



The Role of Trading Bots in Smart Money Laundering by White-Collar Criminals

Article Info

ABSTRACT

Article type: (Times New Roman 9 Bold)
Research Article
(Times New Roman 9)

Article history:

Received
Received in revised form
Accepted
Available online
(Times New Roman 9)

Keywords:

Smart money laundering,
Artificial intelligence,
Cryptocurrency, Trading bot,
White-collar criminals, Anti-money laundering regulations

Smart money laundering has emerged as one of the major challenges facing financial systems in the digital age, as it has transformed traditional methods of concealing the proceeds of crime through the use of advanced technologies. In this context, white-collar criminals, by employing tools such as trading bots, artificial intelligence-based systems, and cryptocurrencies, are able to design complex processes for the transfer, layering, and integration of illicit funds in ways that make it difficult for regulatory authorities to identify the true origin of such assets.

This study, conducted through a descriptive-analytical method, aims to examine the role of emerging technologies in facilitating smart money laundering by white-collar offenders and to analyze the legal challenges arising therefrom. The findings indicate that the use of algorithmic trading, the execution of a high volume of micro-transactions, and the exploitation of cryptocurrency platforms can significantly complicate the tracing of financial flows, while many supervisory mechanisms and anti-money laundering regulations still remain grounded in traditional models of financial oversight.

The results further demonstrate that effective confrontation with smart money laundering requires the modernization of legal frameworks, the strengthening of crime-detection methods based on financial data analysis, and the development of regulatory cooperation at both national and international levels. Moreover, attention to preventive approaches, including the regulation of cryptocurrency exchange activities, the enhancement of transparency in financial transactions, and the application of technologies such as machine learning within supervisory systems, can play a significant role in reducing the abuse of emerging technological capacities by criminals.

Cite this article:



© The Author. Publisher: Razavi University of Islamic Sciences

پولشویی هوشمند به عنوان یکی از چالش های مهم نظام های مالی در عصر دیجیتال مطرح است که با بهره گیری از فناوری های نوین، شیوه های سنتی پنهان سازی عواید حاصل از جرم را دگرگون ساخته است. در این میان، مجرمان یقه طلایی با استفاده از ابزارهایی مانند ربات های معامله گر، سامانه های مبتنی بر هوش مصنوعی و ارزهای دیجیتال، قادرند فرآیندهای پیچیده ای از انتقال، لایه بندی و یکپارچه سازی وجوه غیرقانونی را طراحی کنند، به گونه ای که شناسایی متشاء واقعی این وجوه برای نهادهای نظارتی دشوار می شود. این پژوهش با هدف بررسی نقش فناوری های نوین در تسهیل پولشویی هوشمند توسط مجرمان یقه طلایی و تحلیل چالش های حقوقی ناشی از آن، به روش توصیفی _ تحلیلی انجام شده است. یافته های تحقیق نشان می دهد که استفاده از معاملات الگوریتمی، انجام حجم گسترده ای از تراکنش های خرد و بهره گیری از بسترهای رمزارزی می تواند فرآیند ردیابی جریان های مالی را پیچیده تر سازد، در حالی که بسیاری از سازوکارهای نظارتی و مقررات ضد پولشویی همچنان بر الگوهای سنتی نظارت مالی استوار هستند. همچنین نتایج پژوهش بیانگر آن است که مقابله مؤثر با پولشویی هوشمند مستلزم به روزرسانی چارچوب های قانونی، تقویت روش های کشف جرم مبتنی بر تحلیل داده های مالی و توسعه همکاری های نظارتی در سطح ملی و بین المللی است. همچنین توجه به رویکردهای پیشگیرانه، از جمله تنظیم گری فعالیت صرافی های رمزارزی، ارتقای شفافیت تراکنش های مالی و بهره گیری از فناوری هایی مانند یادگیری ماشین در نظام های نظارتی، می تواند در کاهش سوءاستفاده مجرمان از ظرفیت های فناوری های نوین نقش مؤثری ایفا کند.

کلیدواژه ها:

پولشویی هوشمند، هوش مصنوعی، ارز دیجیتال، ربات معامله گر، مجرمان یقه طلایی، مقررات ضد پولشویی.

استناد:

ناشر: دانشگاه علوم اسلامی رضوی. ©نویسنده.



مقدمه

پولشویی^۱ پدیده‌ای فراملی و پیچیده است که آثار آن در سطح ملی و بین‌المللی آشکار می‌شود. گروه ویژه اقدام مالی^۲ پولشویی را فرایندی می‌داند که طی آن عواید حاصل از جرم پردازش می‌شود تا منشاء غیرقانونی آن پنهان بماند و در ظاهر، مشروع جلوه کند.^۳ برآوردهای دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد نشان می‌دهد که سالانه بین ۲ تا ۵ درصد از تولید ناخالص داخلی جهان، معادل حدود ۸۰۰ میلیارد تا ۲ تریلیون دلار، از این طریق تطهیر می‌شود.^۴

با گسترش فناوری‌های مالی و تحول در زیرساخت‌های معاملاتی، شیوه‌های پولشویی نیز از الگوهای سنتی فاصله گرفته و به سمت روش‌های پیچیده‌تر حرکت کرده‌اند. استفاده از ساختارهای تجاری چندلایه، معاملات فرامرزی، فناوری‌های دفترکل توزیع‌شده، سامانه‌های معاملاتی خودکار و الگوریتم‌های هوشمند، شناسایی و رهگیری جریان‌های مشکوک را دشوارتر کرده است. در این میان، پیوند پولشویی با سایر حوزه‌های مجرمانه، از جمله امنیت و تأمین مالی تروریسم، بر اهمیت مقابله با این پدیده افزوده است.

عواید حاصل از فعالیت‌های غیرقانونی معمولاً از طریق بهره‌گیری از سازوکارهای ظاهراً مشروع، مانند ساختارهای پیچیده تجاری یا معاملات فرامرزی، وارد چرخه اقتصاد رسمی می‌شوند تا منشاء غیرقانونی آن‌ها پنهان مانده و ظاهری قانونی پیدا کنند. از این رو، پولشویی به یکی از چالش‌های مهم و پیچیده در مسیر توسعه تجارت و نظم اقتصادی در سطح جهانی تبدیل شده است. افزون بر این، این پدیده ارتباطی نزدیک با مسائل امنیتی و همچنین تأمین مالی تروریسم دارد. (Bergström, 2024: 178)

در این میان، گسترش و نفوذ فناوری‌های نوین در عرصه‌های مالی، ابعاد تازه‌ای به فرایندهای پولشویی بخشیده است. پیوند روزافزون فعالیت‌های اقتصادی با فناوری‌های پیشرفته موجب شده است متغیرهای پنهان و سازوکارهای پیچیده‌تری در فرایند پولشویی وارد شود و در نتیجه شناسایی و رهگیری آن با دشواری بیشتری همراه گردد. به‌ویژه، تراکنش‌ها و مبادلاتی که در بستر فناوری‌های دفترکل توزیع‌شده^۵ انجام می‌شوند و در بسیاری موارد از نظارت و تنظیم‌گری کامل برخوردار نیستند، به‌عنوان تهدیدی بالقوه برای جامعه مطرح شده‌اند، چراکه این بسترها می‌توانند برای اهدافی نظیر پولشویی، تأمین مالی تروریسم و فرار مالیاتی مورد سوءاستفاده قرار گیرند.

۱. یکی از خصوصیات جرم پولشویی، علیرغم اینکه یک جرم کاملاً مستقل محسوب می‌شود، نیاز به ارتکاب یک جرم دیگر به عنوان بخشی از رکن مادی خود است که آن جرم منشاء یا اصلی نامیده می‌شود. (رضوی فرد، ۱۳۹۸: ۱۰۸)

۲. FATF

۳. FATF (2022), International standards on combating money laundering and the financing of terrorism and proliferation, available at: www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf (accessed 15 April 2021)

۴. UNODC

۵. در توضیح باید گفت که، جریان‌های مالی غیرقانونی گسترده (IFFs) ثروت را از کشورهای با مالیات بالا و کشورهای نوظهور به حوزه‌های قضایی با مالیات پایین تر منتقل می‌کنند که در نتیجه توسعه بلندمدت اقتصاد جهانی را تهدید می‌کند بنگرید:

Contractor, F.J. (2016), Tax avoidance by multinational companies: methods, policies, and ethics, AIB Insights, Vol. 16 No. 2, pp. 10-13.

۶. Distributed Ledger Technologies

(Scholl & Bolívar, 2019: 604) استفاده از فناوری‌های نوین مانند سامانه‌های معاملاتی خودکار، الگوریتم‌های هوشمند و بسترهای دیجیتال مالی، امکان جابه‌جایی و لایه‌بندی سریع منابع مالی را فراهم کرده است. چنین تحولاتی سبب شده است که پدیده پولشویی از قالب‌های سنتی فاصله گرفته و به سمت اشکال پیچیده‌تر و فناورانه حرکت کند، امری که چالش‌های تازه‌ای را برای نظام‌های حقوقی و نهادهای مبارزه با پولشویی ایجاد کرده است.

در سال‌های اخیر، روند دیجیتالی‌شدن تأثیر چشمگیری بر صنعت مالی در سراسر جهان گذاشته است. هرچند بانکداری دیجیتال فرصت‌ها و مزایای متعددی را برای بانک‌ها و مشتریان فراهم کرده است، اما هم‌زمان ظهور و گسترش فناوری‌های نوآورانه توجه و بهره‌برداری سازمان‌های مجرمانه را نیز به همراه داشته است. این گروه‌ها با استفاده از بسترهای دیجیتال تلاش می‌کنند عواید حاصل از فعالیت‌های غیرقانونی را در محیط‌های مالی جدید تطهیر کنند؛ پدیده‌ای که از آن با عنوان «پولشویی دیجیتال» یاد می‌شود. (1: Tiemann, 2025) البته ظهور اینترنت و فناوری‌های دیجیتال مزایای و راحتی زیادی را برای زندگی مردم به ارمغان آورده است، از خرید آنلاین گرفته تا رسانه‌های اجتماعی. با این حال، درها را به روی نوع جدیدی از فعالیت‌های مجرمانه به نام سایبری شویی^۱ (پولشویی سایبری) نیز باز کرده است.

