theory. *Journal of Money Laundering Control, 28*(4/5), 680-698. https://doi.org/10.1108/JMLC-07-2024-0114

31. Maheswari, G., Vinith, A., Sathyanarayanan, A. S., & Sowmi Saltonya, M. (2024). An ensemble framework for network anomaly detection using isolation forest and autoencoders. In *Proceedings of the 2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems (ADICS)* (pp. 1-6). IEEE. https://doi.org/10.1109/ADICS58448.2024.10533499

32. Meier, H. B., Marthinsen, J. E., Gantenbein, P. A., & Weber, S. S. (2023). Swiss bank (customer) secrecy and the international exchange of information. In *Swiss Finance: Banking, Finance, and Digitalization* (pp. 159-250). Springer. https://doi.org/10.1007/978-3-031-23194-0_4

33. Morshed, A., & Khrais, L. T. (2025). Cybersecurity in digital accounting systems: Challenges and solutions in the Arab Gulf region. *Journal of Risk and Financial Management, 18*(1), 41. https://doi.org/10.3390/jrfm18010041

34. Nanyun, N. M., & Nasiri, A. (2021). Role of FATF on financial systems of countries: Successes and challenges. *Journal of Money Laundering Control, 24*(2), 234-245. https://doi.org/10.1108/JMLC-06-2020-0070

35. Ofori, E., & Appiah, M. O. (2025). Multinational tax evasion and money laundering: Examining the financial investigation system in Ghana. *Journal of Money Laundering Control, 28*(2), 442-462. https://doi.org/10.1108/JMLC-09-2024-0150

36. Onufer, M. (2022). The roles and responsibilities of U.S. financial institutions in combatting human trafficking. In *Human trafficking* (pp. 328-339). Routledge. https://doi.org/10.4324/9781003124672-19

37. Oreqat, A. (2021). The degree of satisfaction of Facebook users about its features, usage motives and achieved gratifications: An applied study on students of the Faculty of Mass Communication at the Middle East University. *Middle East Journal of Communication Studies, 1*(1), 7-35. https://doi.org/10.71220/2585-001-001-001

38. Othman, M. (2025). AI and FinTech adoption in Jordanian banking: Toward inclusive and culturally aligned innovation. *Banks and Bank Systems, 20*(4), 45-59. https://doi.org/10.21511/bbs.20(4).2025.05

39. Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cybersecurity solutions. *IEEE Access, 12,* 12229-12256. https://doi.org/10.1109/ACCESS.2024.3355547

40. Pandurangan, P., Rakshi, A. D., Sundar, M. S. A., Samrat, A. V., Meenambiga, S. S., Vedanarayanan, V., Meena, R. S., Namasivayam, K. R., & Moovendhan, M. (2024). Integrating cutting-edge technologies: AI, IoT, blockchain and nanotechnology for enhanced diagnosis and treatment of colorectal cancer – A review. *Journal of Drug Delivery Science and Technology, 91,* Article 105197. https://doi.org/10.1016/j.jddst.2024.105197

41. Parycek, P., Schmid, V., & Novak, A.-S. (2024). Artificial intelligence and automation in administrative procedures: Potentials, limitations, and framework conditions. *Journal of the Knowledge Economy, 15*(2), 8390-8415. https://doi.org/10.1007/s13132-023-01433-3

42. Paul, R. (2024). European artificial intelligence "trusted throughout the world": Risk-based regulation and the fashioning of a competitive common AI market. *Regulation & Governance, 18*(4), 1065-1082. https://doi.org/10.1111/rego.12563

43. Phan, T. T. T. (2025). Leveraging graph neural networks and optimization algorithms to enhance anti-money-laundering systems. In *Advances in data science and optimization of complex systems (ICAMCS 2024)* (pp. 300-311). Springer LNNS. https://doi.org/10.1007/978-3-031-90606-0_25

44. Popik-Mazur, A. (2025). A systematic literature review of illicit financial flows and money laundering: Current state of research and estimation methods. *Journal of Economics and Management, 47*(1), 257-298. https://doi.org/10.22367/jem.2025.47.11

