A Review on Anti money Laundering Systems for Cryptocurrencies

[1]Gautam Kunal, [2]Rajeev Raghuwansi
[1,2]Department of CSE, Radharaman Engineering College, Bhopal (M.P.)
[1]gauk007@gmail.com, [2]ktrajeev.mgi@gmail.com

* Corresponding Author: Gautam Kunal

Abstract: Cryptocurrencies have been developing very rapidly in recent years, and their use is becoming more and more widespread in different areas. The use of digital currencies for legal uses is advancing along with technological development, but, at the same time, criminal activities are also emerging to take advantage of this boom. The aim of this paper has been, first, to analyze the various ways in which individuals and criminal organizations have taken advantage of the phenomenon of cryptocurrencies to carry out fraudulent activities such as laundering money of illicit origin. This study focuses on the detection of illicit activities (e.g., scams, financing terrorism, and Ponzi schemes) on cryptocurrency infrastructures, both at an account and transaction level. Previous work has identified that class imbalance and the dynamic environment created by the evolving techniques deployed by criminals to avoid detection are widespread in this domain.

Keywords: *Cryptocurrencies; Risks; Fraud Practices; Prevention; Risk Reduction.*

I. Introduction

Cryptocurrency is a digital currency in which transactions are verified and records maintained by a decentralized system using cryptography, rather than by a centralized authority. It is not issued by any central authority, rendering it theoretically immune to government interference or manipulation. According to blockchain analytics firm Chainalysis, Criminals laundered $2.8bn in 2019 in Bitcoin to exchanges. Money laundering is a threat to the world economy , and so, Anti-Money Laundering (AML) guidelines are set to prevent the damage caused by this activity. The Financial Action Task Force started to recommend that financial institutions should migrate from rule-based systems to a more risk-oriented approach to prevent money laundering [1]. The European Union recently adopted the 'Fifth Anti-Money Laundering Directive' (5AMLD) to counteract financing of terrorism and money laundering. The law applies to exchanges allowing its users to trade crypto-to-crypto or crypto-to-fat (or vice-versa) and wallet service providers holding the users' private keys. These entities are obliged to apply proper customer due diligence, monitor transactions, maintain customer history, and report any transactions which are deemed as suspicious. Similar guidelines were set out by the Financial Action Task Force (FATF) to its member jurisdictions (including the United Kingdom and the United States) to regulate cryptocurrency marketplaces [2]. These guidelines are set to prevent criminals from injecting illicitly gained funds into the financial system while avoiding detection. A lack of AML controls can result in hefty fnes, as can be seen with HSBC and Danske Bank scandals. Given the rise in popularity of cryptocurrencies, coupled with the fear of criminals hiding behind the pseudonymous nature of this technology, governing bodies started to establish regulations to circumvent money laundering. Money laundering using fiat currency has been pervasive for decades and regulators have devised ways to dissuade and take punitive actions against such malfeasance [3]. Many legal provisions and amendments have been enacted to implement anti-money laundering (AML) measures, such as the Bank Secrecy Act in the U.S., and the U.S.A. Patriot Act, to name two. However, the advent of cryptocurrencies such as Bitcoin and Ethereum has disrupted the banking industry by eliminating the use of a central authority and enabling cashless, anonymous transactions (in an anonymous transaction, the identity of the users taking part in the transaction remains hidden). Since, in cryptocurrency transactions, users use pseudonyms, and the currency itself is not nationally issued or regulated, it becomes harder to track down the origins of illicit money. While a single pseudonym can be linked to an individual, e.g., by examining transaction graphs, a criminal could potentially use thousands of different pseudonyms which makes linking difficult. In reports published by blockchain analytics companies Ciphertrace and Chainalysis , money laundering tripled from USD 200 million in 2017 to USD 700 million in 2018, and in 2020, a total of USD 1.3 billion was laundered with USD 41.2 million being laundered using Bitcoin. These significant numbers call for a survey of existing AML approaches, and the challenges in implementing them [4].

