Integrating Machine Learning in Anti-Money Laundering through Crypto: A Comprehensive Performance Review

Japinye A. O.*
Banking Supervision Department, Central Bank of Nigeria, Nigeria

doi: https://doi.org/10.37745/ejaafr.2013/vol12n45480 Published March 23, 2024

Citation: Japinye A. O. (2024) Integrating Machine Learning in Anti-Money Laundering through Crypto: A Comprehensive Performance Review, *European Journal of Accounting, Auditing and Finance Research*, Vol.12, No. 4, pp.,54-80

ABSTRACT: *The integration of machine learning (ML) algorithms in Anti-Money Laundering (AML) practices has garnered significant attention due to its potential to enhance the detection and prevention of illicit activities in the cryptocurrency ecosystem. This systematic literature review analysed the effectiveness of integrating ML algorithms in detecting and preventing crypto laundering activities, identify the most frequently used ML algorithms, examine trends in publication and research methodologies, and discuss key challenges and constraints associated with integrating ML technologies into AML frameworks. A comprehensive search strategy was employed to identify relevant studies, resulting in the inclusion of 52 articles published between 2019 and 2023. The findings reveal a growing interest in the field, with a notable increase in publications in recent years. Traditional ML models such as Logistic Regression, Random Forest, and Support Vector Machine (SVM) remain prevalent, while deep learning models like Multilayer Perceptrons (MLP) and Long Short-Term Memory (LSTM) networks are gaining popularity. Graph Convolutional Networks (GCNs) have emerged as a significant area of exploration, particularly in the context of graph data analysis in cryptocurrencies. Despite advancements in ML, cryptocurrencies continue to pose a high risk of money laundering due to the practical challenge of implementation ownership of the various ML models. Future research should focus on how these challenges will be addressed to ensure the effective and sustainable use of ML technologies in real-world AML practices.*

KEYWORDS: machine learning; anti-money laundering; cryptocurrency; performance review; money laundering; blockchain analytics

INTRODUCTION

Financial crimes have become increasingly complex in recent years, posing significant economic and social threats that are linked to various illicit activities such as money laundering, fraud, human trafficking, sanctions evasion, and terrorism (Gotelaere and Paoli, 2022; Deloitte United Kingdom, 2024). This complexity is exacerbated by the convergence of traditional financial crimes with cybercrimes, which have emerged as the world's leading crime threats and are projected to escalate (INTERPOL, 2022). Anti-money laundering (AML) is taken in this work to mean any measures and regulations that can be put in place to detect and prevent the illegal use of cryptocurrencies for money laundering and other illicit activities. It involves monitoring, identifying, and reporting suspicious transactions or activities related to cryptocurrencies to regulatory authorities. AML aims to ensure that cryptocurrencies are not used as a medium for illicit financial activities, such as terrorist financing, drug trafficking, and other forms of illegal transactions. Globally, the continued regulatory focus on Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) frameworks highlight the persistent efforts aimed at preventing the illicit exploitation of national financial systems, especially in developed countries (Gaviyau and Sibindi, 2023; KPMG, 2023). However, the decentralized dynamics of cryptocurrencies present novel challenges in detecting, preventing, and mitigating financial crimes, necessitating innovative strategies and technologies to safeguard the integrity of financial systems and protect stakeholders from the detrimental effects of criminal activities.

The decentralized and pseudonymous nature of cryptocurrencies combined with the methods criminals use to exploit them pose significant challenges for law enforcement agencies and regulators in combating financial crimes, especially money laundering (Perkins, 2018; Murphy, 2021; Trozze et al., 2022; Makarov and Schoar, 2022). Technology plays a crucial role in combating cryptocurrency money laundering, offering various tools and methods to detect and prevent illicit activities (Anichebe, 2020). Blockchain analytics is a key technology in this regard (Hegadi et al., 2023). This involves analyzing the blockchain to trace the flow of funds and identify suspicious transactions. Forensic tools are also used to investigate cryptocurrency transactions, providing insights into the movement of funds and the identities of the parties involved (Douglas, 2018). Another important technology is the development of machine learning algorithms, which can analyze large volumes of cryptocurrency transaction data to detect patterns indicative of money laundering (Ruiz and Angelis, 2021). These algorithms can flag suspicious transactions for further investigation, helping law enforcement agencies and financial institutions identify and disrupt illicit activities.

Despite the benefits of technology in combating cryptocurrency money laundering, there are also challenges and limitations. One challenge is the evolving nature of cryptocurrency technologies, which can make it difficult for existing tools and algorithms to keep up with new laundering techniques (Giudici, Milne and Vinogradov, 2019). Additionally, the decentralized nature of cryptocurrencies presents challenges in terms of jurisdiction and enforcement, as transactions can occur across borders and outside the reach of traditional regulatory frameworks (World Economic Forum, 2021). Furthermore, the anonymity and pseudo-anonymity offered by cryptocurrencies can make it challenging to trace transactions and identify the individuals behind them (Hazar, 2020). While technology has made significant strides in combating cryptocurrency money laundering, ongoing research and development are needed to address these challenges (Dupuis and Gleason, 2020). This will enhance the effectiveness of anti-money laundering efforts in the cryptocurrency space.

The exploration of new AML strategies is driven by the need for agile and adaptive approaches to detection and prevention (Han et al., 2020). In this regard, the emergence of novel machine learning techniques, which have demonstrated the ability to analyze vast amounts of data and identify patterns indicative of illicit activities, significantly bolstered AML efforts (Chen et al., 2018). Therefore, emerging AML dynamics have led to a notable shift towards the exploration of artificial intelligence (AI) technologies within the AML domain. Researchers are exploring and extending state-of-the-art

AI methods tailored specifically for AML purposes. For example, Han et al. (2020) highlight the growing interest in leveraging AI technologies, particularly through advanced natural language processing and deep-learning techniques, to enhance AML capabilities. Moreover, there is a notable focus on innovation within AML strategies, particularly with the advent of new financial instruments (Conjeaud et al., 2022; Milnerowicz et al., 2023). Moreover, compliance officers are facing challenges in understanding the complexities of managing digital assets within the framework of AML regulations. Furthermore, there has been a significant shift from a compliance-centric mindset to a risk management mindset within the AML and anti-financial crime industry (Han et al., 2020). This indicates a trend towards increased sophistication in frameworks and strategies.

This research aims to advance the understanding of integrating machine learning (ML) methodologies in Anti-money Laundering (AML) practices. It provides empirical insights into the practical implications of ML in combating money laundering and discusses how it can enhance AML efforts. This systematic literature review aims to provide a comprehensive analysis of the current research landscape regarding the integration of machine learning (ML) in anti-money laundering practices. The review aims to evaluate the methodologies, machine learning algorithms used, data sources, performance metrics, and key findings of the selected studies in this domain. The objectives of this systematic literature review are as follows:

1. To analyze the effectiveness of integrating machine learning algorithms in detecting and preventing crypto laundering activities.
2. To identify the most frequently used machine learning algorithms in the context of anti-money laundering and assess their performance.
3. To examine the trends in publication and research methodologies related to integrating machine learning in anti-money laundering practices.
4. To identify and discuss the key challenges and constraints associated with integrating machine learning technologies into anti-money laundering frameworks and provide recommendations for addressing these challenges.

This review adopts a structured approach. Beginning with this introduction that provides an overview of the research topic and outlines the objectives and contributions of the study, the review will proceed to the conceptual framework. This section discusses the conceptual underpinnings of cryptocurrencies and money laundering, and machine learning techniques in AML. Subsequently, the review will detail the methodological approach, describing the systematic review protocol and outlining the procedures for database selection, search strategy, study selection criteria, and data extraction. Afterwards, the review will venture into machine learning techniques in AML, discussing the comparative performances of various developed models in the literature.

Conceptual and Theoretical Framework

Cryptocurrencies and Money Laundering

Cryptocurrencies have gained significant attention and adoption in recent years, offering a digital alternative to traditional currencies (Giudici, Milne and Vinogradov, 2019; Vigliotti and Jones, 2020; Nadeem et al., 2021). Based on blockchain technology, cryptocurrencies are decentralized and operate independently of central banks. Bitcoin, the first and most well-known cryptocurrency, was introduced in 2009, and since then, thousands of other cryptocurrencies have been created, each with its unique features and purposes (Lipman, 2023). On the other hand, money laundering is the process of disguising the origins of illegally obtained money, typically by passing it through a complex sequence of transfers or commercial transactions (Levi and Reuter, 2011; Korauš et al., 2024). This illegal activity allows criminals to make illicit funds appear legitimate. Money laundering poses a serious threat to the integrity of financial systems and is often associated with various criminal activities, including drug trafficking, human trafficking, and terrorism financing (Lawlor-Forsyth and Gallant, 2017). The increasing popularity of cryptocurrencies has raised concerns about their potential use in money laundering activities (Kethineni, 2019). Cryptocurrencies offer a degree of anonymity and ease of transfer that can be attractive to money launderers seeking to conceal the origins of their funds. In addition, the decentralized nature of cryptocurrencies and the lack of a central authority overseeing transactions make them particularly challenging to regulate and monitor for illegal activities.

Cryptocurrencies possess several characteristics that make them appealing for money laundering purposes (Ibrahim, Nnamani and Omoloja, 2021). Pseudo-anonymity is one of the key characteristics, where transactions are recorded on the blockchain but the identities of the parties involved are encrypted (Cretarola, Figà-Talamanca and Grunspan, 2021). This provides a level of privacy and anonymity, making it challenging to trace the flow of funds. Additionally, cryptocurrencies are globally accessible, allowing funds to be moved across borders quickly and easily, further complicating efforts to monitor and regulate transactions (Giudici, Milne and Vinogradov, 2019; Cretarola, Figà-Talamanca and Grunspan, 2021). The decentralized nature of cryptocurrencies, not controlled by any central authority, also adds to their appeal for money laundering. This decentralization makes it difficult for authorities to regulate or monitor transactions effectively. Criminals exploit these characteristics in various ways. Mixing services, or tumblers, are used to mix transactions from multiple users, obscuring the original source of funds (Chohan, 2017; Shojaeenasab, Motamed and Bahrak, 2020). Privacy coins, like Monero, Dash, and Zcash, offer enhanced privacy and anonymity, making it nearly impossible to trace the flow of funds (Stojan, 2023). Layering is another technique, involving moving funds through multiple transactions and accounts to obscure the original source (Mooij, 2023). Criminals may also use multiple wallets and exchanges to transfer funds, making it challenging for authorities to track the flow of money (Nowroozi et al., 2022). Peer-to-peer (P2P) exchanges also allow users to trade cryptocurrencies directly with one another, without a centralized exchange. This method can be used to transfer funds anonymously, as P2P exchanges do not require users to disclose their identities.