میان پولشویی دیجیتال و پولشویی سایبری تفاوتی اساسی وجود دارد. در پولشویی سایبری معمولاً از ابزارها و روش‌هایی نظیر بیت‌کوین و سایر رمزارزها، کارت‌های اعتباری سرقتی، حساب‌های بانکی جعلی، فیشینگ و انواع بدافزارها برای انتقال و پنهان‌سازی عواید نامشروع استفاده می‌شود. در مقابل، مفهوم پولشویی دیجیتال دامنه‌ای گسترده‌تر دارد و تمامی شیوه‌های پولشویی را در بر می‌گیرد که به‌نوعی از فناوری‌های دیجیتال و بسترهای نوین مالی بهره می‌برند.^۲ (Ilker & Aydos, 2020: 764-766) اما با ظهور هوش مصنوعی و ربات‌های معامله‌گر ما با شکل دیگری از پولشویی مواجه هستیم که به پولشویی هوشمند موسوم است. با توجه به ساختار این جرائم مجرمان عادی اساساً قادر به ارتکاب آن نمی‌باشند. لذا نقش مجرمان یقه رنگی خصوصاً مجرمان یقه طلایی^۳ که مورد توجه این پژوهش است بسیار پررنگ می‌گردد.

اگرچه ممکن است در وهله اول شباهت زیادی میان مجرمان یقه سفید^۴ و یقه طلایی وجود دارد، زیرا جرائم متداول یقه سفید نیز شامل کلاهبرداری، اختلاس، پولشویی، تجارت داخلی و فرار مالیاتی است. با این حال چند

1. Cyber-laundering

۲. علاوه بر رمزارزها و فضای سایبری، شامل تجارت الکترونیکی، پرداخت‌های دیجیتال و NFTها نیز می‌شود.

3. Gold-collar criminals

۴. مجرمان یقه سفید (White-collar crime) اصطلاحی است که توسط ادوین ساترلند در سال ۱۹۳۹ برای توصیف مجرمانی که در سازمان‌ها، شرکت‌ها و مشاغل حرفه‌ای مرتکب جرم می‌شوند، معرفی شد.

تفاوت مهم^۱ موجب تمایز آنها از هم می گردد. جرایم ارتكابی یقه سفیدها^۲ به مناسبت انجام حرفه خود دارای ماهیت نیرنگ آمیز است. (نجفی ابرندآبادی، ۱۴۰۳: ۱۶) بر این مبناء جرم پولشویی از یک سو، در شکل جدید آن در حال گسترش است و از سوی دیگر نبود خلاء مقررات مرتبط و مکانیزم های مقابله ای مشروع امکان شناسایی دقیق و پیگرد آن را با چالش جدی مواجه می کند. لذا در این پژوهش بدنبال پاسخ به این سوال هستیم که ربات های معامله گر چه نقشی در ارتكاب جرم پولشویی هوشمند توسط مجرمان یقه طلایی دارند؟

۱. نقش ربات های معامله گر و هوش مصنوعی در پولشویی هوشمند

مجرمان یقه طلایی به افرادی اطلاق می شود که در بالاترین سطوح قدرت اقتصادی یا سازمانی قرار دارند و جرائم خود را عمدتاً در بسترهای اقتصادی و ساختارهای سازمانی، به ویژه در محیط های تجاری و گاه دولتی، ارتكاب می دهند. این دسته از جرائم معمولاً شامل مصادیقی همچون فساد مالی، پولشویی، اختلاس، تقلب مالیاتی و کلاهبرداری های کلان است. (Brants, 2007: 309) مجرمان یقه طلایی معمولاً برای ارتكاب جرائم مالی از شیوه هایی پیچیده و پیشرفته بهره می گیرند که اغلب در قالب سازوکارهای ظاهراً قانونی و با پوششی مشروع انجام می شود. بخش قابل توجهی از جرائم مالی ارتكابی توسط این گروه با فناوری های نوین پیوند خورده و مصادیقی همچون پولشویی دیجیتال، فرار مالیاتی، اختلاس و کلاهبرداری های رایانه ای را در بر می گیرد. افزون بر این، رشد سریع فناوری و به کارگیری شتاب زده آن در حوزه های مالی، زمینه ها و انگیزه های بهره برداری مجرمانه از این ابزارها را افزایش داده است؛ امری که با توجه به خلأهای قانونی و نظارتی موجود در این حوزه، چالش های بیشتری را نیز به همراه دارد. (Zakaria, 2023: 123)

واقعیت آن است که حرفه ای ترین مجرمان اغلب در حاشیه دید نهادهای نظارتی باقی می مانند و نه تحت تعقیب مستقیم پلیس قرار دارند و نه دستگاه قضایی لزوماً از فعالیت های آنان آگاه است. در بسیاری از موارد، حتی اصل مشارکت آنان در رفتارهای مجرمانه نیز ناشناخته می ماند، زیرا فعالیت هایشان به گونه ای طراحی شده است که از منظر عمومی و نظارتی پنهان بماند. شناسایی این دسته از مجرمان از دشوارترین مراحل فرآیند کشف جرم به شمار می رود، چراکه شبکه ارتباطی آنان در پشت لایه های متعدد امنیتی اعم از فنی و فیزیکی مستتر شده است. آنان نه تنها نقش مستقیم خود در ارتكاب جرم را پنهان می کنند، بلکه روابط، سازوکارها و پیوندهایی را که بستر وقوع جرم را فراهم می سازد نیز از دید نهادهای نظارتی مخفی نگه می دارند. (Marriott, 2016: 239-241) در واقع، در اینجا با جرائمی مواجه هستیم که از سوی نخبگان اقتصادی و سیاسی ارتكاب می یابد؛ امری که با تصور

۱. مجرمان یقه سفید معمولاً افراد حرفه ای، کارمندان، مدیران میانی یا افرادی با تخصص مالی و حقوقی هستند که از دانش و موقعیت شغلی خود برای ارتكاب جرایم اقتصادی مانند اختلاس، کلاهبرداری یا پولشویی استفاده می کنند. در مقابل، مجرمان یقه طلایی در سطوح بالای ساختار قدرت و تصمیم گیری قرار دارند؛ مانند مدیران ارشد، مقامات بانکی، مسئولان حاکمیتی یا مالکان شرکت های بزرگ.

۲. مجرمان یقه سفید مبتنی بر نیرنگ و فریب هستند؛ مرتکبان این جرایم با برخورداری از خصیصه هایی همچون بهره هوشی بالا، موقعیت سنجی و توان تطبیق پذیری با محیط کاری می توانند اقدامات فریبکارانه خود را با زیرکی در مدت مدیدی پنهان نمایند. (دارابی، ۱۳۹۷: ۱۳۴)

رایج در افکار عمومی، مبنی بر اینکه مجرمان عمدتاً افرادی کم‌سواد یا فاقد جایگاه اجتماعی هستند، تفاوتی آشکار دارد. حقیقت آن است که با گسترش فناوری، گونه‌ای از مجرمان ظهور و بروز بیشتری یافته‌اند که نه تنها از سطح تحصیلات و موقعیت اجتماعی بالاتری برخوردارند، بلکه آشنایی قابل توجهی نیز با فناوری‌های نوین دارند و از این ظرفیت‌ها برای انتخاب و به‌کارگیری شیوه‌های تازه در ارتکاب جرائم مالی استفاده می‌کنند. (Otusanya, 2012: 175) در واقع مجرمان همیشه به دنبال راه جدیدی برای ارتکاب جرم هستند و سیستم پولشویی هر روز تغییر می‌کند لذا کشورها باید به طور منظم، سیاست‌ها و عملیات ضد پولشویی خود را به روز کنند. بنابراین شناسایی دلایل و عوامل وقوع پولشویی جهت جلوگیری از آن با اهمیت می‌باشد. (پیوندی و گل ارضی، ۱۴۰۳: ۸۷) از همین رو، مجرمان و پیشروان جرم پولشویی از بستر بانکداری الکترونیک به شیوه‌های گوناگون برای مشروع نشان دادن پول‌های کثیف خود استفاده می‌کنند. (شاکری بهبهانی، ۱۳۹۸: ۱) پول‌شویی به‌عنوان پدیده‌ای جهانی و جرمی با ماهیت فرامرزی، همواره با اشکال مختلف جرائم سازمان‌یافته از جمله تروریسم، قاچاق انسان و قاچاق مواد مخدر ارتباط داشته است. این پدیده آثار زیان‌باری بر ساختارهای اقتصادی برجای می‌گذارد، زیرا زمینه گسترش تجارت‌های غیرقانونی و فعالیت‌های پنهان را فراهم می‌کند. از جمله پیامدهای آن می‌توان به تقویت فرار مالیاتی، قاچاق مواد مخدر، فساد، قاچاق انسان و سایر اشکال جرائم سازمان‌یافته اشاره کرد. (Hendriyetty & Grewal, 2017: 68-70) از سوی دیگر، محدودیت تعداد کارشناسان خبره، کندی سیستم‌ها، تراکم پاسخ‌های مثبت کاذب فراوان در هر روز، فرسایشی و پیچیده بودن عملیات شناسایی رفتار مشتریان مظنون به پول‌شویی و طولانی بودن تهیه گزارشات مربوط به این اشخاص و ارسال آن به مقامات ذیربط، ضرورت استفاده از تکنیک‌های جایگزین مانند الگوریتم‌های هوشمند را نمایان می‌سازد. (ارجمند نژاد، حبیبی و بابائی کیایی، ۱۴۰۳: ۲) از همین رو، یکی از شیوه‌هایی که همواره در پولشویی مورد استفاده قرار می‌گیرد، تجارت کردن است و در گذشته به شیوه‌های سنتی و امروزه به صورت هوشمند انجام می‌پذیرد. در حقیقت برای اینکه پولشویی هوشمند را بهتر بشناسیم ابتدا باید «تجارت هوشمند» را به درستی درک کنیم.