II. Literature Review

Vassallo et al.[1] propose Adaptive Stacked eXtreme Gradient Boosting (ASXGB), an adaptation of eXtreme Gradient Boosting (XGBoost), to better handle dynamic environments and present a comparative analysis of various ofine decision tree-based ensembles and heuristic-based data-sampling techniques. Our results show that: (i) ofine decision treebased gradient boosting algorithms outperform state-of-the-art Random Forest (RF) results at both an account and transaction level, (ii) the data-sampling approach NCL-SMOTE further improves recall at a transaction level, and (iii) our proposed ASXGB successfully reduced the impact of concept drift while further improving recall at a transaction level.

Kolachala et al.[2] examine current anti-money laundering (AML) mechanisms in cryptocurrencies and payment networks from a technical and policy perspective, and point out practical challenges in implementing and enforcing them. We first discuss blacklisting, a recently proposed technique to combat money laundering, which seems appealing, but leaves several unanswered questions and challenges with regard to its enforcement. We then discuss payment networks and find that there are unique problems in the payment network domain that might require customdesigned AML solutions, as opposed to general cryptocurrency AML techniques.

Developed a financial institution initiatives [3] based on Robotic Process Automation (RPA) solutions that allow to improve processes' efficiency like investigations of suspicious transactions, the screening of names to identify PEPs, the KYC on-boarding and recertification. Some natural language solutions (translation) are also used.

Shahbazi et al.[4] the Hierarchical Risk Parity and unsupervised machine learning applied on the cryptocurrency framework. The process of professional accounting in term of inherent risk connected with cryptocurrency regarding the occurrence likelihood and statement of financial impact. Determining cryptocurrency risks comprehended to have a high rate of occurrence likelihood and the access of private key which is unauthorized. The professional cryptocurrency experience in transaction cause the lower risk comparing the less experienced one. The Hierarchical Risk Parity gives the better output in term of returning the adjusted risk tail to get the better risk management result.The result section shows the proposed model is robust to various intervals which are re-balanced and the co-variance window estimation.

Wu et al.[5] focus on the detection of the addresses belonging to mixing services, which is an important task for anti-money laundering in Bitcoin. Specifically, we provide a feature-based network analysis framework to identify statistical properties of mixing services from three levels, namely, network level, account level, and transaction level. To better characterize the transaction patterns of different types of addresses, we propose the concept of attributed temporal heterogeneous motifs (ATH motifs). Experiments on real Bitcoin datasets demonstrate the effectiveness of our detection model and the importance of hybrid motifs including ATH motifs in mixing detection.

Pocher et al.[6] provides a techno-legal taxonomy of approaches to balance privacy and transparency in CBDCs without thwarting accountability, but it also underlines cross-sectoral impacts. The contribution heeds regulation-by-design as its core methodological foundation, with Privacy-Enhancing Technologies as the relevant use case. Thus, it highlights that not only technology aids legal purposes, but also that some regulatory requirements ought to be designed into technology for one to reach agreed-upon results and/or standards.

Day et al.[7] conducted a named entity recognition task and identified the key relation types to construct a cryptocurrency anti-money laundering knowledge graph (KG). Accordingly, we developed the "Judicia17," a key relation type for cryptocurrency anti-money laundering KG. The contribution of this study is that the proposed "Judica17" relation types of cryptocurrency anti-money laundering KG can be applied to construct a legal knowledge graph.

Mabunda et al.[8] discusses the intersection between Anti-Money Laundering efforts and the challenges that are introduced by cryptocurrencies such as Bitcoin. It also looks at the case of Liberty Reserve to highlight these challenges.

Baek et al.[9] performed an unsupervised learning expectation maximization (EM) algorithm to cluster the data set. Based on the features engineered from the unsupervised learning, we performed an anomaly detection using Random Forest (RF). In this study, we offered an insight into labeling the cryptocurrency wallets by providing a model for detecting the cryptocurrency with anomalous transactions. We advocate that labeling the wallets with discernible transactions may help financial institutions, private sectors, financial intelligence, and government agencies identify and detect the transactions with illicit activities.

Badawi et al.[10] present an efficient anti-money laundry system that analyzes the transactions of cryptocurrency to learn data patterns that can identify licit and illicit transactions. Our system utilizes known machine learning mechanisms such as shallow neural networks and decision trees to construct the classification models. Without loss of generality, we evaluate our system on a recent bitcoin anti-money laundry dataset, the elliptic dataset, and use the classification accuracy as a performance indicator. Our analysis shows that shallow neural networks and decision trees achieve classification accuracy capped at 89.9% and 93.4%, respectively.