Theoretical Foundations of Machine Learning in AML

Statistical Learning Theory

Statistical learning theory serves as the cornerstone of modern machine learning, providing a framework for understanding the process of learning from data (von Luxburg and Schoelkopf, 2008; Makin, 2022). It provides the theoretical foundation for many machine learning algorithms used in

AML. Supervised learning is a type of machine learning where the algorithm is trained on labeled data, meaning the input data is paired with the correct output (Li, Kiseleva and Maarten de Rijke, 2020; Wang et al., 2023). In the context of AML, supervised learning can be used to train models to recognize patterns associated with money laundering in financial transactions. For example, a supervised learning algorithm could be trained to classify transactions as either legitimate or suspicious based on features such as transaction amount, frequency, and destination. Unsupervised learning, on the other hand, is used when the data is not labeled (Naeem et al., 2023). The algorithm must learn the underlying structure of the data without the guidance of labeled examples. In AML, unsupervised learning can be used to detect anomalies or unusual patterns in financial transactions that may indicate money laundering activity. For example, clustering algorithms can group transactions that are similar to each other, helping to identify potentially suspicious transactions. Semi-supervised learning is a combination of supervised and unsupervised learning (van Engelen and Hoos, 2019). It is used when only a small amount of labeled data is available, but there is a larger amount of unlabeled data. Semi-supervised learning algorithms can leverage the unlabeled data to improve the performance of the model. In AML, semi-supervised learning can be used to enhance the detection of suspicious patterns by incorporating information from both labeled and unlabeled data.

Cognitive Computing Models

Cognitive computing models, particularly neural networks and deep learning, have revolutionized the field of Anti-Money Laundering (AML) by enabling more advanced and accurate detection of suspicious activities (Dragoni and Rospocher, 2018). Neural networks are computational models inspired by the human brain's neural structure, consisting of interconnected nodes that process information (Yang et al., 2018). Deep learning is a subset of neural networks that uses multiple layers to extract higher-level features from data (Alzubaidi et al., 2021). In AML, neural networks and deep learning models are used to analyze vast amounts of financial data to detect anomalies and patterns indicative of money laundering or other financial crimes. These models excel at recognizing complex patterns and relationships in data that may be difficult for traditional methods to identify. For example, neural networks can be trained on historical transaction data to learn the normal behavior patterns of customers. They can then flag transactions that deviate significantly from these patterns, such as unusually large transactions or transactions to high-risk countries. Similarly, deep learning models can analyze text data from financial documents or communications to identify suspicious language or patterns of communication associated with money laundering activities.

One of the key advantages of cognitive computing models is their ability to adapt and improve over time (Bansal et al., 2024). As they are exposed to more data, neural networks and deep learning models can refine their algorithms to become more accurate and effective at detecting suspicious activities. This adaptability is crucial in the constantly evolving landscape of financial crime, where new money laundering techniques and patterns emerge regularly. However, cognitive computing models also come with several significant disadvantages that must be considered (Alzubaidi et al., 2021). They are complex, making them hard to understand and explain. They need lots of high-quality labeled data and can overfit, leading to false positives. Moreover, they require significant computational resources and lack interpretability, making their decisions hard to understand. These limitations highlight the need for careful monitoring and validation when using them in AML.

Natural Language Processing (NPL)

Natural Language Processing (NLP) plays a crucial role in Anti-Money Laundering (AML) by enabling the analysis of unstructured data, such as text from financial documents or communications, to identify suspicious activities (Dong et al., 2023). NLP techniques can be used to extract relevant information from this unstructured data and process it for AML purposes. One of the primary applications of NLP in AML is in the analysis of text data to detect patterns or anomalies indicative of money laundering (Han et al., 2018). For example, NLP can be used to analyze transaction descriptions or customer communications to identify keywords or phrases associated with illicit activities. Financial institutions can flag suspicious activities for further investigation by extracting and processing this information. NLP can also be used to improve the efficiency of AML processes by automating tasks that would otherwise require manual intervention (Varshney and Baral, 2022). For instance, NLP-powered chatbots can be used to interact with customers and gather information about their transactions, helping to identify potential money laundering activities more quickly and accurately.

Ensemble Learning Methods

Ensemble learning methods are machine learning techniques that combine multiple individual models to improve the overall performance of the system (Dasari et al., 2023). Two popular ensemble learning methods used in Anti-Money Laundering (AML) are random forests and gradient boosting (Zhang and Trubey, 2018; Jullum et al., 2020). Random forests are an ensemble learning method that uses multiple decision trees to make predictions (Schonlau and Zou, 2020). Each tree is trained on a random subset of the data, and the final prediction is made by aggregating the predictions of all the trees. Random forests are effective in AML because they can handle large datasets with many features and are less prone to overfitting than individual decision trees (Jullum et al., 2020). Gradient boosting is another ensemble learning method that builds multiple weak learners, typically decision trees, sequentially (Bentéjac, Csörgő and Martínez-Muñoz, 2020). Each new tree is trained to correct the errors of the previous trees, gradually improving the model's performance. Gradient boosting is often used in AML because it can capture complex relationships in the data and achieve high levels of accuracy (Zhang and Trubey, 2018). In AML, ensemble learning methods can be applied to improve the accuracy and robustness of predictive models used for detecting suspicious activities. Ensemble methods can reduce the risk of overfitting and improve the generalization of the model to new, unseen data by combining multiple models. This can lead to more reliable and effective detection of money laundering activities, helping financial institutions comply with regulations and protect against financial crime.

Transfer Learning and Domain Adaptation

Transfer learning and domain adaptation are techniques used in machine learning to apply knowledge from one domain or dataset to another, improving the efficiency of models in detecting financial crimes in the context of Anti-Money Laundering (AML) (Suryanto et al., 2022). Transfer learning involves transferring knowledge from a source domain, where there is an abundance of labeled data, to a target domain, where labeled data may be scarce. In AML, transfer learning can be used to leverage models trained on large, labeled datasets from other industries or domains to improve the performance of AML models, even when labeled AML data is limited (Lebichot et al., 2019). Domain adaptation is a related concept that focuses on adapting a model trained on one domain to perform well on a different, but related, domain. In AML, domain adaptation can be used to adapt models trained on data from one financial institution to perform well on data from another institution, even if the data distributions are slightly different (Suryanto et al., 2022). Both transfer learning and domain adaptation can improve the efficiency of machine learning models in AML by reducing the amount of labeled data needed for training and by leveraging knowledge from related domains or datasets. These techniques can help financial institutions detect financial crimes more effectively and efficiently, ultimately improving their ability to comply with regulations and protect against illicit financial activities.

Explainable AI Models

Explainable AI models are essential in Anti-Money Laundering (AML) for several reasons, particularly in regulatory compliance and risk assessment (Weber, Carl and Hinz, 2023). These models provide transparent and interpretable results, enabling financial institutions to understand and trust the decisions made by AI systems (Minh et al., 2021). In regulatory compliance, explainable AI models can help financial institutions meet the requirements of regulatory bodies by providing clear explanations for the decisions made by AI systems. This transparency is crucial for demonstrating compliance with regulations such as the Bank Secrecy Act (BSA) and the EU's Fourth Anti-Money Laundering Directive (AMLD4). Explainable AI models also play a vital role in risk assessment by helping financial institutions understand the factors that contribute to the risk level of a transaction or customer (Dsilva, Johannes Schleiss and Stober, 2023). These models enable institutions to identify and mitigate potential risks more effectively by providing explanations for their decisions. Moreover, explainable AI models help build trust in AI systems among stakeholders, including regulators, customers, and internal users. When AI systems can provide clear explanations for their decisions, stakeholders are more likely to trust the results and rely on them for decision-making.

METHODOLOGY

A systematic literature review was adopted for this study because it provides the highest level of evidence and the least common based on the levels of evidence pyramid in research (Tawfik et al., 2019). Therefore, a comprehensive search strategy was developed to identify relevant academic studies on the integration of machine learning in anti-money laundering (AML) practices. The methodological steps taken are described in the following subsections.

Research Question Formulation

The primary research question of this study is:

What is the performance of machine learning algorithms in enhancing the effectiveness of anti-money laundering measures, and what are the key findings identified in the existing literature?

This research question focuses on evaluating the performance of machine learning algorithms in the context of anti-money laundering (AML). The review aims to assess how effectively machine learning techniques can enhance the detection and prevention of cryptocurrency-related money laundering activities. Specifically, the review seeks to explore existing research to understand the approaches, methodologies, and technologies used in integrating machine learning into AML practices.

Database Selection

The search encompassed several key databases renowned for their comprehensive coverage in the fields of cryptocurrency, machine learning, and AML. IEEE Xplore is one of the primary databases explored which provided access to a plethora of research articles that explored the intersections of cryptocurrency, machine learning, and AML. ScienceDirect, another pivotal database, offered a vast repository of peer-reviewed journals and articles across various disciplines, including those pertinent to the research topic. The ACM Digital Library was also a crucial resource, providing access to a wealth of research articles. Other databases explored include Springer, JSTOR and Scopus. These databases were instrumental in providing a comprehensive view of the current research landscape surrounding the integration of machine learning in AML. Additionally, Google Scholar was utilized to supplement the search for relevant literature. Google Scholar's broad search scope, ensured a comprehensive search that captured a diverse range of perspectives and findings related to the research topic.