تجارت هوشمند در بستر پولشویی به بهره‌گیری از فناوری‌های پیشرفته، از جمله هوش مصنوعی و الگوریتم‌های یادگیری ماشین، برای پنهان‌سازی و جابه‌جایی عواید حاصل از فعالیت‌های غیرقانونی در نظام‌های مالی دیجیتال اشاره دارد. در این شیوه، مجرمان سایبری با استفاده از ابزارهای تحلیلی پیشرفته اقدام به انجام معاملات خودکار، شناسایی الگوهای کم‌ریسک برای انتقال وجوه و دور زدن سازوکارهای نظارتی می‌کنند. به‌کارگیری این فناوری‌ها از طریق ایجاد زنجیره‌ای از معاملات متعدد و پیچیده می‌تواند منشاء واقعی سرمایه را پنهان سازد و در نتیجه، ردیابی جریان‌های مالی مشکوک را برای نهادهای نظارتی با دشواری بیشتری مواجه کند. (Isolauri & Ameer, 2022: 427) در توصیف هوش مصنوعی باید گفت که توانایی یک ماشین برای عملکردهای شناختی مرتبط با ذهن انسان است و حل مساله، استدلال و ادراک همگی اهداف هوش مصنوعی هستند. (خرازی، ۱۴۰۴: ۱۴۰۴)

۴) در این راستا نقش ربات های معامله گر بسیار حائز اهمیت می باشد زیرا ربات های معامله گر در تجارت هوشمند نقش کلیدی در اجرای سریع و خود کار معاملات مالی دارند. در زمینه پولشویی، از این ربات ها برای انجام معاملات متعدد، خرد کردن مبالغ کلان به تراکنش های کوچک ترو تغییر مسیر سرمایه ها به شیوه ای استفاده می شود که نهادهای نظارتی قادر به شناسایی منشأ غیرقانونی آن نباشند.

همچنین با بهره گیری از هوش مصنوعی، موسسات مالی می توانند:

۱) الگوهای پیچیده پولشویی و فعالیت های مشکوکی را که شناسایی آنها برای سیستم های سنتی مبتنی بر قانون ممکن بود چالش برانگیز باشد، شناسایی کنند.

۲) تجزیه و تحلیل حجم عظیمی از داده ها به صورت بلادرنگ برای شناسایی ناهنجاری ها جهت بررسی بیشتر، بهبود دقت و کارایی در تشخیص و جلوگیری از فعالیت های مشکوک.

۳) خود کارسازی فرآیند نظارت بر تراکنش ها و بررسی دقیق مشتری، کاهش نیاز به مداخله دستی و بهبود کارایی در صنعت.

۴) با بهره گیری از قدرت هوش مصنوعی، متخصصان مبارزه با پولشویی می توانند توانایی خود را در شناسایی فعالیت های بالقوه پولشویی افزایش داده و ریسک را به طور موثرتری کاهش دهند. (حاجی زاده فلاح، ۱۴۰۴)^۱



شکل ۱: مراحل شکل گیری چرخه پول شویی و تمیز نمودن پول کثیف

(علیمرادی دوکوهی و نوروزی، ۱۴۰۳: ۴۹)

با این توصیف به نظر می رسد اهمیت این تحول تنها در سرعت و سهولت انجام تراکنش ها نیست، بلکه در کاهش قابلیت ردیابی و افزایش پیچیدگی الگوهای مالی نیز نهفته است. مجرمان یقه طلایی که معمولاً در سطوح بالای ساختارهای مالی و اقتصادی فعالیت دارند، با استفاده از دانش تخصصی و دسترسی به ابزارهای مالی پیشرفته،

می‌توانند از ربات‌های معامله‌گر برای انجام حجم بالایی از معاملات سریع و پیچیده در بازارهای مالی برای پولشویی استفاده کنند. بنابراین، مسئله اصلی نه خود فناوری، بلکه نحوه استفاده مجرمانه از آن در چارچوب خلأهای نظارتی و ضعف‌های قانونی است.

۱-۱. پولشویی هوشمند و تفاوت آن با روش‌های سنتی

بر اساس کنوانسیون‌های سازمان ملل متحد، پول‌شویی به فرایند تبدیل یا انتقال دارایی‌های حاصل از فعالیت‌های غیرقانونی اطلاق می‌شود که با هدف پنهان‌سازی منشأ نامشروع آن‌ها یا کمک به مرتکبان جرم برای بهره‌برداری از عواید حاصل از جرم صورت می‌گیرد.^۱ این فرایند معمولاً در پی ارتکاب سایر فعالیت‌های مجرمانه شکل می‌گیرد؛ از جمله قاچاق مواد مخدر، سرقت، قاچاق کالا، فرار مالیاتی، تروریسم، قاچاق مشروبات الکلی، سرقت آثار هنری، سرقت وسایل نقلیه و کلاهبرداری (Bichler, Malm & Cooper, 2017: 2) واقعیت آن است که رفتارهای مجرمانه مانند قاچاق، اختلاس و کلاهبرداری مالیاتی ممکن است بسیار سودآور باشند اما قبل از اینکه وجوه غیرقانونی به دست آمده آزادانه خرج شوند، باید مشروع به نظر برسند که این امر از طریق پولشویی انجام می‌پذیرد و با رشد فناوری شاهد اشکال نوینی از پولشویی هستیم.

در ماهیت، پولشویی به معنای پنهان‌سازی منشأ غیرقانونی عواید حاصل از فعالیت‌های مجرمانه است. برای مشروع جلوه دادن این وجوه، شیوه‌ها و سازوکارهای متعددی به کار گرفته می‌شود که یکی از مهم‌ترین آنها بهره‌گیری از بستر تجارت بین‌المللی است. در این چارچوب، «پولشویی مبتنی بر تجارت» به فرایندی اطلاق می‌شود که طی آن عواید حاصل از جرم از طریق انتقال ارزش در معاملات تجاری پنهان می‌شود و منشأ غیرقانونی آن‌ها ظاهری مشروع می‌یابد. این امر غالباً از طریق ارائه نادرست اطلاعات مربوط به قیمت، مقدار یا کیفیت کالاهای وارداتی و صادراتی صورت می‌گیرد. (Buchanan, 2004: 115-117)

گروه ویژه اقدام مالی نیز در گزارش‌های خود در سال‌های ۲۰۰۶^۲ و ۲۰۰۸^۳ توجه ویژه‌ای به این شیوه از پول‌شویی معطوف کرده است.^۴ در این روش، ممکن است از سازوکارهای قانونی تجارت بین‌المللی برای انتقال ارزش و جابه‌جایی وجوه استفاده شود؛ به گونه‌ای که از طریق صدور صورت‌حساب‌هایی با قیمتی بالاتر

1. UNODC, "United Nations Convention Against Transnational Organized Crime and the Protocols Thereto," United Nations, Vienna, 2004.

2. Trade-based money laundering (TBML)

3. Financial Action Task Force (2006), Trade-based Money Laundering, Financial Action Task Force, OECD, available at: <https://www.fatf-gafi.org/media/fatf/documents>

4. Financial Action Task Force (2008), Best Practices Paper on Trade Based Money Laundering, OECD, available at: <http://www.fatf-gafi.org/>

۵. مشخص نیست اولین بار چه زمانی اصطلاح "TBML" ابداع شد اما آن را به تحقیقات انجام شده بین دهه ۱۹۶۰ و ۱۹۸۰ نسبت می‌دهد، زمانی که الگوهای قیمت‌گذاری غیرعادی تجارت بین‌المللی باعث ایجاد سوء ظن مبنی بر انتقال غیرقانونی پول از طریق مرزها شد. بنگرید:

Zdanowicz, J.S. (2009), "Trade-based money laundering and terrorist financing", Review of Law and Economics, Vol. 5 No. 2, pp. 855-878, doi: 10.2202/1555-5879.1419.

یا پایین‌تر از ارزش واقعی بازار، ارسال بیش از مقدار واقعی یا کمتر از مقدار اعلام‌شده کالاها و خدمات، یا ارائه توصیف نادرست از کیفیت کالا و خدمات، ارزش مالی جابه‌جا گردد. در حوزه خدمات نیز، به دلیل دشواری در اندازه‌گیری دقیق ارزش خدمات و نبود قیمت‌های ثابت، امکان سوءاستفاده بیشتری وجود دارد، به‌طوری که یک خدمت ممکن است حتی چندین بار صورت‌حساب شود. از این رو، هدف نهایی این نوع از پولشویی، ادغام و وارد کردن عواید غیرقانونی در چرخه اقتصاد رسمی و جهانی است. (Buchanan, 787-789: 2014) تحلیل تاریخی اسناد بین‌المللی نشان می‌دهد که بحث بار اثبات دلیل در جرایم، از ماده ۹ اساسنامه دیوان نورنبرگ (۱۹۴۵) آغاز شد و در اسناد بعدی همچون کنوانسیون وین (۱۹۸۸)، کنوانسیون پالرمو و کنوانسیون مبارزه با فساد مالی سازمان ملل (۲۰۰۳) توسعه یافت. کنوانسیون وین با تمرکز بر جرم‌انگاری پولشویی، ضمن تأکید بر لزوم احراز علم مرتکب، بار اثبات را در برخی موارد معکوس کرده و دولت‌ها را توصیه می‌کند ترتیباتی در قوانین داخلی خود فراهم آورند تا منشأ اموال مشکوک مشخص گردد. این توصیه‌ها جنبه الزام‌آور ندارد و اجرای آن به اختیار کشورها گذاشته شده است.^۱ (رشیدی، شاملو و سایانی، ۱۳۹۹: ۳۳۸-۳۳۷) جرم پولشویی اگرچه نوعی از جرایم ثانویه می‌باشد، لکن متصف به وصفی است که آن را از این گونه جرایم متمایز می‌سازد. استقلال این جرم از جرایم اولیه، وصف خاصی است که در جرایم ثانویه دیگر موجود نبوده و همین وصف نیز جرم‌انگاری پولشویی را تبدیل به راهکاری کارآمد برای مبارزه با جرایم سازمان‌یافته می‌نماید. (زرنشان و شجاعی نصرآبادی، ۱۳۹۶: ۱۷۳)

تیواری و همکاران (۲۰۲۰) در پژوهشی به بررسی ادبیات مرتبط با پولشویی پرداخته و آن را در شش محور اصلی دسته‌بندی کرده‌اند: (۱) چارچوب‌های مقابله با پولشویی، (۲) آثار و پیامدهای اقتصادی، (۳) بازیگران کلیدی درگیر در این پدیده، (۴) گستره و ابعاد مسئله، (۵) فرصت‌ها و بسترهای نوظهور، و (۶) شیوه‌های شناسایی پولشویی. در میان این ابعاد مختلف، روش‌ها و سازوکارهایی که برای شست‌وشوی عواید حاصل از جرم به کار گرفته می‌شوند نیز به‌طور ویژه مورد توجه و بررسی قرار گرفته‌اند. (Tiwari, Gepp & Kumar, 2020: 271-276) با این حال، تفاوت اصلی پولشویی هوشمند با روش‌های سنتی تنها در استفاده از ابزارهای دیجیتال خلاصه نمی‌شود، بلکه در نحوه طراحی و اجرای فرآیندهای مالی نیز نمود پیدا می‌کند.^۲

۱. در کنوانسیون‌های پالرمو و مبارزه با فساد مالی نیز اصل بار اثبات معکوس تکرار شده، به‌گونه‌ای که کشورها می‌توانند متهم را ملزم به اثبات مشروعیت درآمدها یا اموال مورد مصادره کنند. با این حال، این قاعده محدود به جرایم مشخص شده در اسناد بین‌المللی است و نحوه و قلمرو اجرای آن در حوزه اختیارات نظام‌های حقوقی داخلی کشورها قرار دارد. بدین ترتیب، اسناد بین‌المللی ضمن تأکید بر اهمیت بار اثبات معکوس در مقابله با جرایم سازمان‌یافته و پولشویی، پیاده‌سازی آن را به شرایط و قوانین داخلی واگذار کرده‌اند.