Crawford et al.[11] made an effort to understand and try our best to exhaustively discover Bitcoin mixing or tumbling services (essentially money laundering mechanisms) which exist or had existed. In our study, 69 services were identified, and evaluation of the public discussion around these services reveals certain trends in Bitcoin user understanding of privacy issues and enforcement of anti-money laundering regulation. So far, Law enforcement interference with Bitcoin laundering services is uncommon, while our study showed that most services failed due to lack of user trust. Trust is perhaps the greatest challenge amongst Bitcoin anonymization services, as many services that have existed appear to be outright scams, and even legitimate services sometimes disappear with user funds.

Shamili et al.[12] analysed the distributed decentralized network with the nodes at any place can access the data behaviour intention performance and liesbased on the protocol named uniswap protocol, which helps the users to exchange the crypto-coins. Uniswap protocol is defined to be the automated liquidity protocol provision on the blockchain Ethereum platform. With the uniswap, a user can buy or sell the ERC20 tokens in the decentralized distributed network by using an Ethereum smart contract. This paper will help the users in the blockchain network to useuniswap protocol as a trustworthy and efficient way of exchanging the crypto-coins or the tokens in the blockchain network.

Swain et al.[13] a systematic literature review was conducted to examine the challenges associated with these technologies, along-with the suggested solutions to mitigate them or lessen them.

Zhou et al.[14] propose a visual analysis approach to support their daily work. The approach consists of a new algorithm that automatically detects suspicious money laundering accounts and a multiviewed user interface that visualizes the algorithm results and relevant transaction data. An abacus-inspired visualization is designed in the interface to depict transaction patterns contained in numerous cryptocurrency transactions, which can help supervisors find money laundering clues and deduce the trading tactic adopted by launderers. Finally, an algorithm performance experiment, a case study, and a field study are conducted with real-world data to demonstrate the effectiveness of our solution.

Wahrstatter et al.[15] introduce a novel set of features that we use to identify potential criminal activity more accurately. Furthermore, we apply our clustering algorithm to a CoinJoin-adjusted variant of the Bitcoin user graph, which enables us to analyze the network at a more detailed, user-centric level while still offering opportunities to address advanced privacy-enhancing techniques at a later stage. By comparing the results with our ground truth data set, we find that our improved clustering method is able to capture significantly more illicit activity within the most suspicious clusters. Finally, we find that users associated with illegal activities commonly have significant short paths to CoinJoin wallets and show tendencies toward outlier behavior. Our results have potential contributions to anti-money laundering efforts and combating the financing of terrorism and other illegal activities.

III. Payment Networks and Money Laundering

Payment channel networks [13] have been proposed as a workaround to the Bitcoin scalability problem (maximum ten transactions/second), where multiple payments are routed over a single payment channel, and blockchain writes are done only when the channel is closed, or if there is a dispute between the (usually two) parties using the channel for transactions. When two parties open a payment channel, they need to write the current channel balance to the blockchain, and if applicable, the current state of the channel's variables. Beyond that, all updates are done between the parties and are not written to the channel, unless either of the parties behaves maliciously. To facilitate transactions between two parties that may not have a payment channel currently open between them, networks of payment channels have been proposed [14], where two unconnected users can route payments between them, if there exists a path comprising of several connected users between them, e.g., Alice can route payments to Bob if there exists a path Alice → Charlie → Denise → Bob. Having a path of users also helps Alice and Bob avoid opening a private ledger channel between them (a private ledger channel is defined as a payment channel that exists only between two parties and it maintains a record of all their transactions), and thus incurring expensive blockchain write fees. This can be advantageous, especially in situations where Alice and Bob transact very infrequently.

Conceptually, a payment network can be modeled as a directed graph where users represent vertices, weighted edges represent link balances, and the directionality of the edge represents the direction of the payment flow. A user can route payments to another user over a path in the network that has sufficient balances on its links. Once a payment gets routed from a sender to a receiver, all edges along the path will get decremented by the transmitted amount. One of the advantages of payment networks is that users can perform global, cross-currency transactions in seconds, as opposed to days for traditional bank wire transfers, besides the transaction fees being a fraction of what a bank might charge.