Search Terms

A comprehensive set of search terms was developed to ensure the retrieval of relevant academic sources. The search terms were carefully selected to encompass various aspects of the research topic, including cryptocurrency machine learning, AML, and related concepts. Key search terms related to cryptocurrency included "cryptocurrency," "crypto," "digital currency," "Bitcoin," "Ethereum," "blockchain," and "virtual currency". These terms were chosen to capture literature discussing the security measures and technologies employed to protect against cyber threats in AML contexts. For machine learning, terms such as "machine learning," "artificial intelligence," "algorithm, " "deep learning," and "ensemble learning" were included to retrieve articles that explore the application of machine learning techniques in AML for fraud detection and risk assessment.

To capture literature specifically addressing AML practices, terms like "anti-laundering," "financial crime," "money laundering," and "tax evasion" were incorporated. Additionally, terms related to specific technologies and methodologies were included, such as "big data analytics," "natural language processing," "anomaly detection," and "fraud detection". Furthermore, to ensure a comprehensive search, Boolean operators (AND, OR, NOT) were used to combine the search terms effectively. Truncation was also employed to capture variations of search terms. An example of a used search string with truncation is given below:

("crypto*" OR "*coin" OR "blockchain") AND ("machine learning" OR "artificial intelligence" OR "deep learning") AND ("anti-*" OR "launder*" OR "fraud detect*")

Inclusion and Exclusion Criteria

The inclusion criteria for selecting studies were focused on purely academic sources that conducted some form of experiment with machine learning. These also serve as quality assessment criteria for this study. Studies must specifically address the integration of machine learning in the context of AML practices. In order to facilitate reasonable comparison, included studies were further required to have employed the same dataset, the Elliptic Dataset. The Elliptic Dataset is a publicly available dataset containing transaction information from the Bitcoin blockchain. It includes over 200,000 labeled transactions, categorized as "licit" or "illicit," along with features such as transaction size, age, and transaction neighbours' information. The major challenge of working with the Elliptic Dataset and similar cryptocurrency transaction datasets is dealing with the imbalanced nature of the data. In these datasets, the majority of transactions are legitimate, while only a small fraction is associated with illicit activities like money laundering. This imbalance can lead to difficulties in training machine learning models effectively, as they may become biased towards the majority class (legitimate transactions) and perform poorly in detecting the minority class (illicit transactions). Addressing this challenge requires careful consideration of sampling techniques, model evaluation metrics, and algorithm selection. This is arguably the most performance-determining factor that will differentiate the various techniques employed by the studies.

Table 3.1: Inclusion and exclusion criteria

Inclusion Criteria	Exclusion Criteria
Academic studies focusing on integrating machine learning in AML practices	Non-academic sources such as news articles, blog posts, opinion pieces, and non-peer-reviewed publications
Academic papers, journal articles published within the last 5 years	Studies not directly related to integrating machine learning in AML practices
Studies presenting original research, case studies, theoretical frameworks, or conceptual models	Publications older than 5 years
Papers written in English	Papers not written in English
Studies that employed the Elliptic dataset to carry out experiments	Studies that use any other dataset

This review included journal articles from the last 5 years to ensure the relevance and timeliness of the information. The review considers studies that present original research. Case studies, theoretical frameworks, or conceptual models related to the research topic were not considered. Only papers written in English are included to ensure accessibility for analysis and synthesis. On the other hand, the exclusion criteria are designed to exclude non-academic sources and studies that do not directly contribute to the research topic. Non-academic sources such as news articles, blog posts, opinion pieces, and non-peer-reviewed publications are excluded. Studies that are not directly related to the integration of machine learning in AML practices are also excluded. Additionally, publications older than 5 years are excluded to prioritize recent advancements and insights. Papers not written in English are excluded as they may pose challenges for understanding and analysis. The inclusion and exclusion criteria are summarized in Table 3.1.

RESULTS

Fifty-two (52) papers were included in this study based on the various inclusion and exclusion criteria. This section presents the findings of the systematic literature review. The review aimed to analyze the current landscape of research in the domain of integrating cybersecurity measures with machine learning in anti-money laundering practices, focusing on the methodologies, machine learning algorithms used, data sources, performance metrics, and key findings of the selected studies. In the subsequent subsections, the results are presented in a structured manner to provide insights into the effectiveness of integrating machine learning in anti-money laundering, offering valuable implications for future research and industry practices.

Trend of Publication

Table 4.1 organises the publications by year, highlighting the temporal evolution of research in this area. This shows that research in this field has been steadily increasing, with a significant number of publications in recent years, particularly in 2022 and 2023. This also suggests a growing interest and possibly an increasing recognition of the importance of machine learning in AML practices. The result also reveals that conference papers outnumber journal papers in the earlier years (2019-2021), but the trend starts to balance out in 2022 and 2023. This shift could indicate a maturing research field, where more substantial and in-depth studies are being published in journals.

Table 4.1: Publication trend

Year	**Journal Paper**	**Conference Paper**	**Total**
2019	0	1	1
2020	1	4	5
2021	3	6	9
2022	4	9	13
2023	9	15	24
Total	17	35	52

The increasing number of publications over the years suggests a growing depth of research in the field. This indicates also a growing interest and activity in the field, possibly driven by advancements in technology, increased research funding, or emerging trends and challenges in the field. The ratio of journal papers to conference papers remains relatively stable, with a slightly higher number of conference papers overall. This could suggest that researchers in this field value both the depth of journal publications and the visibility and timely dissemination of conference papers.

Trend of Algorithms Explored from 2019-2023

The exploration of machine learning algorithms in research literature reveals a rich diversity of approaches used to address various challenges. The results are presented in the word cloud in Figure 4.1 below and Table 4.2 below. Traditional models like Logistic Regression, Random Forest, and Support Vector Machine (SVM) are still prevalent, showcasing their enduring relevance and effectiveness in certain contexts. However, the rise of deep learning is evident, with models like Multilayer Perceptrons (MLP) and Long Short-Term Memory (LSTM) networks gaining popularity for their ability to handle complex data patterns. Among the most explored machine learning algorithms in the literature, several stand out for their versatility and effectiveness across a wide range of applications. Graph Convolutional Network (GCN) is one of the most explored algorithms in recent years, particularly in the context of graph data. Graph Convolutional Networks (GCNs) have emerged as a significant area of exploration in the context of cryptocurrency data analysis. GCNs are particularly well-suited for analyzing graph-structured data, such as transaction networks in cryptocurrencies. They enable the modeling of relationships between nodes in a graph, which is crucial for understanding the flow of transactions and identifying anomalous behaviour. Furthermore, GCNs have been extended and adapted in various ways to improve their performance and address specific challenges. Variants such as Graph Attention Network (GAT), GraphSAGE, and EvolveGCN have been proposed to enhance the capabilities of GCNs in handling different types of graphs and learning more expressive node representations. The extensive exploration of GCNs highlights the importance of graph-based learning in modern machine learning research and its potential applications in this domain.

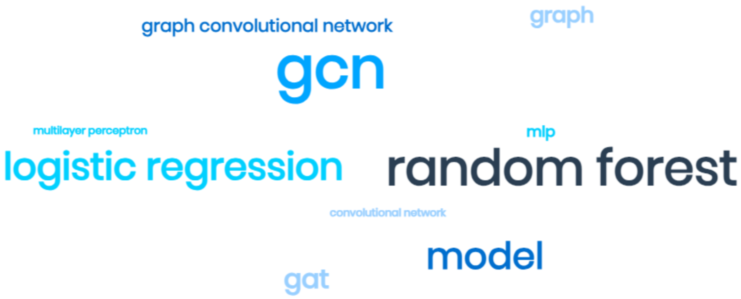

Figure 4.1: Word cloud of the most explored algorithms

Table 4.2: Algorithm trend

word	count	relevance
GCN	52	1
Random Forest	41	0.93
Logistic Regression	28	0.66
GAT	19	0.42
MLP	13	0.31

Random Forest is another popular choice due to its ability to handle both classification and regression tasks, as well as its robustness against overfitting. Its ensemble learning approach, combining multiple decision trees, often yields high performance and is relatively easy to interpret, making it a go-to model for many researchers. Logistic Regression, while a simple linear model, remains highly relevant due to its interpretability and efficiency. It is often used as a baseline model for comparison and is particularly suitable for binary classification tasks. Its simplicity and effectiveness in modeling relationships between variables make it a valuable tool in many machine learning projects. Another extensively explored algorithm is the Gradient Boosting Machine (GBM) family, which includes models like XGBoost, LightGBM, and CatBoost. These algorithms excel in handling structured data and are known for their ability to capture complex patterns in the data. Their popularity stems from their high predictive performance and efficiency, making them well-suited for large-scale machine learning tasks. Deep learning models, especially Multilayer Perceptrons (MLP) and variants like Long Short-Term Memory (LSTM) networks, have also seen significant exploration. These models, with their ability to learn hierarchical representations of data, are particularly effective for tasks involving sequential or time-series data. Their success in areas such as natural language processing and image recognition has led to their widespread adoption and continuous development in research.

Trend of the Best Performing Models

Table 4.3 below highlights several best-performing models across different studies. These models have consistently demonstrated high accuracy and effectiveness in detecting and preventing crypto laundering activities. Among the most frequent best-performing models are Random Forest, XGBoost, and Graph Convolutional Networks (GCNs). These models have been shown to achieve high classification accuracy and other performance metrics across multiple studies, making them popular choices in the field of anti-money laundering.