۲. در شیوه‌های سنتی معمولاً انتقال و لایه‌بندی وجوه از طریق شبکه‌ای از حساب‌ها و اشخاص انجام می‌شد، در حالی که در پولشویی هوشمند این فرآیند می‌تواند از طریق الگوریتم‌ها و سامانه‌های معاملاتی خودکار در مدت زمان کوتاه و در حجم بالایی از تراکنش‌ها صورت گیرد و این ویژگی، تشخیص الگوهای مشکوک را برای نهادهای نظارتی پیچیده‌تر می‌کند.

اقدامات پیشگیرانه در مبارزه با پولشویی و تأمین مالی تروریسم باید متناسب با ریسک، ارزیابی و طراحی شوند. از این رو می‌بایست در حوزه‌های کم‌خطر، کنترل‌های ساده یا کاهش یافته اعمال شود و حوزه‌های دارای ریسک بالاتر مشمول روش‌های پیشرفته باشند. (جمالی حاجیانی، عبداللهی و میرزایی، ۱۴۰۳: ۲۲۹) درواقع کشورها می‌بایست ریسک‌های پولشویی و تأمین مالی تروریسم در خصوص کشور را شناسایی، ارزیابی و بررسی کنند و اقدام‌هایی مشتمل بر تأسیس یک مرجع یا ساز و کارهای جهت همکاری و اقدام‌های مرتبط با ارزیابی ریسک در پیش گیرند، همچنین آن‌ها می‌بایست منابعی جهت اطمینان یافتن در خصوص اینکه ریسک‌ها به نحو موثر کاهش یافته است بکار گیرند. (سبحانی، ۱۴۰۴: ۱۶۶) همچنین اتکای پولشویی هوشمند به فناوری‌های پیشرفته موجب شده است که مرز میان فعالیت‌های مالی مشروع و نامشروع تا حدی مبهم شود. بسیاری از ابزارهایی که در بازارهای مالی برای افزایش سرعت و کارایی معاملات طراحی شده‌اند، در صورت استفاده هدفمند توسط مجرمان می‌توانند به ابزاری برای پنهان‌سازی منشاء وجوه تبدیل شوند.

ظهور فناوری بلاکچین نیز بر پیچیدگی فرایندهای نوین پول‌شویی افزوده است. در بستر بلاکچین، پولشویی می‌تواند از طریق مراحل همچون لایه‌گذاری، ساختاردهی و در نهایت ادغام عواید غیرقانونی در نظام مالی صورت گیرد. با این حال، چارچوب‌های کنونی مبارزه با پول‌شویی در مواجهه با این شیوه‌های نوین با چالش‌هایی روبه‌رو هستند، زیرا ماهیت و سازوکارهای این نوع از پول‌شویی به‌طور کامل روشن و قابل شناسایی نیست. (Ozer & Aydos, 2025: 4)

در عمل، طیف گسترده‌ای از تکنیک‌ها برای انجام پولشویی مورد استفاده قرار می‌گیرد. با این حال، با توجه به شرایط محیطی، تحولات فناورانه و تغییرات مقرراتی، مجرمان ممکن است از روش‌های نوظهور یا ترکیبی از چندین شیوه به‌طور هم‌زمان بهره‌برند. از جمله تکنیک‌های رایج شناسایی شده در این حوزه می‌توان به انتقال الکترونیکی وجوه، بانکداری کارگزاری، ساختاربندی تراکنش‌ها، استفاده از کارینوها، سرمایه‌گذاری در املاک و مستغلات، کارت‌های پیش‌پرداخت، بانکداری آنلاین، و همچنین بهره‌گیری از شرکت‌های صوری و تراست‌ها اشاره کرد. پیچیدگی این روش‌ها بسته به شرایط و بسترهای مورد استفاده متفاوت است و به همین دلیل، همگام با پیشرفت‌های فناوری و تغییر در مقررات دولتی، شیوه‌های تازه‌ای نیز برای انجام پولشویی شکل می‌گیرد. (Gilmour, 2016: 3) در واقع، در یک سطح، بخشی از جابه‌جایی‌های بین‌المللی پول شامل جریان‌های مالی فراملی غیرقانونی و زیان‌بار است و در سطحی دیگر، جرائم سازمان‌یافته فراملی به‌عنوان نقطه آغاز و محرک فرایند پول‌شویی عمل می‌کنند. این جریان‌ها با بهره‌گیری از فناوری‌های نوین، بسیاری از شیوه‌های سنتی مقابله با پول‌شویی را دور می‌زنند و در مواردی بدون بر جای گذاشتن ردپای آشکار، به انجام اشکال هوشمند و پیچیده پول‌شویی مبادرت می‌ورزند. (Mer, Singhal & Viridi, 2024: 175-177) در حقیقت پولشویی هوشمند به دلیل استفاده از فناوری‌های پیشرفته، از جمله هوش مصنوعی و ربات‌های معامله‌گر، با چالش‌های قانونی و نظارتی روبه‌روست. بسیاری از قوانین موجود برای شناسایی پولشویی سنتی طراحی شده‌اند و قادر به ردیابی

الگوهای پیچیده و پنهان سازی پیشرفته‌ای که در پولشویی هوشمند استفاده می‌شود، نیستند. خلاء قانونی در این حوزه باعث می‌شود که مجرمان بتوانند از ضعف‌های نظارتی سوءاستفاده کرده و تراکنش‌های غیرقانونی را با استفاده از فناوری‌های نوین از دید نهادهای مالی و مقامات مسئول پنهان کنند. همچنین، عدم به‌روزرسانی کافی در سیستم‌های تشخیص تقلب و نبود استانداردهای جهانی برای کنترل این نوع فعالیت‌ها، نظارت مؤثر بر این فرآیند را دشوارتر می‌کند. البته در کنار این موارد چالش نبود تعریف دقیق از پولشویی هوشمند را نیز باید به آن اضافه کرد.

۲-۱. نقش ربات‌های هوشمند در پنهان کردن فعالیت‌های مالی غیر قانونی

دولت‌ها تنها چیزی را پول می‌دانند که به صورت رسمی توسط دولتها و از طریق بانک مرکزی آنها انتشار یافته است. (پروین و الهیاری فرد، ۱۴۰۳: ۱۵۵۷) از این رو، یک فرد یا سازمان نمی‌تواند وجوه حاصل از منابع غیرقانونی مانند قاچاق انسان، آدم‌ربایی، اخاذی، رشوه، فرار مالیاتی یا خرید و فروش مواد مخدر را به طور مستقیم به نظام بانکی وارد کند؛ زیرا بانک‌ها با استفاده از سازوکارهای نظارتی و کنترلی، توانایی شناسایی تراکنش‌های غیرعادی را دارند و در چنین شرایطی منشأ این وجوه قابل توجه نخواهد بود. به همین دلیل، این دسته از عواید غیرقانونی غالباً با عنوان پول سیاه شناخته می‌شوند و می‌توانند آثار مخرب و قابل توجهی بر ساختارهای اقتصادی بر جای بگذارند. بر همین اساس، قوانین و مقررات مبارزه با پولشویی در بسیاری از کشورها، اعم از اقتصادهای نوظهور و کشورهای توسعه‌یافته، با جدیت تدوین و اجرا می‌شود. (Samanta, Kumar Mohanta, Prasad Pati & Jena, 2019: 425-427) مجرمان همیشه سعی کرده‌اند منشأ دارایی‌های به دست آمده از جنایات را پنهان، تا همه آثار خلافتکاری خود را پاک کنند. این روزها روش‌های پولشویی پیچیده تر شده و منطق تطهیر، دیگر تغییر شکل اسکناس به شمش طلا نیست، بلکه ساخت ویتترین قانونی برای عملیات و فعالیت‌های غیرقانونی است. (نوروزی، خوشگو و ابوالقاسمی، ۱۴۰۳: ۵۷) در ایران قانون مبارزه با پولشویی به پیروی از قانون تشدید، طریق نامشروع تحصیل را جرم انگاری کرده است. چیزی که گرانیگاه هر دو قانون است، عدم مشروعیت روش و چگونگی تحصیل مال است و ماهیت مال تحصیل شده و مشروع یا نامشروع بودن آن مؤثر در مقام نیست. لذا دریافت مالی که از رهگذر جرم بدست آمده باشد، بدون علم و اطلاع به منشأ مجرمانه آن جرم نبوده و مشمول قانون پولشویی نیست. (رستمی، ۱۳۹۸: ۴۰۴۰) نقش ربات‌های هوشمند در پنهان سازی فعالیت‌های مالی غیرقانونی را باید در توانایی آن‌ها برای انجام همزمان و سریع حجم گسترده‌ای از تراکنش‌ها جست‌وجو کرد. این سامانه‌ها قادرند با استفاده از الگوریتم‌های پیچیده، وجوه مالی را در میان حساب‌ها، بازارها و بسترهای مختلف جابه‌جا کنند؛ به گونه‌ای که شناسایی منشأ اولیه پول با دشواری بیشتری همراه شود. در چنین شرایطی، سرعت و تعدد تراکنش‌ها می‌تواند فرآیند نظارت و ردیابی مالی را با چالش جدی مواجه سازد. بر این مبناء بی تردید ابزارهای سنتی قادر به شناسایی پولشویی نوین نیستند و لذا بکارگیری هوش مصنوعی در تشخیص فعالیت‌های مالی غیر

قانونی مانند پولشویی اهمیت دارد. در این بین عملکرد ربات های هوشمند در پولشویی نیز روز به روز فرآیند این شناسایی را دشوار می کند. در کنار ضرورت ایجاد ابزارهای لازم برای مقابله با پولشویی هوشمند، تدوین قوانین برای حمایت های اجرایی و قضایی و همچنین راه اندازی مراکزی به منظور غربالگری هوشمند ضرورت دارد. در زمان تدوین این پژوهش متأسفانه در ایران این خلاء احساس می شود و امید است دستاوردهای این مقاله بتواند در بهبود شرایط مفید باشد. در بررسی پولشویی هوشمند توسط ربات های معامله گر ملاحظه می گردد که سه تکنیک مهم در انجام این فرآیند قابل انجام است که این مراحل توسط ویلیام روزنبلات شامل خرد کردن تراکنش ها^۱، لایه بندی مالی^۲ و ادغام (یکپارچه سازی)^۳ توصیف گردید.