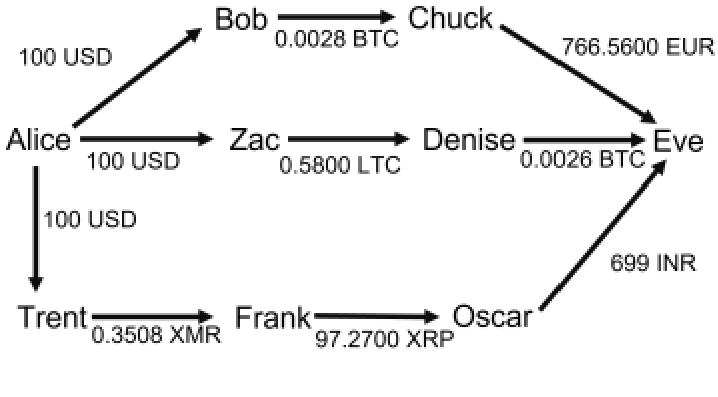

Figure 1: Payment network

In the real-world, the largest payment network by market capitalization, Ripple, has been fined USD 700,000 by U.S. regulators, partly for failing to implement a credible AML program in place to curb financial crimes. Although Ripple has since then pledged to implement stringent AML procedures, payment networks designs proposed in the literature would benefit from proactively building AML controls into their system design and adversary models. Based on the characteristics of payment networks described so far, we now outline a few challenges for implementing stringent and effective AML measures.

IV. Challenges in Preventing Money Laundering in Payment Networks

Transactions in payment networks are split into multiple fragments and spread among different users in a process called structuring [15]. Implementing AML guidelines becomes difficult since the fragmented amounts could be converted into multiple currencies across various geographical locations and we need to take into account the conversion history of all coins. Apart from this, most payment networks offer anonymity by making it hard to link the sender/receiver with the coins being transferred. This would make it hard to identify a coin as originating from illegal sources.

Payment channel networks post the final balances to the blockchain and not every individual transaction. How would we track individual transaction amounts between the sender and receiver, e.g., if one coin involved in a particular transaction is reported as illegally obtained?

Most of the payment networks have their transaction limits well within the threshold of the U.S. and global regulatory authorities [16] which makes them exempt from following AML guidelines. A user can easily split a large amount into smaller amounts within the thresholds. While the tactic of structuring the money with an intent of laundering it is illegal there is no mechanism to check whether the money is being structured or not. Payment networks only check if a given transaction is within their threshold or not.

In blacklisting, the transactions of the users involved in a crime are blacklisted and their coins are tainted. However, if we have a malicious user whose sole purpose is to taint the coins of a dense network of users, he will use his coins to initiate multiple transfers. The coins then travel along the network, tainting the coins of all the honest users in the path. This tainting of coins happens in some magnitude, no matter which policy is used for blacklisting. Hence the net value of the coins lost is more than the coins invested by the illicit user. Preventing this is a challenge.

V. Anti Money Laundering Regulatory Guidelines

In the U.S, financial crimes, including money laundering are regulated by the Bank Secrecy Act , the relatively newer Money Laundering Control Act , and the U.S.A. Patriot Act. The Financial Crimes Enforcement Network (FinCEN), within the U.S. Dept. of Treasury, is the agency responsible for enforcing the regulations. Other organizations such as Financial Industry Regulation Authority (FINRA), which operates under the Securities and Exchange Commission too have come up similar guidelines to prevent money laundering. The Financial Action Task Force (FATF) is a global, inter-government body that develops policies to prevent money laundering and curb terrorist financing, to which end it has put forward a set of similar guidelines that member countries must follow. We now briefly cover some of the FinCEN's and FATF's significant recommendations and then point out challenges in their correct interpretation and enforcement.

VI. Conclusion

In this paper we have outlined several practical challenges with implementing and enforcing AML mechanisms in cryptocurrencies and payment networks. Of the enormous research in the past few years that has been done on building systems that support and enable blockchain-enabled financial applications such as mixers and payment networks, to name two, there are hardly any systems that have AML mechanisms as part of their stated design goals. Retrofitting existing systems with something as fundamental as AML mechanisms and regulatory compliance is not easy, and goes against established principles of not adding security as an afterthought. In this paper, we have discussed the main aspects of current U.S. and FATF AML guidelines; analyzing the AML guidelines of other countries might be an interesting direction for future work.