45. Saggese, P., Segalla, E., Sigmund, M., Raunig, B., Zangerl, F., & Haslhofer, B. (2024). Assessing the solvency of virtual asset service providers: Are current standards sufficient? *Applied Economics, 57*(49), 8178-8193. https://doi.org/10.1080/00036846.2024.2396640

46. Sultan, N., Mohamed, N., Said, J., & Mohd, A. (2024). The sustainability of the international AML regime and the role of the FATF: The objectivity of the greylisting process of developing jurisdictions like Pakistan. *Journal of Money Laundering Control, 27*(1), 76-92. https://doi.org/10.1108/JMLC-12-2022-0166

47. Taqa, S. B. A. (2025). The mediating role of remote communication on the relationship between electronic human resource management practices and organizational performance in Iraqi commercial banks. *Middle East Journal of Communication Studies, 5*(1), 1-52. https://doi.org/10.71220/2585-005-001-002

48. Tuhirirwe, C., & Alexander, R. (2025). Efficacy of country legal frameworks and international guidelines in curtailing money laundering and terrorist financing activities in grey list countries: Case studies of Kenya and Uganda. *Journal of Economic Criminology, 8,* 100153. https://doi.org/10.1016/j.jeconc.2025.100153

49. Urooj, S. (2024). A dynamic threshold analysis of effect of Financial Action Task Force (FATF) measures on financial inclusion: Evidence from the world. *Journal of Money Laundering Control, 27*(4), 696-709. https://doi.org/10.1108/JMLC-07-2023-0128

http://dx.doi.org/10.21511/imfi.23(3).2026.27

50. Usman, N., Griffiths, M., & Alam, A. (2025). FinTech and money laundering: Moderating effect of financial regulations and financial literacy. *Digital Policy, Regulation and Governance, 27*(3), 301-326. https://doi.org/10.1108/DPRG-04-2024-0068

51. Vilella, S., Capozzi, A., Fornasiero, M., Moncalvo, D., Ricci, V., Ronchiadin, S., & Ruffo, G. (2025). Weirdnodes: Centrality based anomaly detection on temporal networks for the anti-financial crime domain. *Applied Network Science, 10,* Article 14. https://doi.org/10.1007/s41109-025-00702-1

52. Wang, H., Liang, Q., Hancock, J. T., & Khoshgoftaar, T. M. (2024). Feature selection strategies: A comparative analysis of SHAP-value and importance-based methods. *Journal of Big Data, 11,* Article 44. https://doi.org/10.1186/s40537-024-00905-w

53. 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 fore*nsics. arXiv. Retrieved from https://arxiv.org/abs/1908.02591

54. Wronka, C. (2022). "Cyber-laundering": The change of money laundering in the digital age. *Journal of Money Laundering Control, 25*(2), 330-344. https://doi.org/10.1108/JMLC-04-2021-0035

55. Wronka, C. (2023). Financial crime in the decentralized finance ecosystem: New challenges for compliance. *Journal of Financial Crime, 30*(1), 97-113. https://doi.org/10.1108/JFC-09-2021-0218

56. Zhang, Y., & Zhang, Q. (2025). Navigating the invisible: Ironic compliance, forced labor, and the commodification of offline rights in digitalized workplaces. *Journal of Business Ethics, 203,* 55-72. https://doi.org/10.1007/s10551-025-06057-y

57. Zhon, H., & Asiama, A. A. (2022). The prevalence and mechanisms of cyber fraud activities among Ghanaian youths: Routine activity, space transition, and rational choice from differential association perspective. In *2022 IEEE International Symposium on Technology and Society (ISTAS)* (pp. 1-7). https://doi.org/10.1109/ISTAS55053.2022.10227127

APPENDIX A. DATA SOURCES

These sources of public data that have been utilized for developing or explaining the blockchain, machine learning, tagging, and regulation components of the study have been detailed in the appendix. The new design has separated the transaction level benchmark from the sources used for regulation.