برخی از نویسندگان مراحل بیشتری را برای فرایند پولشویی برشمرده و میان آنها تمایز قائل شده اند. با این حال، تأکید می شود که طی شدن تمامی این مراحل در همه موارد الزامی نیست و بسته به شرایط، ممکن است تنها بخشی از این مراحل در فرایند پولشویی تحقق یابد. (Levi & Soudijn, 2020: 582-580) بر این مبناء استفاده از ربات های هوشمند موجب شده است که برخی رفتارهای مالی غیرعادی در قالب معاملات ظاهراً مشروع پنهان شوند. بسیاری از این ربات ها به نحوی طراحی می شوند که الگوهای معاملاتی آنها مشابه فعالیت های عادی بازار به نظر برسد و همین امر احتمال شناسایی اقدامات مشکوک را کاهش می دهد. این امر خصوصاً در ارتباط با ارزهای دیجیتال از اهمیت بیشتری برخوردار است. بر همین اساس در ادامه با توجه به اهمیت ارزهای دیجیتال در فرآیند پولشویی هوشمند به مطالعه آن پرداخته می شود.

۱-۲-۱. ایجاد و اجرای تعداد بالای تراکنش های کوچک

خرد کردن تراکنش ها به معنای ایجاد و اجرای تعداد بالای تراکنش های کوچک است که شامل تقسیم بخش های عظیمی از پول به واحدهای کوچکتر می باشد. این روش کمک می نماید که در حین انجام تراکنش کمتر شک ایجاد شود و لذا می تواند از شناسایی جلوگیری کند.

با گسترش روزافزون فناوری و افزایش مشارکت افراد در اقتصاد دیجیتال در سراسر جهان، ضرورت تدوین مقررات و به کارگیری ابزارهای نظارتی کارآمد برای مقابله با بهره برداری مجرمانه از این بسترها بیش از پیش احساس می شود. در این میان، پیشرفت های فناوریانه نقش ربات های معامله گر را در بازارهای مالی پررنگ تر کرده است. ربات های معامله گر قادرند حجم زیادی از تراکنش های کوچک را در بازارهای مالی و صرافی های رمزارزی به صورت خودکار اجرا کنند. این تراکنش ها غالباً به گونه ای طراحی می شوند که الگوی آنها طبیعی و عادی به نظر برسد و در نتیجه از سامانه های نظارتی و هشدارهای ضد پولشویی عبور کنند. در چنین شرایطی، شناسایی و ردیابی منشاء واقعی وجوه با دشواری بیشتری برای نهادهای نظارتی همراه خواهد بود. (Levi

1. Smurfing
2. Layering
3. Integration

586: 2020, Soudijn &) یکی از مهم ترین ویژگی های این شیوه، عادی جلوه دادن جریان های مالی غیرقانونی در بستر تراکنش های روزمره است. در واقع، زمانی که حجم گسترده ای از نقل و انتقالات خرد به صورت مستمر و خودکار انجام می شود، تشخیص ارتباط میان آن ها برای نهادهای نظارتی دشوارتر خواهد شد. در واقع وظیفه ربات های هوشمند در این خصوص این است که درآمدهای غیرقانونی را که توسط مجرمان بدست آمده بنحوی پنهان نمایند که منبع اصلی و اولیه آن مشروع جلوه نماید. بدیهی است که تراکنش های کوچک و خرد کمتر جلب توجه می نماید و امکان ارتباط تراکنش های کوچک با هم بسیار دشوار است. بطورمثال یک ربات ها ممکن است میلیون ها دلار پول غیرقانونی را به هزاران حساب مختلف ارسال کنند و سپس این وجوه را با تأخیر زمانی مشخص دوباره جمع کند.

برای مقابله مؤثر با این پدیده، ضروری است سامانه های کنونی مبارزه با پولشویی از قابلیت های پیشرفته تری برخوردار باشند، به گونه ای که بتوانند تحلیل پیوندها، تحلیل شبکه ای تراکنش ها، طبقه بندی ریسک ها و شناسایی معاملات غیرقانونی یا مشکوک را به طور دقیق انجام دهند. اهمیت این امر از آنجا ناشی می شود که تحلیل عملیات پولشویی به ویژه در مواردی که شامل تعداد زیادی تراکنش های خرد است فرایندی بسیار پیچیده به شمار می آید. چنین تحلیلی مستلزم پردازش حجم عظیمی از داده ها از منابع مختلف، از جمله صورت حساب ها، فعالیت های حساب های بانکی و سایر داده های مالی مرتبط و نیز استخراج اطلاعات معنادار از میان این داده ها است. (Mallik, Raisul Islam, Uddin, Azam Ali & Trisha, 2025: 95) استفاده از ربات های معامله گر در اجرای تراکنش های خرد نشان می دهد که فناوری های مالی، در کنار مزایای اقتصادی، می توانند زمینه سوءاستفاده مجرمانه را نیز فراهم کنند. هرچه سرعت انجام معاملات و حجم داده های مالی بیشتر شود، امکان پنهان شدن فعالیت های غیرقانونی در میان تراکنش های مشروع نیز افزایش می یابد. لازم به ذکر است که این تکنیک پولشویی در واقع با بهره گیری از الگوریتم های معاملاتی و نوسانات طبیعی بازار، امکان مخفی سازی منشأ پول را افزایش داده و ردیابی تراکنش ها را برای نهادهای نظارتی دشوار می سازد. استفاده از این روش در حوزه رمزارزها به دلیل ماهیت غیرمتمرکز و نیمه ناشناس این بازارها، رواج بیشتری یافته و چالشی اساسی برای سیستم های مبارزه با پولشویی ایجاد کرده است.

۱-۲-۲. پولشویی هوشمند از طریق لایه بندی

۱. فرض کنید یک شبکه مجرمانه مبلغ قابل توجهی پول حاصل از فعالیت های غیرقانونی را در اختیار دارد و قصد پنهان سازی منشأ آن را دارد. در این حالت می توان از یک ربات معامله گر استفاده کرد که این مبلغ را در مدت کوتاهی به صدها یا هزاران تراکنش کوچک تقسیم کرده و از طریق چندین حساب کاربری در صرافی های مختلف رمزارز به انجام معاملات متعدد بپردازد. این ربات می تواند به صورت خودکار دارایی ها را میان ارزهای دیجیتال مختلف جابه جا کند یا معاملات خرید و فروش پی درپی انجام دهد تا جریان مالی ظاهری عادی ایجاد شود. در ادامه، پس از گذشت زمان و ایجاد فاصله میان تراکنش ها، این وجوه در حساب های دیگر دوباره جمع شده و به شکل سرمایه گذاری یا دارایی مشروع وارد چرخه اقتصادی می شوند، امری که ردیابی منشأ اولیه پول را برای نهادهای نظارتی بسیار دشوار می کند.

افزایش استانداردهای گزارش‌دهی و ارتقای سطح شفافیت در نظام بانکی طی سال‌های اخیر موجب شده است مجرمان برای دستیابی به اهداف خود به روش‌های پیچیده‌تر و پیشرفته‌تری روی آورند. با این حال، نوآوری‌های مالی، جهانی‌شدن بازارهای مالی و همچنین گزارش‌دهی محدود درباره مالکان نهایی در برخی حوزه‌های قضایی، همچنان زمینه‌هایی را برای تسهیل این فعالیت‌ها فراهم کرده است. در این میان، لایه‌بندی یکی از مراحل اساسی در فرایند پولشویی به شمار می‌رود که با هدف پنهان‌سازی منشأ غیرقانونی وجوه از طریق ایجاد زنجیره‌ای پیچیده از تراکشی‌های مالی انجام می‌شود. با این وجود، از منظر حقوقی و در فرایند رسیدگی قضایی، آنچه اهمیت اساسی دارد احراز عناصر تشکیل‌دهنده جرم است، به بیان دیگر، تحقق عناصر قانونی، مادی و معنوی جرم از اهمیت بیشتری نسبت به ابزارهای مورد استفاده در ارتکاب آن برخوردار است. (Cassella, 2018: 494-495) در توضیح بطور ساده باید گفت که در این مرحله، دارایی‌های نامشروع از طریق مجموعه‌ای از انتقالات مالی سریع، خرید و فروش دارایی‌های دیجیتال و استفاده از واسطه‌های مالی مختلف در شبکه‌های بانکی و رمزارزی جابه‌جا می‌شوند تا مسیر اولیه آن‌ها غیرقابل شناسایی شود.