Table 4.3: Best-performing models

S/N	Study/Paper	Best Performing Model	Evaluation Metrics Used
1	Al Badawi and Al-Haija (2021)	ODT	Classification accuracy: 93.4%, Classification precision: 93.55%, Classification recall: 93.41%, F1-score: 93.5%, Area under the curve (AUC): 0.95
2	Alarab and Prakoonwit (2022a)	Random Forest	Accuracy: 99.42% for Random Forest on Bitcoin dataset and 99.38% for XGBoost on Ethereum dataset, F1-score: 93.93% for Random Forest on Bitcoin dataset and 98.34% for XGBoost on Ethereum dataset, AUC-score: 91.90% for Random Forest on Bitcoin dataset and 99.70% for XGBoost on Ethereum dataset
3	Alarab and Prakoonwit (2022b)	Temporal-GCN	Accuracy: 97.7%, F1-score: 80.6%
4	Alarab, Prakoonwit and Nacer (2020a)	Ensemble Learning	Accuracy: 98.13%, Precision: 99.11%, Recall: 71.93%, F1 score: 83.36%, AUC: 0.933
5	Alarab, Prakoonwit and Nacer (2020b)	GCN-based	Precision: 0.899, Recall: 0.678, F1 score: 0.773, Accuracy: 0.974
6	Alkhatib and Abualigah (2023)	GCN-SGAN	Precision: 0.988, Recall: 0.980, Accuracy: 0.992, F1: 0.981
7	Alotibi et al. (2022)	RF algorithm	F1-score = 0.99, precision = 0.99, recall = 0.99, ROC curve = 0.99
8	Boughaci and Alkhawaldeh (2020)	Random Forest	Correctly Classified Instances: 99.48%, TP Rate: 99.5%, FP Rate: 0.52%, Precision: 99.5%, Recall: 99.5%, ROC: 100%, PRC: 100%

S/N	Study/Paper	Best Performing Model	Evaluation Metrics Used
9	Bynagari and Ayub (2021)	ASXGB	Accuracy: 0.960, Sensitivity: 0.827, Recall: 0.816, F1-score: 0.821
10	Cunha et al. (2023)	Random Forest	F1-score: 0.83, Precision: 0.98, Recall: 0.72
11	de Juan Fidalgo, Cámara and Peris-Lopez (2022)	LSTM	Precision: 0.991, Recall: 0.981, F1 score: 0.985
12	Du et al. (2022)	GraphSniffer	Accuracy: 0.994, Precision: 0.894, Recall: 0.751, F1-Score: 0.816
13	Ehara and Takahashi (2023)	Random Forest	F1-Score: 0.94, Precision: 0.93, Recall: 0.95, Accuracy: 0.97
14	Elbaghdadi, Mezroui and Oualkadi (2021)	Random Forest	Accuracy: 0.98851, Precision: 0.65901, Recall: 0.44866
15	Elmougy and Liu (2023)	Random Forest with feature refinement	For transactions: Precision = 0.986, Recall = 0.727, F1 Score = 0.835, Micro-F1 Score = 0.981, MCC = 0.833, For actors: Precision = 0.921, Recall = 0.802, F1 Score = 0.857, Micro-F1 Score = 0.959, MCC = 0.813
16	Ezhilmathi and Selvakumara (2023)	Random Forest	Precision: 0.981, Recall: 0.651, F1-score: 0.782, Macro-Average F1-score: 0.977, Area under ROC curve: 0.999
17	Feldman et al. (2021)	XGBoost with TomekLinks resampling	Accuracy: 0.9921, Precision: 0.995, Recall: 0.922, F1 score: 0.957, Index of balanced accuracy (IBA): 0.9599
18	Guo et al. (2023)	LB-GLAT	Accuracy: of 0.9776, Precision: 0.9317, Recall: 0.8494, F1-score: 0.8887, AUC: 0.9806
19	Han et al. (2022)	ClusterGCNConv	Precision: 0.8607, Recall: 0.6334, F1 score: 0.7298, Micro-averaged F1 score: 0.9695
20	Hegadi et al. (2023)	LightGBM	Precision: 0.985, Recall: 0.594, F1-score: 0.741, Micro-avg F1-score: 0.974, Cross-validation score: 0.985, Computing time: 9.9 seconds
21	Heidari and Bahrak (2022)	GCN and MLP	Accuracy: 99.58%, Recall: 98.87%, Precision: 95.37%, F1-score: 97.09%
22	Humranan and Supratid (2023)	GCN-6L with FL loss	Precision: 0.9673, Recall: 0.9928, F1: 0.9796, Accuracy: 96.15%

S/N	Study/Paper	Best Performing Model	Evaluation Metrics Used
23	Kolesnikova, Mezentseva and Mukatayev (2021)	Skip-GCN	Accuracy: 0.812, Completeness: 0.623, F1-score: 0.705, Micro-AVG F1-score: 0.966
24	Li et al. (2022a)	Weighted GraphSAGE	Precision: 0.5365, Recall: 0.879, F1-Score: 0.884, Accuracy: 0.875
25	Li et al. (2023)	Cosine similarity-based graph convolutional neural network	Accuracy: 92.01%, Precision: 50.4%, F1: 52.6%, ROC: 64.68%
26	Li and He (2023)	BT2	AUC: 0.93, Precision: 0.86, Recall: 0.87, F1-score: 0.86, Accuracy: 0.86
27	Li et al. (2022b)	ChebNet-GRU	Precision: 0.943, Recall: 0.595, F1-score: 0.729, Micro-average F1-score: 0.971
28	Liu, Xu and Sun (2023)	DDAGAD-EGA	Precision = 0.33, Recall = 0.77, F1-score = 0.59
29	Lo et al. (2023)	Inspection-L using AF+DNE	Precision: 0.972, Recall: 0.721, F1-score: 0.828, AUC: 0.916
30	Lorenz et al. (2020)	Random forest (RF)	Illicit F1-score: 0.83, Number of labels required to achieve near-optimal performance: 500 (1.7% of the total)
31	Mohan et al. (2022)	Graph convolutional decision forest	Illicit F1 score: 0.9525, Precision: 0.9936, Recall: 0.9166, Micro-average F1 score: 0.9191
32	Nicholls, Kuppa and Le-Khac (2023)	ENF with GAT as the backbone model	F1-score: 0.94, Precision: 0.93, Recall: 0.95
33	Ouyang et al. (2023)	Bit-CHetG	Micro F1 Score: 0.95, Macro F1 Score: 0.94, Accuracy: 0.95
34	Patel et al. (2022)	EvAnGCN-H	F1 score: 0.7312, MicroAvg F1 score: 0.7288, Precision: 0.8134, Recall: 0.6331
35	Pocher et al. (2023)	GCN	F1-score: 0.844, Precision: 0.843, Recall: 0.844, Accuracy: 0.844, ROC AUC: 0.844
36	Ruiz and Angelis (2021)	Random forest	Precision: 0.998, Recall: 0.91, F1-score: 0.952
37	Shakiba Tasharrofi and Taheri (2021)	DE-GCN	Micro-Average F1-score: 0.978, F1-score: 0.792, Recall: 0.663, Precision: 0.985
38	Sharma et al. (2023)	Inspection-L	Precision: 0.828, Recall: 0.828, F1-score: 0.721, AUC-Score: 0.972

S/N	Study/Paper	Best Performing Model	Evaluation Metrics Used
39	Singh et al. (2021)	AdaGCN and AdaGAT	Both achieved F1-score of 0.83 on illicit transaction prediction, Precision: 0.97, Recall: 0.72, F1-score: 0.83
40	Sun, Meng and Zheng (2022)	GAME-BC	Accuracy: 0.922, Recall: 0.892, F1-score: 0.907
41	Sureshbhai, Bhattacharya and Tanwar (2020)	KaRuNa	Accuracy: 0.9899, Precision: 0.9957, Recall: 0.9973, F-measure: 0.9965
42	Suri et al. (2023)	Hard voting classifier	Accuracy: 0.99, Specificity: 0.99, Sensitivity: 1.00, F1-score: 0.99
43	Vassallo, Vella and Ellul (2021)	ASXGB	Accuracy: 0.979, Precision: 0.986, Recall: 0.692, F1-Score: 0.813
44	Weber et al. (2019)	Random Forest (RF)	0.956 precision, 0.670 recall, 0.788 F1 score for illicit class, and 0.977 micro-averaged F1 score
45	Yang, Liu and Li (2023)	LSTM + GCN	Accuracy: 0.987, Precision: 0.985, Recall: 0.986, F1-score: 0.986, AUC: 0.998
46	Yu et al. (2022)	ParGCN	Precision: 0.907, Recall: 0.912, F1-score: 0.910, Micro-average F1-score: 0.986
47	Yu et al. (2023)	AEtransGAT	Accuracy: 0.981, Precision: 0.920, Recall: 0.878, F1-score: 0.899
48	Yu, Zhang and Wen (2021)	Extended GAT + random forest	Precision: 0.993, Recall: 0.714, F1-score: 0.834
49	Zanardo et al. (2022)	LightGBM with hyperparameters auto-tuning library (FLAML)	Precision: 0.969, Recall: 0.710, Micro-F1: 0.980, F1: 0.819
50	Zhao, Dong and Bian (2023)	GCN + SSL + Prior	Precision: 0.66, Recall: 0.69, F1-score: 0.69
51	Zheng, Wen and Li (2021)	MP-GAT	Precision: 0.868, Recall: 0.688, F1: 0.767, Accuracy: 0.973
52	Zheng (2022)	GRU-GAT	Accuracy: 99.17%, Recall: 95.45%, F1-score: 95.22%

The literature generally highlights the effectiveness of machine learning models, particularly GCNs, in combating crypto laundering. When all the studies are considered together, it becomes evident that Graph Convolutional Networks (GCNs) emerge as one of the most effective models for detecting crypto laundering activities. GCNs leverage the graph structure of cryptocurrency transactions to capture complex relationships and patterns, allowing them to outperform traditional models in this domain. The evaluation metrics used in these studies, including accuracy, precision, recall, F1-score, and area under the curve (AUC), align well with each other, indicating a consensus on the important metrics for evaluating model performance in this context. These metrics collectively assess the model's ability to correctly identify illicit transactions while minimizing false positives and false negatives. Other models, such as Random Forest and XGBoost, also perform well and are frequently cited as best-performing models in individual studies.