References

[1] D. Vassallo, V. Vella, and J. Ellul, "Application of Gradient Boosting Algorithms for Anti - money Laundering in Cryptocurrencies," *SN Comput. Sci.*, vol. 2, no. 3, pp. 1–15, 2021, doi: 10.1007/s42979-021-00558-z.

[2] K. Kolachala, E. Simsek, M. Ababneh, and R. Vishwanathan, "SoK: Money Laundering in Cryptocurrencies," *ACM Int. Conf. Proceeding Ser.*, 2021, doi: 10.1145/3465481.3465774.

[3] FATF, "Opportunities and Challenges of New Technologies for AML/CFT," no. July, p. 72, 2021.

[4] Z. Shahbazi and Y.-C. Byun, "Machine Learning-Based Analysis of Cryptocurrency Market Financial Risk Management," *IEEE Access*, vol. 10, pp. 37848–37856, 2022, doi: 10.1109/ACCESS.2022.3162858.

[5] J. Wu, J. Liu, W. Chen, H. Huang, Z. Zheng, and Y. Zhang, "Detecting Mixing Services via Mining Bitcoin Transaction Network With Hybrid Motifs," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 52, no. 4, pp. 2237–2249, 2022, doi: 10.1109/TSMC.2021.3049278.

[6] N. Pocher and A. Veneris, "Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 2, pp. 1776–1788, 2022, doi: 10.1109/TNSM.2021.3136984.

[7] M.-Y. Day, P.-T. Chiu, Y.-W. Teng, and C.-L. Liu, “Developing Relation Types of Cryptocurrency Anti-Money Laundering Knowledge Graph,” in *2022 IEEE 23rd International Conference on Information Reuse and Integration for Data Science (IRI)*, 2022, pp. 90–94. doi: 10.1109/IRI54793.2022.00031.

[8] S. Mabunda, “Cryptocurrency: The New Face of Cyber Money Laundering,” in *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*, 2018, pp. 1–6. doi: 10.1109/ICABCD.2018.8465467.

[9] H. Baek, J. Oh, C. Y. Kim, and K. Lee, “A Model for Detecting Cryptocurrency Transactions with Discernible Purpose,” in *2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN)*, 2019, pp. 713–717. doi: 10.1109/ICUFN.2019.8806126.

a. A. Badawi and Q. A. Al-Haija, “Detection of money laundering in bitcoin transactions,” in *4th Smart Cities Symposium (SCS 2021)*, 2021, vol. 2021, pp. 458–464. doi: 10.1049/icp.2022.0387.

[10] J. Crawford and Y. Guan, “Knowing your Bitcoin Customer: Money Laundering in the Bitcoin Economy,” in *2020 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE)*, 2020, pp. 38–45. doi: 10.1109/SADFE51007.2020.00013.

[11] P. Shamili and B. Muruganantham, “Blockchain based Application: Decentralized Financial Technologies for Exchanging Crypto Currency,” in *2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, 2022, pp. 1–9. doi: 10.1109/ACCAI53970.2022.9752485.

[12] S. Swain and S. Gochhait, “ABCD technology- AI, Blockchain, Cloud computing and Data security in Islamic banking sector,” in *2022 International Conference on Sustainable Islamic Business and Finance (SIBF)*, 2022, pp. 58–62. doi: 10.1109/SIBF56821.2022.9939683.

[13] F. Zhou *et al.*, “Visual Analysis of Money Laundering in Cryptocurrency Exchange,” *IEEE Trans. Comput. Soc. Syst.*, pp. 1–15, 2022, doi: 10.1109/TCSS.2022.3231687.

[14] A. Wahrstätter, J. Gomes, S. Khan, and D. Svetinovic, “Improving Cryptocurrency Crime Detection: CoinJoin Community Detection Approach,” *IEEE Trans. Dependable Secur. Comput.*, pp. 1–11, 2023, doi: 10.1109/TDSC.2023.3238412.