Table A1. Corrected variable-level data sources and analytical roles

Variable / Component	Source	URL
Anonymized transaction nodes	Elliptic labelled Bitcoin benchmark (Kaggle / Elliptic)	https://www.kaggle.com/datasets/ellipticco/elliptic-data-set
Directed payment-flow edges	Elliptic labelled Bitcoin benchmark (Kaggle / Elliptic)	https://www.kaggle.com/datasets/ellipticco/elliptic-data-set
Anonymized node features	Elliptic labelled Bitcoin benchmark (Kaggle / Elliptic)	https://www.kaggle.com/datasets/ellipticco/elliptic-data-set
Licit / illicit / unknown labels	Elliptic labelled Bitcoin benchmark (Kaggle / Elliptic)	https://www.kaggle.com/datasets/ellipticco/elliptic-data-set
Temporal ordering / benchmark time-step information	Elliptic labelled Bitcoin benchmark (Kaggle / Elliptic)	https://www.kaggle.com/datasets/ellipticco/elliptic-data-set
Raw blockchain context only	Google BigQuery Bitcoin public dataset overview	https://cloud.google.com/bigquery/public-data
Future exchange-tagging extensions only	GraphSense platform; not used to assign current labels to countries	https://graphsense.org/
Degree centrality (computed)	Computed from the anonymized transaction graph	https://www.kaggle.com/datasets/ellipticco/elliptic-data-set
Clustering coefficient (computed)	Computed from the anonymized transaction graph	https://www.kaggle.com/datasets/ellipticco/elliptic-data-set
Flow entropy (computed)	Computed from directed payment-flow structure	https://www.kaggle.com/datasets/ellipticco/elliptic-data-set
Isolation Forest anomaly score	Model-generated from standardized benchmark features	https://www.kaggle.com/datasets/ellipticco/elliptic-data-set
Autoencoder reconstruction error	Model-generated from standardized benchmark features	https://www.kaggle.com/datasets/ellipticco/elliptic-data-set
Supervised validation labels	Elliptic licit/illicit labels, excluding unknown class	https://www.kaggle.com/datasets/ellipticco/elliptic-data-set
SHAP feature weights	Model-generated interpretability output	https://www.kaggle.com/datasets/ellipticco/elliptic-data-set
AML/CFT contextual indicators	Basel AML Index (jurisdiction-level ML/TF risk context)	https://index.baselgovernance.org/
Analytical caveat	Context only; not predictors or country-label sources in the revised model	https://index.baselgovernance.org/
Source-review analytical workbook	Internal consistency/check file for labelled subset and reported outputs; not original Elliptic raw data	Uploaded/reviewed analytical workbook; original Elliptic files still required for audit replication

Table A2. Country and regulatory context sources

Country / Context	Source	URL
United States	Financial Crimes Enforcement Network (FinCEN)	https://www.fincen.gov/
Singapore	Monetary Authority of Singapore (AML page)	https://www.mas.gov.sg/regulation/anti-money-laundering
Singapore	MAS regulations and guidance (AML topic filter)	https://www.mas.gov.sg/regulation/anti-money-laundering
Singapore	National anti-money laundering strategy (MAS publication)	https://www.mas.gov.sg/regulation/anti-money-laundering
United Arab Emirates	Central Bank of the UAE (AML/CFT)	https://www.centralbank.ae/en/our-operations/anti-money-laundering-and-combating-the-financing-of-terrorism/
United Arab Emirates	UAE Government portal (combatting money laundering)	https://u.ae/en/information-and-services/justice-safety-and-the-law/handling-money-laundering
United Arab Emirates	NAMLCFTC (National AML/CFT Committee)	https://www.namlcftc.gov.ae/
All three (context only)	Basel AML Index (annual public editions; jurisdiction-level risk context)	https://index.baselgovernance.org/

http://dx.doi.org/10.21511/imfi.23(3).2026.27