Critical Discussion and Commentary

The findings of this study highlight the practical implications of integrating machine learning in real-world anti-money laundering (AML) practices, particularly in enhancing the detection and prevention of crypto laundering activities. Among the best-performing models identified, Random Forest, XGBoost, and Graph Convolutional Networks (GCNs) offer distinct advantages that can be leveraged in AML operations. Random Forest, known for its versatility, can effectively classify transactions as legitimate or suspicious, aiding in the identification of potential money laundering schemes (Jullum et al., 2020; Lo et al., 2022). Its ensemble learning approach, combining multiple decision trees, provides a robust method for analyzing transaction data and detecting patterns indicative of illicit activities. Similarly, XGBoost's speed and performance make it well-suited for handling large datasets in AML (Vassallo, Vella and Ellul, 2021; Bakry et al., 2023). Its ability to handle complex data patterns and avoid overfitting enhances its utility in identifying and classifying suspicious transactions.

Graph Convolutional Networks (GCNs) stand out for their effectiveness in analyzing graph-structured data, such as transaction networks in cryptocurrencies (Weber et al., 2018; Alarab and Prakoonwit, 2022b; Wei et al., 2023). GCNs can detect anomalous behaviour and illicit transactions that may evade traditional detection methods by modeling the relationships between nodes in a graph. Their ability to capture complex relationships within transaction networks makes them valuable tools for improving the accuracy and efficiency of AML efforts. The application of these models in real-world AML practices offers several benefits. Going by the evidence reviewed, these models can significantly enhance the accuracy of detecting suspicious activities, reducing false positives and negatives. Moreover, the efficiency and scalability of these models enable real-time analysis of transactions, allowing for timely responses to potential threats.

However, despite these advancements in machine learning and the application of sophisticated algorithms, cryptocurrencies continue to present a high risk for money laundering (BBC News, 2022; FATF, 2023). The why is one of the main theses of this review. Besides the inherent characteristics of cryptocurrencies that pose challenges for anti-money laundering efforts, there are other implementation-related challenges, such as ownership and responsibility. One of the key challenges is determining who takes ownership of implementing anti-money laundering measures in the context of cryptocurrencies. Unlike traditional financial systems where financial institutions and regulatory bodies play a central role in implementing and enforcing anti-money laundering regulations, the decentralized nature of the Bitcoin network poses a unique challenge. Since the Bitcoin network is not owned or controlled by any single entity, there is no central authority that can be held responsible for implementing anti-money laundering measures. This lack of centralization complicates efforts to enforce regulations and ensure compliance with anti-money laundering laws.

Cryptocurrency exchanges could potentially take on a significant role and responsibility in implementing anti-money laundering measures. As centralized entities that facilitate the buying, selling, and trading of cryptocurrencies, exchanges are in a position to implement Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures to verify the identities of their users and monitor transactions for suspicious activity. By implementing robust KYC and AML measures, exchanges can help prevent money laundering and illicit activities on their platforms. They can also collaborate with regulatory authorities to ensure compliance with local regulations and reporting requirements. However, while exchanges can play a crucial role in combating money laundering, they may not be able to address all the challenges associated with cryptocurrencies, such as transactions conducted outside of exchanges or the use of privacy coins that offer enhanced anonymity. Collaborative efforts between exchanges, regulators, and other stakeholders are essential to effectively address the risks of money laundering in the cryptocurrency space.

The studies reviewed in this research provide valuable insights into the effectiveness of machine learning algorithms in enhancing anti-money laundering measures. However, one significant gap is the lack of practical implementation strategies and considerations for real-life application, especially concerning the involvement of various stakeholders. Practical implementation requires a comprehensive understanding of the operational dynamics and regulatory environment of cryptocurrency exchanges, financial institutions, regulatory bodies, and law enforcement agencies. While the studies demonstrate the potential of machine learning algorithms, they fall short in addressing the practical challenges and complexities of integrating these algorithms into existing anti-money laundering frameworks. It is crucial for future research to not only focus on the technical aspects of machine learning but also consider the practical implications and feasibility of implementation. This includes addressing issues such as data privacy, regulatory compliance, scalability, and interoperability with existing systems. Furthermore, collaboration among stakeholders is paramount for the successful implementation of machine learning in anti-money laundering practices. Exchanges, regulators, law enforcement agencies, and technology providers need to work together to develop and implement effective strategies that leverage machine learning while addressing the unique challenges of the cryptocurrency ecosystem.

CONCLUSION

This systematic literature review provides a comprehensive analysis of the current state of research in the field of anti-money laundering. The study aimed to analyze methodologies, machine learning algorithms used, data sources, performance metrics, and key findings of selected studies to evaluate the effectiveness of integrating machine learning in anti-money laundering practices. The review revealed a growing interest in this field, as evidenced by the increasing number of publications over the years. Traditional machine learning models like Logistic Regression, Random Forest, and Support Vector Machine (SVM) remain prevalent, but there is a notable rise in the use of deep learning models such as Multilayer Perceptrons (MLP) and Long Short-Term Memory (LSTM) networks. Among the most explored algorithms, Graph Convolutional Networks (GCNs) stand out for their effectiveness in analyzing graph-structured data, particularly in the context of cryptocurrency transaction networks. The study also identified several best-performing models, including Random Forest, XGBoost, and GCNs, which consistently demonstrated high accuracy and effectiveness in detecting and preventing crypto laundering activities. The alignment of evaluation metrics across studies indicates a consensus on the important metrics for evaluating model performance in this context. While the studies reviewed in this research provide valuable insights into the potential of machine learning in anti-money laundering, future research should focus on practical implementation strategies and stakeholder collaboration to ensure the effective and sustainable use of these technologies in real-world scenarios.

REFERENCES

Al Badawi, A. and Al-Haija, Q.A. (2021). Detection of Money Laundering in Bitcoin Transactions. In: *Proceedings Volume of the 4th IET International Smart Cities Symposium, 4th SCS-2021, November 21-23, 2021, Bahrain*. doi:https://doi.org/10.1049/icp.2022.0387.

Alarab, I. and Prakoonwit, S. (2022a). Effect of data resampling on feature importance in imbalanced blockchain data: Comparison studies of resampling techniques. *Data Science and Management*, 5. doi:https://doi.org/10.1016/j.dsm.2022.04.003.

Alarab, I. and Prakoonwit, S. (2022b). Graph-Based LSTM for Anti-money Laundering: Experimenting Temporal Graph Convolutional Network with Bitcoin Data. *Neural Processing Letters*. doi:https://doi.org/10.1007/s11063-022-10904-8.

Alarab, I., Prakoonwit, S. and Nacer, M.I. (2020a). Comparative Analysis Using Supervised Learning Methods for Anti-Money Laundering in Bitcoin. In: *Proceedings of the 2020 5th International Conference on Machine Learning Technologies*. doi:https://doi.org/10.1145/3409073.3409078.

Alarab, I., Prakoonwit, S. and Nacer, M.I. (2020b). Competence of Graph Convolutional Networks for Anti-Money Laundering in Bitcoin Blockchain. In: *Proceedings of the 2020 5th International Conference on Machine Learning Technologies*. doi:https://doi.org/10.1145/3409073.3409080.

Alkhatib, K. and Abualigah, S. (2023). Anti-Laundering Approach for Bitcoin Transactions. In: *2023 14th International Conference on Information and Communication Systems (ICICS)*. doi:https://doi.org/10.1109/icics60529.2023.10330498.

Alotibi, J., Almutanni, B., Alsubait, T., Alhakami, H. and Baz, A. (2022). Money Laundering Detection Using Machine Learning and Deep Learning. *International Journal of Advanced Computer Science and Applications*, 13(10). doi:https://doi.org/10.14569/ijacsa.2022.0131087.

Alzubaidi, L., Zhang, J., Humaidi, A.J., Al-Dujaili, A., Duan, Y., Al-Shamma, O., Santamaría, J., Fadhel, M.A., Al-Amidie, M. and Farhan, L. (2021). Review of Deep learning: concepts, CNN architectures, challenges, applications, Future Directions. *Journal of Big Data*, [online] 8(1). Available at: https://journalofbigdata.springeropen.com/articles/10.1186/s40537-021-00444-8.

Anichebe, U. (2020). Combating Money Laundering in an Age of Technology and Innovation. *SSRN Electronic Journal*. doi:https://doi.org/10.2139/ssrn.3627681.

Bakry, A.N., Alsharkawy, A.S., Farag, M.S. and Raslan, K.R. (2023). Automatic Suppression of False Positive Alerts in anti-money Laundering Systems Using Machine Learning. *The Journal of Supercomputing*. doi:https://doi.org/10.1007/s11227-023-05708-z.

Bansal, G., Chamola, V., Hussain, A., Guizani, M. and Niyato, D. (2024). Transforming Conversations with AI—A Comprehensive Study of ChatGPT. *Cognitive Computation*, 2020. doi:https://doi.org/10.1007/s12559-023-10236-2.

BBC News (2022). *Crypto money laundering rises 30%, report finds*. [online] BBC News. Available at: https://www.bbc.com/news/technology-60072195 [Accessed 10 Mar. 2024].

Bentéjac, C., Csörgő, A. and Martínez-Muñoz, G. (2020). A Comparative Analysis of Gradient Boosting Algorithms. *Artificial Intelligence Review*, 54. doi:https://doi.org/10.1007/s10462-020-09896-5.

Boughaci, D. and Alkhawaldeh, A.A.K. (2020). Enhancing the Security of Financial Transactions in Blockchain by Using Machine Learning techniques: Towards a Sophisticated Security Tool for Banking and Finance. In: *2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH)*. doi:https://doi.org/10.1109/smart-tech49988.2020.00038.

Bynagari, N.B. and Ayub, A. (2021). Anti-Money Laundering Recognition through the Gradient Boosting Classifier. *Academy of Accounting and Financial Studies Journal*, 25(5).