هرچه در آمد غیرقانونی که مرتکبان به دست می‌آورند بیشتر باشد، احتمال بیشتری وجود دارد که از یک متخصص پول‌شویی یا ربات‌های معامله‌گر و هوش مصنوعی استفاده کنند. اما گزارش‌های «گروه ویژه اقدام مالی» بیانگر آن است که به دلیل مشکل عمومی نظارت محدود، مشخص کردن میزان استفاده مجرمان از چنین شبکه‌هایی دشوار است، اما گروه‌های مجرمانه سازمان‌یافته با درجه بالا، برای پولشویی از متخصصان که ممکن است از مدیران و متخصصان فناوری و هوش مصنوعی باشند استفاده می‌کنند تا منشأ غیرقانونی درآمدهای خود را پنهان کنند. (گزارش گروه ویژه اقدام مالی، ۲۰۱۸: ۱۳-۱۲) آنچه مرحله لایه‌بندی را در پولشویی هوشمند خطرناک‌تر می‌کند، ترکیب پیچیدگی مالی با سرعت پردازش فناوری‌های نوین است. در واقع استفاده از ربات‌های معامله‌گر این امکان را فراهم کرده است که تعداد زیادی از تراکنش‌ها به صورت همزمان و در مدت کوتاه انجام شود و همین مسئله موجب می‌شود پیگیری مسیر واقعی جریان پول برای نهادهای نظارتی با دشواری بیشتری همراه باشد.

در مرحله لایه بندی نقش اصطلاحاً حاملان پول^۱ دارای اهمیت می باشد زیرا وظیفه آن‌ها معمولاً یا انجام فعال تراکنش‌هایی از طریق حساب‌های بانکی‌شان است، یا تنها ارائه اطلاعات حساب به هماهنگ‌کننده خود. (گزارش گروه ویژه اقدام مالی، ۲۰۱۸: ۲۴-۲۲) طبق گزارش سی‌فَس^۲، در سال ۲۰۱۸ مقامات بریتانیا، ۱۳۹ حساب بانکی متعلق به حاملان پول را شناسایی کردند که نسبت به سال پیش از آن ۲۶٪ افزایش داشته است. از میان افراد موجود در نمونه این مطالعه، ۷۰٪ مرد و ۵۰٪ زیر ۲۶ سال بوده‌اند. این افراد عمدتاً از طریق شبکه‌های اجتماعی و

۱. حاملان پول (Money Mules) به افرادی اطلاق می‌شود که از حساب‌های بانکی خود برای انتقال پول‌های غیرقانونی استفاده می‌کنند، بدون آنکه آگاهی کامل از منشأ این پول‌ها داشته باشند.

۲. سی‌فَس (Cifas) یک سازمان غیرانتفاعی در بریتانیا است که به‌طور تخصصی به مبارزه با تقلب و جرم‌های مالی پرداخته و به‌ویژه بر پیشگیری از تقلب در حوزه‌های مختلف، از جمله پول‌شویی، سرقت هویت و تقلب‌های مالی متمرکز است.

پیام‌رسان‌های فوری جذب شده‌اند.^۱ در مرحله لایه‌بندی، هدف بنیادین مجرمان، گسستن پیوند میان وجوه غیرقانونی و منشأ مجرمانه آن‌ها از طریق ایجاد زنجیره‌ای از تراکنش‌های مالی پیچیده است. در این فرایند، به‌منظور دشوارتر کردن ردیابی جریان‌های مالی و پنهان‌سازی مسیر پول، از ابزارهای نوینی بهره‌گیری می‌شود که ربات‌های معامله‌گر یکی از کلیدی‌ترین آن‌ها هستند. نحوه عملکرد این ربات‌ها در این مرحله به شیوه‌های متعددی صورت می‌پذیرد، از جمله پنهان‌سازی ماهیت تراکنش‌ها، بهره‌گیری از بستر رمزارزها، انتقال وجوه میان حساب‌های متعدد و همچنین ایجاد حجم انبوهی از تراکنش‌های پیچیده در بازه‌های زمانی بسیار کوتاه. این اقدامات، با خود کارسازی و افزایش سرعت گردش مالی، عملاً نظارت‌های سنتی بر جریان‌های پولی را مختل کرده و شناسایی ردپای پول‌های شست‌وشو شده را برای نهادهای نظارتی به چالشی جدی تبدیل می‌کند. (Villányi, 2021: 5-7) لایه بندی در واقع یکی از مهمترین بخش‌های پولشویی است که در فرآیند پولشویی هوشمند این کار توسط هوش مصنوعی و ربات‌های معامله‌گر انجام می‌شود. بهره‌گیری از هوش مصنوعی در مرحله لایه‌بندی نشان می‌دهد که پولشویی نوین بیش از گذشته به دانش تخصصی و مهارت‌های فنی وابسته شده است. مجرمان با استفاده از الگوریتم‌های هوشمند می‌توانند الگوهای رفتاری سیستم‌های نظارتی را شناسایی کرده و نحوه انجام تراکنش‌ها را به گونه‌ای تنظیم کنند که کمتر در معرض شناسایی قرار گیرند.

۱-۳. فرآیند یکپارچه سازی در پولشویی هوشمند

در فرآیند پولشویی پس از لایه بندی، نوبت به ادغام یا یکپارچه سازی می‌رسد که مهمترین و در عین حال مرحله پایانی پولشویی است. در این پایان این مرحله است که پول بصورت صورت ظاهراً قانونی به اقتصاد تزریق و وارد چرخه مالی می‌گردد.

در واقع فرآیند ادغام در پولشویی به مرحله نهایی اشاره دارد که در آن عواید غیرقانونی وارد اقتصاد مشروع می‌شود به گونه‌ای که به نظر می‌رسد قانونی هستند. این معمولاً شامل استفاده از پول‌های غیرقانونی برای خرید دارایی‌هایی مانند خودروها، کسب و کارها، املاک و مستغلات و دیگر کالاها یا خدمات با ارزش می‌شود. هدف از این مرحله، پنهان‌سازی منشأ غیرقانونی پول و ادغام آن در سیستم مالی است تا مجرم بتواند از منافع حاصل از آن بدون جلب توجه بهره‌برداری کند. با تبدیل عواید به دارایی‌های ظاهراً قانونی، مجرمان می‌توانند کار ردیابی و مصادره این دارایی‌ها توسط مقامات قانونی را به شدت دشوار کنند و بدین ترتیب چرخه پولشویی را به پایان برسانند. (گزارش شبکه اجرای مقررات جرائم مالی^۲، ۲۰۱۴: ۲) آنچه مرحله ادغام را در پولشویی هوشمند متمایز می‌کند، تلاش مجرمان برای طبیعی جلوه‌دادن ورود پول به اقتصاد است. در این مرحله، نقش فناوری بیشتر در ایجاد فعالیت عادی، نمود پیدا می‌کند. به این معنا که تراکنش‌ها و خریدهای انجام‌شده طوری تنظیم می‌شوند که در چارچوب رفتارهای معمول اقتصادی قرار بگیرند. مسئله مهم این است که هرچه این تراکنش‌ها پراکنده‌تر و

1. <https://www.cifas.org.uk/newsroom/fraudscape-2019-release>

2. https://www.fincen.gov/sites/default/files/shared/prevention_guide.pdf

در بسترهای بیشتری انجام شوند، تشخیص ارتباط میان آن‌ها دشوارتر شده و شناسایی منشأ اصلی وجوه تقریباً غیرممکن می‌شود.

با پایان مرحله ادغام دیگر امکان شناسایی منشأ پول وجود ندارد، زیرا پول آنقدر از منشأ اصلی خود دور می‌شود که ردگیری آن نیاز به تحلیل شبکه‌ای تراکنش‌ها و سیستم‌های پیشرفته داده کاوی دارد. با توجه به اینکه بهره‌گیری از سیستم هوش مصنوعی و ربات‌های معامله‌گر این فرآیند را پیچیده‌تر می‌کنند در حال حاضر ساز و کار مقابله با پولشویی در موسسات مالی و بانکها قادر به تشخیص پولشویی هوشمند به راحتی نیستند. با این حال نگرانی دیگر در این زمینه مربوط است به صراف‌های دیجیتال و پولشویی از طریق ارزهای دیجیتال که دیگر قابل نظارت نیستند.

۱-۴. ارزهای دیجیتال و پولشویی هوشمند

در سال‌های اخیر، عوامل متعددی موجب شده است تا ارزهای دیجیتال بیش از هر زمان دیگری در کانون توجهات اقتصادی و فناورانه قرار گیرند. در این میان، ماهیت غیرمتمرکز این دارایی‌ها، چالش‌های نوین و پیچیده‌ای را در حوزه مبارزه با پولشویی پدید آورده است. ویژگی‌هایی نظیر سرعت بالای تراکنش‌ها، هزینه‌ی ناچیز انتقال و قابلیت حفظ ناشناسی، ارزهای دیجیتال را به ابزاری جذاب و بالقوه برای جابه‌جایی و پنهان‌سازی عواید ناشی از فعالیت‌های مجرمانه تبدیل کرده است، امری که ردیابی و کنترل جریان‌های مالی مشکوک را برای نهادهای نظارتی به مراتب دشوارتر از گذشته ساخته است. (Dionysopoulos, Marra & Urquhart, 2024: 3-4) ارزهای دیجیتال به دلیل آنکه ماهیت غیر قابل نظارت دارد محلی امن برای اشخاص و گروه‌هایی شده است که با استفاده از آن می‌توانند نیت‌ها سوء خود را به نتیجه برسانند. این به وضوح ارزهای دیجیتال را از ارزهای ملی جدا می‌کند و شکی نیست که ارزهای دیجیتال امکان بکارگیری در جرم و جنایت را دارند. (قاسمی، نیاکانی و جواهری، ۱۴۰۳: ۳۵-۳۳)

ارزهای دیجیتال و پولشویی هوشمند دارای ارتباط نزدیکی هستند و دلیل آن به دو موضوع مهم مرتبط می‌شود. نخست اینکه ارزهای دیجیتال را می‌توان به صورت مستعار یا ناشناس منتقل کرد. علاوه بر این، تراکنش‌ها به طور خودکار بررسی نمی‌شوند و بسیار سریع و بدون تشریفات اضافه هستند. دوم اینکه امکان دور زدن کیف پول‌ها چه از طریق تراکنش‌های خرد، هک یا تکنیک‌های دیگر وجود دارد. در این مرحله است که شکافی را در مقررات مربوط به ارزهای دیجیتال آشکار می‌کند.