Chen, Z., Van Khoa, L.D., Teoh, E.N., Nazir, A., Karuppiah, E.K. and Lam, K.S. (2018). Machine Learning Techniques for anti-money Laundering (AML) Solutions in Suspicious Transaction detection: A Review. *Knowledge and Information Systems*, [online] 57(2), pp.245–285. doi:https://doi.org/10.1007/s10115-017-1144-z.

Chohan, U.W. (2017). *The Cryptocurrency Tumblers: Risks, Legality and Oversight*. [online] papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080361.

Conjeaud, O., Jimenez, M., Werner, S. and Wild, P. (2022). *Anti-money-laundering Innovations and Evolving Financial Crime risks: The Future of Compliance*. [online] McKinsey & Company. Available at: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/anti-money-laundering-innovations-and-evolving-financial-crime-risks-the-future-of-compliance [Accessed 7 Feb. 2024].

Cretarola, A., Figà-Talamanca, G. and Grunspan, C. (2021). Blockchain and cryptocurrencies: Economic and Financial Research. *Decisions in Economics and Finance*, 44(2), pp.781–787. doi:https://doi.org/10.1007/s10203-021-00366-3.

Cunha, L.L., Brito, M.A., Oliveira, D.F. and Martins, A.P. (2023). Active Learning in the Detection of Anomalies in Cryptocurrency Transactions. *Machine learning and knowledge extraction*, 5(4), pp.1717–1745. doi:https://doi.org/10.3390/make5040084.

Dasari, A.K., Biswas, S.Kr., Thounaojam, D.M., Devi, D. and Purkayastha, B. (2023). Ensemble Learning Techniques and Their Applications: An Overview. *Cognitive Science and Technology*, pp.897–912. doi:https://doi.org/10.1007/978-981-19-8086-2_85.

de Juan Fidalgo, P., Cámara, C. and Peris-Lopez, P. (2022). Generation and Classification of Illicit Bitcoin Transactions. *Proceedings of the International Conference on Ubiquitous Computing & Ambient Intelligence (UCAmI 2022)*, pp.1086–1097. doi:https://doi.org/10.1007/978-3-031-21333-5_108.

Deloitte United Kingdom. (2024). *Future of Financial Crime*. [online] Available at: https://www2.deloitte.com/uk/en/pages/financial-advisory/articles/future-of-financial-crime.html [Accessed 7 Feb. 2024].

Dong, H., Dong, J., Yuan, S. and Guan, Z. (2023). Adversarial Attack and Defense on Natural Language Processing in Deep Learning: A Survey and Perspective. *Lecture Notes in Computer Science*, 13655, pp.409–424. doi:https://doi.org/10.1007/978-3-031-20096-0_31.

Douglas (2018). *Cryptocurrency and the Blockchain: A Discussion of Forensic Needs*. [online] International Journal of Cyber-Security and Digital Forensics. Available at: https://www.academia.edu/38053267/Cryptocurrency_and_the_Blockchain_A_Discussion_of_Forensic_Needs [Accessed 11 Mar. 2024].

Dragoni, M. and Rospocher, M. (2018). Applied Cognitive computing: challenges, approaches, and real-world Experiences. *Progress in Artificial Intelligence*, 7(4), pp.249–250. doi:https://doi.org/10.1007/s13748-018-0166-4.

Dsilva, V., Johannes Schleiss and Stober, S. (2023). Trustworthy Academic Risk Prediction with Explainable Boosting Machines. *Lecture Notes in Computer Science*, 13916, pp.463–475. doi:https://doi.org/10.1007/978-3-031-36272-9_38.

Du, H., Shen, M., Sun, R., Jia, J., Zhu, L. and Zhai, Y. (2022). *Malicious Transaction Identification in Digital Currency via Federated Graph Deep Learning*. [online] IEEE Xplore. doi:https://doi.org/10.1109/INFOCOMWKSHPS54753.2022.9797992.

Dupuis, D. and Gleason, K.C. (2020). *Money Laundering with Cryptocurrency: Open Doors and the Regulatory Dialectic*. [online] Ssrn.com. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3681297 [Accessed 11 Mar. 2024].

Ehara, T. and Takahashi, H. (2023). Bitcoin Fraudulent Transaction Detection Vulnerability. *Smart innovation, systems and technologies*, pp.183–193. doi:https://doi.org/10.1007/978-981-99-3068-5_17.

Elbaghdadi, A., Mezroui, S. and Oualkadi, A.E. (2021). SVM: An Approach to Detect Illicit Transaction in the Bitcoin Network. *Lecture notes in networks and systems*, pp.1130–1141. doi:https://doi.org/10.1007/978-3-030-66840-2_86.

Elmougy, Y. and Liu, L. (2023). Demystifying Fraudulent Transactions and Illicit Nodes in the Bitcoin Network for Financial Forensics. In: *KDD'23, August6–10,2023, LongBeach,CA,USA*. Cornell University. doi:https://doi.org/10.1145/3580305.3599803.

Ezhilmathi, S. and Selvakumara, S.S. (2023). Identifying Illicit Transactions in Bitcoin Tumbler Services Using Supervised Machine Learning Algorithms. In: *2023 12th International Conference on Advanced Computing (ICoAC)*. doi:https://doi.org/10.1109/icoac59537.2023.10249782.

FATF (2023). *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*. [online] Fatf-gafi.org. Available at: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-currency-definitions-aml-cft-risk.html [Accessed 10 Mar. 2024].

Feldman, E.V., Ruchay, A.N., Matveeva, V.K. and Samsonova, V.D. (2021). Bitcoin Abnormal Transaction Detection Based on Machine Learning. *Communications in computer and information science*, pp.205–215. doi:https://doi.org/10.1007/978-3-030-71214-3_17.

Gaviyau, W. and Sibindi, A.B. (2023). Global Anti-Money Laundering and Combating Terrorism Financing Regulatory Framework: A Critique. *J. Risk Financial Manag.*, 16(7), pp.313–313. doi:https://doi.org/10.3390/jrfm16070313.

Giudici, G., Milne, A. and Vinogradov, D. (2019). Cryptocurrencies: Market Analysis and Perspectives. *Journal of Industrial and Business Economics*, [online] 47(1-18). doi:https://doi.org/10.1007/s40812-019-00138-6.

Gotelaere, S. and Paoli, L. (2022). Prevention and Control of Financial Fraud: A Scoping Review. *European Journal on Criminal Policy and Research*. doi:https://doi.org/10.1007/s10610-022-09532-8.

Guo, C., Zhang, S., Zhang, P., Alkubati, M. and Song, J. (2023). LB-GLAT: Long-Term Bi-Graph Layer Attention Convolutional Network for Anti-Money Laundering in Transactional Blockchain. *Mathematics*, 11(18), pp.3927–3927. doi:https://doi.org/10.3390/math11183927.

Han, H., Wang, R., Chen, Y., Xie, K. and Zhang, K. (2022). Research on Abnormal Transaction Detection Method for Blockchain. *Communications in Computer and Information Science*, pp.223–236. doi:https://doi.org/10.1007/978-981-19-8043-5_16.

Han, J., Barman, U., Hayes, J., Du, J., Burgin, E. and Wan, D. (2018). *NextGen AML: Distributed Deep Learning based Language Technologies to Augment Anti Money Laundering Investigation*. [online] AMLWeb. doi:https://doi.org/10.18653/v1/P18-4007.

Han, J., Huang, Y., Liu, S. and Towey, K. (2020a). Artificial Intelligence for anti-money laundering: A Review and Extension. *Digital Finance*, 2(3-4), pp.211–239. doi:https://doi.org/10.1007/s42521-020-00023-1.

Han, J., Huang, Y., Liu, S. and Towey, K. (2020b). Artificial intelligence for anti-money laundering: A review and extension. *Digital Finance*, 2(3-4), pp.211–239. doi:https://doi.org/10.1007/s42521-020-00023-1.

Hazar, H.B. (2020). Anonymity in Cryptocurrencies. *Eurasian Studies in Business and Economics*, 14(1), pp.171–178. doi:https://doi.org/10.1007/978-3-030-53536-0_12.

Hegadi, R., Tripathi, B., Namratha, S.H., Parveez, A., Chaturvedi, A., Hariprasad, M. and Priyanga, P. (2023). Anti-money Laundering Analytics on the Bitcoin Transactions. *Lecture Notes in Electrical Engineering*, pp.405–418. doi:https://doi.org/10.1007/978-981-99-5091-1_29.

Heidari, A. and Bahrak, B. (2022). A graph-based Deep Learning Approach for Illegal Transaction Detection in Bitcoin. *Research Square (Research Square)*. doi:https://doi.org/10.21203/rs.3.rs-2194869/v1.

Humranan, P. and Supratid, S. (2023). A Study on GCN Using Focal Loss on Class-Imbalanced Bitcoin Transaction for Anti-Money Laundering Detection. In: *2023 International Electrical Engineering Congress (iEECON)*. doi:https://doi.org/10.1109/ieecon56657.2023.10126580.

Ibrahim, S., Nnamani, D. and Omoloja, A. (2021). Cybercrime, Anonymity, and Link to Cryptocurrency. *American Journal of Engineering Research (AJER)*, [online] 10(10). Available at: https://www.researchgate.net/publication/356815618_Cybercrime_Anonymity_and_Link_to_Cryptocurrency [Accessed 11 Mar. 2024].

INTERPOL (2022). *Financial and cybercrimes top global police concerns, says new INTERPOL report*. [online] Interpol.int. Available at: https://www.interpol.int/en/News-and-Events/News/2022/Financial-and-cybercrimes-top-global-police-concerns-says-new-INTERPOL-report [Accessed 7 Feb. 2024].

Jones, R. (2021). *Natwest Fined £264m after Taking Deposits of Laundered Cash in Bin Bags*. [online] The Guardian. Available at: https://www.theguardian.com/business/2021/dec/13/natwest-fined-264m-after-admitting-breaching-anti-money-laundering-rules.

Jullum, M., Løland, A., Huseby, R.B., Ånonsen, G. and Lorentzen, J. (2020). Detecting Money Laundering Transactions with Machine Learning. *Journal of Money Laundering Control*, 23(1), pp.173–186. doi:https://doi.org/10.1108/jmlc-07-2019-0055.

Kethineni, S. (2019). *The Rise in Popularity of Cryptocurrency and Associated Criminal Activity*. [online] International Criminal Justice Review. Available at: https://www.academia.edu/87731294/The_Rise_in_Popularity_of_Cryptocurrency_and_Associated_Criminal_Activity [Accessed 11 Mar. 2024].

Kolesnikova, K., Mezentseva, O. and Mukatayev, T. (2021). *Analysis of Bitcoin Transactions to Detect Illegal Transactions Using Convolutional Neural Networks*. [online] IEEE Xplore. doi:https://doi.org/10.1109/SIST50301.2021.9465983.

Korauš, A., Jančíková, E., Gombár, M., Kurilovská, L. and Černák, F. (2024). Ensuring Financial System Sustainability: Combating Hybrid Threats through Anti-Money Laundering and Counter-Terrorist Financing Measures. *Journal of risk and financial management*, 17(2), pp.55–55. doi:https://doi.org/10.3390/jrfm17020055.

KPMG. (2023). *Fraud and Financial Crime: 2023 Regulatory Challenges*. [online] Available at: https://kpmg.com/us/en/articles/2022/ten-key-regulatory-challenges-2023-fraud-financial-crime.html [Accessed 7 Feb. 2024].

Lawlor-Forsyth, E. and Gallant, M.M. (2017). Financial Institutions and Money laundering: A Threatening relationship? *Journal of Banking Regulation*, 19(2), pp.131–148. doi:https://doi.org/10.1057/s41261-017-0041-4.

Lebichot, B., Le Borgne, Y.-A., He-Guelton, L., Oblé, F. and Bontempi, G. (2019). Deep-Learning Domain Adaptation Techniques for Credit Cards Fraud Detection. *Proceedings of the International Neural Networks Society*, [online] 1, pp.78–88. doi:https://doi.org/10.1007/978-3-030-16841-4_8.

Levi, M. and Reuter, P. (2011). *Money Laundering*. [online] *Oxford Handbooks Online*. Oxford University Press. doi:https://doi.org/10.1093/oxfordhb/9780199844654.013.0015.

Li, A., Wang, Z., Yu, M. and Chen, D. (2022a). Blockchain Abnormal Transaction Detection Method Based on Weighted Sampling Neighborhood Nodes. *2022 3rd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*. doi:https://doi.org/10.1109/icbaie56435.2022.9985815.

Li, X., Yang, Y., Li, B., Li, M., Zhang, J. and Li, T. (2023). Blockchain Cryptocurrency Abnormal Behavior Detection Based on Improved Graph Convolutional Neural Networks. In: *2023 International Conference on Data Security and Privacy Protection (DSPP)*. doi:https://doi.org/10.1109/dspp58763.2023.10404590.

Li, Z. and He, E. (2023). Graph Neural Network-Based Bitcoin Transaction Tracking Model. *IEEE Access*, 11, pp.62109–62120. doi:https://doi.org/10.1109/access.2023.3288026.

Li, Z., Kiseleva, J. and Maarten de Rijke (2020). Rethinking Supervised Learning and Reinforcement Learning in Task-Oriented Dialogue Systems. *Data Archiving and Networked Services (DANS)*, EMNLP 2020. doi:https://doi.org/10.18653/v1/2020.findings-emnlp.316.

Li, Z., Zhang, Y., Wang, Q. and Chen, S. (2022b). Transactional Network Analysis and Money Laundering Behavior Identification of Central Bank Digital Currency of China. *Journal of Social Computing*, [online] 3(3), pp.219–230. doi:https://doi.org/10.23919/JSC.2022.0011.

Lipman, M.A. (2023). On Bitcoin: A Study in Applied Metaphysics. *The Philosophical Quarterly*, 73(3), pp.783–802. doi:https://doi.org/10.1093/pq/pqad030.

Liu, C., Xu, Y. and Sun, Z. (2023). Directed Dynamic Attribute Graph Anomaly Detection Based on Evolved Graph Attention for Blockchain. *Knowledge and Information Systems*. doi:https://doi.org/10.1007/s10115-023-02033-y.

Lo, W., Sarhan, M., Layeghy, S. and Portmann, M. (2022). *Inspection-L: A Self-Supervised GNN-Based Money Laundering Detection System for Bitcoin*. [online] Available at: https://arxiv.org/pdf/2203.10465.pdf [Accessed 30 Aug. 2022].

Lo, W.W., Kulatilleke, G.K., Sarhan, M., Layeghy, S. and Portmann, M. (2023). Inspection-L: self-supervised GNN Node Embeddings for Money Laundering Detection in Bitcoin. *Applied Intelligence*. doi:https://doi.org/10.1007/s10489-023-04504-9.

Lorenz, J., Silva, M.I., Aparício, D., Ascensão, J.T. and Bizarro, P. (2020). Machine Learning Methods to Detect Money Laundering in the Bitcoin Blockchain in the Presence of Label Scarcity. In: *Proceedings of the First ACM International Conference on AI in Finance*. doi:https://doi.org/10.1145/3383455.3422549.

Makarov, I. and Schoar, A. (2022). Cryptocurrencies and Decentralized Finance (DeFi). [online] doi:https://doi.org/10.3386/w30006.

Makin, J.G. (2022). An Introduction to Modern Statistical Learning. *arXiv (Cornell University)*. doi:https://doi.org/10.48550/arxiv.2207.10185.

Milnerowicz, S., Maszewska, J., Skowera, P., Stelmach, M. and Lejman, M. (2023). AML under the Scope: Current Strategies and Treatment Involving FLT3 Inhibitors and Venetoclax-Based Regimens. *International Journal of Molecular Sciences*, 24(21), pp.15849–15849. doi:https://doi.org/10.3390/ijms242115849.

Minh, D., Wang, H.X., Li, Y.F. and Nguyen, T.N. (2021). Explainable Artificial intelligence: A Comprehensive Review. *Artificial Intelligence Review*. doi:https://doi.org/10.1007/s10462-021-10088-y.

Mohan, A., P.V., K., Sankar, P., Manohar K., M. and Peter, A. (2022). Improving anti-money Laundering in Bitcoin Using Evolving Graph Convolutions and Deep Neural Decision Forest. *Data Technologies and Applications*, 57(3), pp.1–17. doi:https://doi.org/10.1108/dta-06-2021-0167.

Mooij, A. (2023). Currency (Layering). *SpringerBriefs in law*, pp.69–86. doi:https://doi.org/10.1007/978-3-031-46417-1_6.

Murphy, H. (2021). How Do Criminals Exploit cryptocurrencies? *Financial Times*. [online] 30 Nov. Available at: https://www.ft.com/content/85c8d520-b2d9-4a35-abdb-2f56cdd48792.

Nadeem, M.A., Liu, Z., Pitafi, A.H., Younis, A. and Xu, Y. (2021). Investigating the Adoption Factors of Cryptocurrencies—A Case of Bitcoin: Empirical Evidence from China. *SAGE Open*, [online] 11(1), p.215824402199870. doi:https://doi.org/10.1177/2158244021998704.

Naeem, S., Ali, A., Anam, S. and Ahmed, M.M. (2023). An Unsupervised Machine Learning Algorithms: Comprehensive Review. *International Journal of Computing and Digital Systems*, 13(1), pp.911–921. doi:https://doi.org/10.12785/ijcds/130172.

Nicholls, J., Kuppa, A. and Le-Khac, N.-A. (2023). FraudLens: Graph Structural Learning for Bitcoin Illicit Activity Identification. In: *ACSAC '23, December 04–08, 2023, Austin, TX, USA*. doi:https://doi.org/10.1145/3627106.3627200.

Nowroozi, E., Seyedshoari, S., Mekdad, Y., Savaş, E. and Conti, M. (2022). Cryptocurrency Wallets: Assessment and Security. *In: Maleh, Y., Alazab, M., Romdhani, I. (eds) Blockchain for Cybersecurity in Cyber-Physical Systems. Advances in Information Security*, 102, pp.1–19. doi:https://doi.org/10.1007/978-3-031-25506-9_1.

Ouyang, S., Bai, Q., Feng, H. and Hu, B. (2023). Bitcoin Money Laundering Detection via Subgraph Contrastive Learning. *Entropy*, 26(211).

Patel, V., Rajasegarar, S., Pan, L., Liu, J. and Zhu, L. (2022). EvAnGCN: Evolving Graph Deep Neural Network Based Anomaly Detection in Blockchain. *Lecture Notes in Computer Science*, pp.444–456. doi:https://doi.org/10.1007/978-3-031-22064-7_32.

Perkins, D.W. (2018). Financial Innovation: 'Cryptocurrencies'. [online] Available at: https://crsreports.congress.gov/product/pdf/IF/IF10824 [Accessed 11 Mar. 2024].

Pocher, N., Zichichi, M., Merizzi, F., Shafiq, M.Z. and Ferretti, S. (2023). Detecting Anomalous Cryptocurrency transactions: an AML/CFT Application of Machine learning-based Forensics. *Electronic Markets*, 33(1). doi:https://doi.org/10.1007/s12525-023-00654-3.

Ruiz, E.P. and Angelis, J. (2021). Combating Money Laundering with Machine Learning – Applicability of supervised-learning Algorithms at Cryptocurrency Exchanges. *Journal of Money Laundering Control*, ahead-of-print(ahead-of-print). doi:https://doi.org/10.1108/jmlc-09-2021-0106.

Schonlau, M. and Zou, R.Y. (2020). The Random Forest Algorithm for Statistical Learning. *The Stata Journal: Promoting Communications on Statistics and Stata*, [online] 20(1), pp.3–29. doi:https://doi.org/10.1177/1536867x20909688.

Shakiba Tasharrofi and Taheri, H. (2021). DE-GCN: Differential Evolution as an Optimization Algorithm for Graph Convolutional Networks. In: *26th International Computer Conference, Computer Society of Iran, Tehran, Iran.* doi:https://doi.org/10.1109/csicc52343.2021.9420542.