اتحادیه اروپا اخیراً مقرر کرده است که با هدف ایجاد یک چارچوب قانونی یکسان در تمام کشورهای عضو اتحادیه اروپا برای محافظت از سرمایه‌گذاران، حفظ ثبات مالی و جلوگیری از پولشویی تصویب کرده است. همچنین این مقرر صراف‌ها و ارائه‌دهندگان خدمات رمزارزی را در چارچوبی منسجم موظف به مجوزدهی، نظارت، شفافیت

و رعایت الزامات ضد پولشویی قرار داده است.¹ این رویکرد نشان می‌دهد که قانونگذاران اروپایی در برابر سوءاستفاده مجرمانه از بازارهای رمزارزی، به‌ویژه در قالب پولشویی هوشمند، به سمت تنظیم‌گری سخت‌گیرانه‌تر حرکت کرده است.

در توصیف این فرایند می‌توان چنین بیان کرد که انتقال وجوه معمولاً از یک کیف پول مبدا که هویت آن مشخص و تحت نظارت است، آغاز می‌شود، این دارایی‌ها ابتدا به یک صرافی ارز دیجیتال ارسال شده و از آنجا به یک کیف پول مقصد انتقال می‌یابند که فاقد هویت احراز شده بوده و خارج از چارچوب‌های نظارتی قرار دارد. در مرحله بعد، دارنده‌ی این کیف پول غیرشفاف، با بهره‌گیری از رمزارهایی که قابلیت ردیابی پایینی دارند، تراکنش‌های متعددی را در بسترهای غیرمتمرکز انجام می‌دهد. این سلسله عملیات که با هدف گسستن زنجیره اطلاعاتی صورت می‌گیرد، باعث می‌شود که شناسایی منشأ اصلی وجوه برای مراجع قانونی و ضابطان قضایی عملاً غیرممکن یا بسیار دشوار شود. (Mooij, 2023: 70) در این میان، ربات‌های معامله‌گر با اجرای معاملات خودکار و الگوریتمی، فرآیند پولشویی از طریق ارزهای دیجیتال را به سطحی پیشرفته‌تر و هوشمندتر رسانده‌اند. این ربات‌ها می‌توانند با اجرای حجم بالایی از معاملات خرد، تبدیل متوالی ارزها و جابه‌جایی دارایی بین صرافی‌های غیرمتمرکز، منشأ پول را به گونه‌ای پیچیده تغییر دهند که رهگیری آن برای نهادهای نظارتی دشوار شود.

به‌منظور پیشگیری از پولشویی هوشمند از طریق بسترهای رمزارزی، راهکار پیشنهادی بر کاهش جدی و نظام‌مند تعامل با کیف پول‌های غیرقانونی متمرکز است، امری که تحقق آن مستلزم وضع قوانین بازدارنده و تدوین استانداردهای حقوقی کارآمد در این حوزه می‌باشد. با این حال، اثربخشی چنین رویکردی منوط به مسدودسازی یا محدودسازی شدید امکان تبادل میان ارزهای دیجیتال با منشأ غیرقانونی و دارایی‌های مجاز است. چنانچه صرافی‌های رمزارزی امکان انتقال دارایی از کیف پول‌های احراز نشده به کیف پول‌های تحت نظارت و قانونی را تسهیل نمایند، عملاً راه‌گزینی برای فعالیت‌های مجرمانه، از جمله پولشویی و تأمین مالی تروریسم²، گشوده شده و کارایی نظارت‌های مالی به‌شدت مخدوش خواهد شد. (Ibid: 71) نکته مهم دیگر پیرامون ارزهای دیجیتال و پولشویی هوشمند آن است که مجرمان از همان ویژگی‌هایی بهره می‌برند که اساساً برای آزادی و سهولت تبادل مالی طراحی شده بود. در حقیقت ناشناس بودن تراکنش‌ها، نبود الزام به احراز هویت کامل و فعالیت صرافی‌های غیرمتمرکز، عملاً محیطی ایجاد کرده‌اند که در آن رفتارهای مشکوک به‌سختی قابل تمایز از فعالیت‌های عادی‌اند. این وضعیت نشان می‌دهد که مقابله مؤثر با پولشویی در فضای رمزارزها تنها با محدودسازی فناوری ممکن نیست. همچنین لازم به ذکر است که با توسعه فناوری، استفاده از تحلیل بلاکچین و هوش مصنوعی در ردیابی الگوهای مشکوک، به‌عنوان راهکاری نوین برای مقابله با این چالش مطرح می‌باشد.

1. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937

2. Money laundering and the financing of terrorism (MLFT)

۲. کاربرد ربات‌های معامله‌گر و هوش مصنوعی برای مجرمان یقه طلایی

مؤسسات مالی مکلف به رعایت استانداردهای انطباق و مقررات سخت گیرانه‌ای هستند که با هدف حصول اطمینان از مشروعیت منابع مالی و سلامت تراکنش‌ها تدوین شده‌اند. با این حال، جریان‌های مجرمانه و مؤسسات مالی فاسد با بهره‌گیری از شیوه‌های غیرقانونی، همواره در تلاش‌اند تا عواید حاصل از فعالیت‌های بزهکارانه از قبیل تأمین مالی تروریسم، قاچاق انسان و مواد مخدر را به چرخه‌ی اقتصاد رسمی تزریق کرده و برای آن مشروعیت ظاهری ایجاد کنند. در این فرایند، مشارکت و حمایت عناصری ضروری است که یا از نفوذ سیاسی و جایگاه‌های تصمیم‌گیر در بدنه دستگاه‌های دولتی برخوردارند و یا به عنوان متخصصان خبره در حوزه‌ی فناوری ایفای نقش می‌کنند. بدین ترتیب، این شکل از پولشویی پیچیده توسط گروهی از مجرمان صورت می‌گیرد که در ادبیات جرم‌شناسی به مجرمان یقه‌طلایی شهرت دارند، کسانی که با تکیه بر دانش فنی و دسترسی به رانت‌های قدرت، بستر ساز و تسهیل‌گر این گونه جرائم سازمان‌یافته محسوب می‌شوند. Alhajeri&Alhashem, 2023: 285) یقه‌طلایی‌ها نیز معمولاً همانند بزهکاران یقه سفید "محترم" و متعلق به "طبقه‌ی بالای جامعه" نیز از موقعیت کاری خود و به مناسبت در جریان شغل و فعالیت‌های حرفه‌ای خود برای ارتکاب جرائم مرتبط یا ناشی از این فعالیت‌های قانونی استفاده می‌کنند. (نجفی ابرندآبادی، ۱۳۸۵: ۱۷) در چنین بستری، استفاده مجرمان یقه‌طلایی از ربات‌های معامله‌گر و سامانه‌های هوش مصنوعی صرفاً به سوءاستفاده فردی از موقعیت شغلی محدود نمی‌شود، بلکه به آن‌ها امکان می‌دهد تا فرآیندهای پولشویی را در درون ساختارهای رسمی مالی پنهان کنند. بر همین اساس، در ادامه ابتدا به چگونگی تسهیل پولشویی هوشمند توسط مجرمان یقه‌طلایی و سپس به کاستی‌های نظام نظارتی و مؤسسات مالی در شناسایی این نوع پولشویی پرداخته می‌شود.

۲-۱. تسهیل پولشویی هوشمند توسط مجرمان یقه‌طلایی

با پیشرفت فناوری‌های دیجیتال، مجرمان یقه‌طلایی نیز روش‌های خود را برای پولشویی تطبیق داده و به سمت استفاده از ربات‌های هوشمند سوق داده‌اند. این افراد که اغلب در بخش‌های مالی، بانکی و شرکت‌های بزرگ فعالیت دارند، از ابزارهای مدرن برای پنهان‌سازی منبع پول‌های غیرقانونی بهره می‌برند. در واقع باید گفت هوش مصنوعی و یادگیری ماشینی یکی از مهم‌ترین فناوری‌هایی است که در این حوزه به کار گرفته می‌شود. الگوریتم‌های پیشرفته قادرند مسیرهای بهینه برای انتقال پول را بدون جلب توجه نهادهای نظارتی شناسایی کنند. همچنین، این سیستم‌ها می‌توانند تراکنش‌های مالی را به گونه‌ای تنظیم کنند که به نظر قانونی و طبیعی برسند، در حالی که در واقع هدف آن‌ها تطهیر پول‌های غیرقانونی است.

از آن جا که جرم‌شناسی اقتصادی متعرض طبقه‌ای شده است که خود متولی جامعه بوده و نسبت به آنها هرگز سوءظنی وجود نداشته است (نجفی ابرندآبادی، ۱۳۹۱: ۱۲) آنچه که در اقدامات مجرمان یقه‌طلایی به منظور

پولشویی هوشمند اهمیت دارد شناخت از الگوی فعالیت موسسات مالی برای مقابله با پولشویی هوشمند است. در حقیقت این افراد برخلاف مجرمان عادی، هم با سازوکارهای داخلی مؤسسات مالی آشنا هستند و هم می‌توانند از ظرفیت ربات‌های معامله‌گر و سامانه‌های هوش مصنوعی به شکلی هدفمند بهره‌برداری کنند. در نتیجه، بسیاری از تراکنش‌هایی که در ظاهر در چارچوب فعالیت‌های روزمره و عادی بازار انجام می‌شود، در واقع بخشی از یک طرح گسترده برای جابه‌جایی و مشروع جلوه دادن عواید نامشروع است، امری که شناسایی به‌موقع آن را برای نهادهای نظارتی دشوار می‌کند.