Sharma, A., Singh, P.K., Podoplelova, E., Gavrilenko, V., Tselykh, A. and Bozhenyuk, A. (2023). Graph Neural Network-Based Anomaly Detection in Blockchain Network. *Lecture notes in networks and systems*, pp.909–925. doi:https://doi.org/10.1007/978-981-99-1479-1_67.

Shojaeenasab, A., Motamed, A. and Bahrak, B. (2020). *Mixing Detection on Bitcoin Transactions Using Statistical Patterns 1*. [online] Available at: https://arxiv.org/pdf/2204.02019 [Accessed 11 Mar. 2024].

Singh, A., Gupta, A., Wadhwa, H., Asthana, S. and Arora, A. (2021). Temporal Debiasing Using Adversarial Loss Based GNN Architecture for Crypto Fraud Detection. *2021 20th IEEE International Conference on Machine Learning and Applications (ICMLA)*. doi:https://doi.org/10.1109/icmla52953.2021.00067.

Sousa, A., Calçada, E., Rodrigues, P. and Pinto Borges, A. (2022). Cryptocurrency adoption: A systematic Literature Review and Bibliometric Analysis. *EuroMed Journal of Business*, 17(3). doi:https://doi.org/10.1108/emjb-01-2022-0003.

Stojan, J. (2023). *Exploring Monero and ZCash: a deep dive into privacy coins - Digital Journal*. [online] Digital Journal. Available at: https://www.digitaljournal.com/business/privacy-coins-an-inside-look-at-monero-and-zcash/article [Accessed 11 Mar. 2024].

Sun, K., Meng, K. and Zheng, Z. (2022). GAME-BC: A Graph Attention Model for Exploring Bitcoin Crime. In: *2022 6th International Symposium on Computer Science and Intelligent Control (ISCSIC)*. doi:https://doi.org/10.1109/iscsic57216.2022.00077.

Sureshbhai, P.N., Bhattacharya, P. and Tanwar, S. (2020). KaRuNa: A Blockchain-Based Sentiment Analysis Framework for Fraud Cryptocurrency Schemes. *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*. doi:https://doi.org/10.1109/iccworkshops49005.2020.9145151.

Suri, A., Rathore, M., Kumar, D., None Aakansha and Shivangi Raghav (2023). An Ensemble Learning Approach for Classifying Illicit Transactions in Bitcoin. In: *Proceedings of the 2023 3rd International Conference on Technological Advancements in Computational Sciences*. doi:https://doi.org/10.1109/ictacs59847.2023.10390133.

Suryanto, H., Mahidadia, A., Bain, M., Guan, C. and Guan, A. (2022). Credit Risk Modeling Using Transfer Learning and Domain Adaptation. *Frontiers in Artificial Intelligence*, 5. doi:https://doi.org/10.3389/frai.2022.868232.

Tawfik, G.M., Dila, K.A.S., Mohamed, M.Y.F., Tam, D.N.H., Kien, N.D., Ahmed, A.M. and Huy, N.T. (2019). A Step by Step Guide for Conducting a Systematic Review and meta-analysis with Simulation Data. *Tropical Medicine and Health*, [online] 47(1), pp.1–9. doi:https://doi.org/10.1186/s41182-019-0165-6.

Trozze, A., Kamps, J., Akartuna, E.A., Hetzel, F.J., Kleinberg, B., Davies, T. and Johnson, S.D. (2022). Cryptocurrencies and Future Financial Crime. *Crime Science*, 11(1). doi:https://doi.org/10.1186/s40163-021-00163-8.

van Engelen, J.E. and Hoos, H.H. (2019). A Survey on semi-supervised Learning. *Machine Learning*, [online] 109. doi:https://doi.org/10.1007/s10994-019-05855-6.

Varshney, N. and Baral, C. (2022). Model Cascading: Towards Jointly Improving Efficiency and Accuracy of NLP Systems. *arXiv (Cornell University)*. doi:https://doi.org/10.18653/v1/2022.emnlp-main.756.

Vassallo, D., Vella, V. and Ellul, J. (2021). Application of Gradient Boosting Algorithms for Anti-money Laundering in Cryptocurrencies. *SN Computer Science*, [online] 2(3), p.143. doi:https://doi.org/10.1007/s42979-021-00558-z.

Vigliotti, M.G. and Jones, H. (2020). The Rise and Rise of Cryptocurrencies. *Springer eBooks*, pp.71–91. doi:https://doi.org/10.1007/978-3-030-21107-3_5.

von Luxburg, U. and Schoelkopf, B. (2008). *Statistical Learning Theory: Models, Concepts, and Results*. [online] arXiv.org. doi:https://doi.org/10.48550/arXiv.0810.4752.

Wang, Y., Chen, Q., Ahmed, M.H.M., Chen, Z., Su, J., Pan, W. and Li, Z. (2023). Supervised Gradual Machine Learning for Aspect-Term Sentiment Analysis. *Transactions of the Association for Computational Linguistics*, 11, pp.723–739. doi:https://doi.org/10.1162/tAML_a_00571.

Weber, M., Chen, J., Suzumura, T., Pareja, A., Ma, T., Kanezashi, H., Kaler, T., Leiserson, C.E. and Schardl, T.B. (2018). *Scalable Graph Learning for Anti-Money Laundering: A First Look*. [online] arXiv.org. doi:https://doi.org/10.48550/arXiv.1812.00076.

Weber, M., Domeniconi, G., Chen, J., Karl, D., Bellei, C., Robinson, T. and Leiserson, C.E. (2019). Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for

Financial Forensics. In: *KDD'19 Workshop on Anomaly Detection in Finance, August 2019, Anchorage, AK, USA*.

Weber, P., Carl, K.V. and Hinz, O. (2023). Applications of Explainable Artificial Intelligence in Finance—a Systematic Review of Finance, Information Systems, and Computer Science Literature. *Management Review Quarterly*, 2023. doi:https://doi.org/10.1007/s11301-023-00320-0.

Wei, T., Zeng, B., Guo, W., Guo, Z., Tu, S. and Xu, L. (2023). A Dynamic Graph Convolutional Network for Anti-money Laundering. *Lecture Notes in Computer Science*, pp.493–502. doi:https://doi.org/10.1007/978-981-99-4761-4_42.

World Economic Forum (2021). *Navigating Cryptocurrency Regulation: An Industry Perspective on the Insights and Tools Needed to Shape Balanced Crypto Regulation S E P T E M B E R 2 0 2 1 Global Future Council on Cryptocurrencies Contents*. [online] Available at: https://www3.weforum.org/docs/WEF_Navigating_Cryptocurrency_Regulation_2021.pdf.

Yang, G., Liu, X. and Li, B. (2023). Anti-money Laundering Supervision by Intelligent Algorithm. *Computers & Security*, 132, pp.103344–103344. doi:https://doi.org/10.1016/j.cose.2023.103344.

Yang, P., Sun, X., Li, W. and Ma, S. (2018). Automatic Academic Paper Rating Based on Modularized Hierarchical Convolutional Neural Network. *arXiv (Cornell University)*. doi:https://doi.org/10.18653/v1/p18-2079.

Yu, L., Jing, Q., Li, R., Cheng, Z. and Xu, C. (2022). ParGCN: Abnormal Transaction Detection based on Graph Neural Networks. In: *2022 IEEE 22nd International Conference on Software Quality, Reliability and Security (QRS)*. doi:https://doi.org/10.1109/qrs57517.2022.00085.

Yu, L., Zhang, F., Ma, J., Yang, L., Yang, Y. and Jia, W. (2023). Who Are the Money Launderers? Money Laundering Detection on Blockchain via Mutual Learning-Based Graph Neural Network. In: *2023 International Joint Conference on Neural Networks (IJCNN)*. doi:https://doi.org/10.1109/ijcnn54540.2023.10191217.

Yu, L., Zhang, N. and Wen, W. (2021). Abnormal Transaction Detection based on Graph Networks. In: *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*. doi:https://doi.org/10.1109/compsac51774.2021.00051.

Zanardo, E., Domiziani, G.P., Iosif, E. and Christodoulou, K. (2022). Identification of Illicit Blockchain Transactions Using Hyperparameters Auto-tuning. *Springer eBooks*, pp.27–38. doi:https://doi.org/10.1007/978-3-031-10507-4_2.

Zhang, Y. and Trubey, P. (2018). Machine Learning and Sampling Scheme: An Empirical Study of Money Laundering Detection. *Computational Economics*, 54(3), pp.1043–1063. doi:https://doi.org/10.1007/s10614-018-9864-z.

Zhao, K., Dong, G. and Bian, D. (2023). Detection of Illegal Transactions of Cryptocurrency Based on Mutual Information. *Electronics*, [online] 12(7), p.1542. doi:https://doi.org/10.3390/electronics12071542.

Zheng, H., Wen, B. and Li, Y. (2021). Recognize Illegal Transactions in the Bitcoin Network Using Graph Attention with DIKW. In: *2021 IEEE 23rd Int Conf on High Performance Computing & Communications*. doi:https://doi.org/10.1109/hpcc-dss-smartcity-dependsys53884.2021.00315.

Zheng, Y. (2022). GRU-GAT Model for Blockchain Bitcoin Abnormal Transaction Detection. In: *2022 IEEE Conference on Telecommunications, Optics and Computer Science (TOCS)*. doi:https://doi.org/10.1109/tocs56154.2022.10016137.

Short biographical notes on all contributors here.

Abayomi Oluwaseun Japinye has 10+ years of experience in banking supervision, cybersecurity, and risk management. As a Cybersecurity Examiner, AML/CFT Examiner, and Bank Supervisor, he excels in implementing security best practices and ensuring regulatory compliance. He evaluates AML/CFT policies, conducts cybersecurity assessments, and enforces standards such as ISO 27001, GDPR, and PCI DSS. Abayomi navigates complex regulatory environments, protecting financial institutions against emerging threats and fostering resilience in the face of evolving cybersecurity challenges.