مؤسسات مالی به‌منظور شناسایی و پیشگیری از جریان‌های پولشویی هوشمند، چارچوب‌های سیاستی ویژه‌ای را تدوین و اجرا کرده‌اند. اگرچه مقررات کنونی مبارزه با پولشویی نقش مؤثری در مهار این پدیده ایفا می‌کنند، اما محدودیت اصلی آن‌ها در تمرکز بر طیف خاص و محدودی از تراکنش‌ها و رفتارهای مالی نهفته است. در همین راستا، پیشرفت‌های فناوریانه اخیر، توانمندی نهادهای مالی را برای شناسایی و جلوگیری از تراکنش‌های مشکوک ارتقا بخشیده و به‌طور خاص، استفاده از هوش مصنوعی به یکی از ابزارهای راهبردی برای مقابله با شیوه‌های نوین پول‌شویی تبدیل شده است. (Nweze, Kofi Avickson & Ekechukwu, 2024: 2813-2816) در عملیات پولشویی هوشمند توسط مجرمان یقه‌طلایی، با تکیه بر دانش تخصصی و نفوذ سازمانی آنان، در سه مرحله‌ی ساختاریافته و هم‌افزا پیاده‌سازی می‌شود. ابتدا در مرحله جای‌گذاری، عواید غیرقانونی از طریق تزریق به بسترهای تجاری و مالی به‌ظاهر مشروع، برای نخستین بار وارد چرخه‌ی اقتصاد رسمی می‌شوند، سپس در مرحله کلیدی و پیچیده لایه‌بندی مجرمان با بهره‌گیری از تکنیک‌های حسابداری، معاملات صوری و تراکنش‌های متقاطع، پیوند میان وجوه و منشاء مجرمانه‌ی آن‌ها را گسسته و ردپای پول را در ساختارهای مالی پنهان می‌کنند و در نهایت، در مرحله یکپارچه‌سازی، این دارایی‌های به‌ظاهر تطهیر شده با انتقال به حساب‌های معتبر و تحت کنترل عاملان، به گونه‌ای بازگردانی می‌شوند که گویی درآمدهایی کاملاً قانونی و مشروع هستند. (Ris, Stankovic & Avramovic, 2020: 131-133) در این راستا مجرمان یقه‌طلایی از ربات‌های معامله‌گر برای پولشویی هوشمند استفاده می‌کنند، زیرا این ربات‌ها توانایی اجرای تراکنش‌های پیچیده و پرحجم را بدون جلب توجه نهادهای نظارتی دارند. این الگوریتم‌های خودکار می‌توانند با انجام معاملات خرد، مکرر و به‌ظاهر قانونی در بازارهای مالی، مانند بورس، فارکس و رمزارزها، منشأ واقعی وجوه غیرقانونی را پنهان کنند. به علاوه همین آشنایی مجرمان یقه‌طلایی با سیاست‌ها و سازوکارهای ضدپولشویی مؤسسات مالی باعث می‌شود بتوانند رفتار خود را با معیارهای نظارتی تطبیق دهند و از خلاءها و نقاط ضعف سیستم به نفع خود استفاده کنند.

۲-۲. ضعف مؤسسات مالی در شناسایی پولشویی هوشمند

آنچه مقابله با پولشویی نوین یعنی پولشویی هوشمند را در مقایسه با مدل سنتی آن دشوار نموده است، بکارگیری فناوری و تغییر در پارادایم پولشویی است. بر این اساس مؤسسات مالی به‌طور فزاینده‌ای درگیر شکاف میان

زیرساخت‌های قدیمی و روش‌های پیشرفته پولشویی هستند و البته این امر مختص ایران نیست و همه کشورها درگیر چنین چالشی هستند. بدیهی است که رویکردهای سنتی در شناسایی فعالیت‌های مشکوک مالی دیگر کارایی گذشته را ندارند، چرا که مجرمان به‌طور مداوم روش‌های خود را با فناوری‌های نوین تطبیق می‌دهند. این شکاف فناورانه باعث ایجاد نقاط کور مهمی در حتی پیشرفته‌ترین و پرهزینه‌ترین برنامه‌های مبارزه با پولشویی گردیده است.

بر این مبناء، مهمترین ریسک و مشکل پیرامون مقابله با پولشویی هوشمند عدم توانایی و ضعف نهادهای نظارتی و مؤسسات مالی در شناسایی فرآیند پولشویی نوین است. در حالی که بیشتر مؤسسات مالی دارای چارچوب‌های پایه‌ای مقابله با پولشویی سنتی و تا حدودی جدید هستند، با این حال نقاط کور و پنهانی در برنامه‌های آنها وجود دارد که می‌تواند بسیار خطرناک باشد. به علاوه این ریسک‌های پنهان صرفاً به مشکلات سیستمی یا نواقص فرآیندی محدود نمی‌شوند. مؤسسات مالی در تلاش برای یکپارچه‌سازی ابزارهای نوین شناسایی با زیرساخت‌های موجود با چالش‌های بزرگی مواجه‌اند. هزینه‌ها و پیچیدگی‌های بالای جایگزینی این سامانه‌های قدیمی، اغلب مانع از بهره‌گیری کامل بانک‌ها از رویکردهای نوآورانه در مقابله با پولشویی می‌شود. در نتیجه، بسیاری از این مؤسسات همچنان با سامانه‌هایی جزیره‌ای فعالیت می‌کنند که توانایی ارتباط مؤثر با یکدیگر را ندارند.¹

اگرچه در پدیده‌ی پولشویی هوشمند به دلیل بهره‌گیری از ربات‌های معامله‌گر که مبتنی بر الگوریتم‌های پیچیده و تحلیل داده‌های آماری عمل می‌کنند، نقش مستقیم عامل انسانی در مقایسه با شیوه‌های سنتی و دیجیتال پیشین به مراتب کاهش یافته است، اما همچنان نمی‌توان ضرورت نظارت انسانی را در شناسایی و مهار این جرایم نادیده گرفت. در این چارچوب، نقش مأموران انطباق به عنوان لایه نظارتی کلیدی بسیار حائز اهمیت است، چرا که آنان با پایش دقیق رفتارهای مشکوک، تحلیل حساب‌های مشتریان و بررسی تراکنش‌های غیرمعمول، به مثابه فیلتری کارآمد عمل می‌کنند که با تکیه بر قضاوت حرفه‌ای، کاستی‌های احتمالی سیستم‌های خودکار را پوشش داده و از نفوذ عواید مجرمانه به بازارهای مالی جلوگیری می‌کنند. (Japinye, 2024: 56-57)

از سوی دیگر، ماهیت غیرمتمرکز و شبه‌ناشناس ارزهای دیجیتال، در کنار شیوه‌های پیچیده‌ای که مجرمان برای بهره‌برداری از این فناوری‌ها به کار می‌گیرند، چالش‌های بنیادین و قابل توجهی را فراروی نهادهای انتظامی، مقامات نظارتی و مؤسسات مالی قرار داده است، امری که مبارزه با جرایم مالی، به‌ویژه پولشویی هوشمند، را با پیچیدگی‌های مضاعفی مواجه ساخته و فرایند کشف و پیشگیری از این تخلفات را دشوارتر کرده است. (Makarov & Schoar, 2022: 1-2)

ظهور فناوری بلاکچین بر عمق این چالش‌ها افزوده است، چرا که برخلاف نظام‌های مالی سنتی که در آن واسطه‌ها به‌عنوان گره‌های مرکزی و نظارتی، مسئولیت احراز هویت، مدیریت حساب‌ها و تأمین امنیت تراکنش‌ها را بر عهده داشتند، تحولات اخیر در فناوری، معماری جایگزینی را برای ثبت و مدیریت داده‌ها معرفی کرده است. در

1. <https://www.tookitaki.com/compliance-hub/hidden-risks-in-anti-money-laundering-compliance-what-banks-miss-most>

این الگوی نوین که تحت عنوان «فناوری دفتر کل توزیع شده»^۱ شناخته می‌شود و بلاکچین یکی از مصادیق برجسته آن است، هیچ نهاد واحدی حاکمیت مطلق بر جریان تراکنش‌ها ندارد، بلکه طرف‌های متعددی موسوم به اعتبارسنج‌ها با نگهداری نسخه‌هایی از دفتر کل و رسیدن به اجماع، مشروعیت و صحت تراکنش‌ها را تأیید می‌کنند، تغییری که با حذف واسطه‌های متمرکز، عملاً نظارت‌های کلاسیک بر جریان‌های مالی را با دشواری‌های ساختاری روبه‌رو ساخته است. (Ibid: 4) بر این اساس توسعه الگوریتم‌های یادگیری ماشین که می‌توانند حجم زیادی از داده‌های تراکنش ارز دیجیتال را تحلیل کرده و الگوهای مشکوک به پولشویی را شناسایی کنند و این به نوعی بکارگیری هوش مصنوعی علیه هوش مصنوعی می‌باشد. این الگوریتم‌ها می‌توانند تراکنش‌های مشکوک را برای بررسی بیشتر علامت‌گذاری کنند و به سازمان‌های اجرایی قانون و مؤسسات مالی کمک کنند تا فعالیت‌های غیرقانونی را شناسایی و مختل کنند.

گزارش بانک تسویه حساب‌های بین‌المللی (بازل)^۲ که گزارش‌های «شاخص بازل ضد پول‌شویی»^۳ را منتشر می‌کند، در عین حال بیانگر آن است که تنها مؤسسات مالی نیستند که برای پولشویی هوشمند مورد استفاده قرار می‌گیرند بلکه صرافی‌های دیجیتال، کازینوهای آنلاین و کسب و کارهای دیجیتال دیگر نیز محل پولشویی هوشمند هستند و ربات‌های معامله‌گر در آنها در هر لحظه از شبانه روز در حال فعالیت می‌باشند که ممکن است این فعالیت جنبه غیر قانونی و برای مقاصد پولشویی باشد که در عمل این مراکز نسبت به بانکها و مؤسسات مالی نظارت کمتری دارند و در برخی موارد در کسب و کارهای آنلاین خصوصی اصلاً نظارتی وجود ندارد.^۴ این به معنای آن است که مجرمان یقه طلایی به راحتی در حال پولشویی هوشمند هستند و این پولشویی از طریق ربات‌های معامله‌گر بقدری با ظرافت در حال انجام است که شناسایی آن بسیار مشکل است. در کنار این موارد باید به خلاءهای قانونی در زمینه مقابله با پولشویی هوشمند نیز اشاره کرد. در واقع در کنار ضعف سیستمی در شناسایی موارد پولشویی هوشمند خلاء قانونی در توصیف این شکل از پولشویی، مصادیق آن و مجازات مربوط به آن بر چالش‌های مقابله با پولشویی هوشمند افزوده است. ضرورت دارد تا برای رفع این چالش که مهمترین آسیب را بصورت خاموش به بدنه اقتصادی کشورمان ایران وارد می‌کند، ضمن پژوهش کافی در این زمینه و تدوین قوانین کیفری لازم، به توسعه و ارتقاء سیستم مقابله با پولشویی بانکی پرداخته و در عین حال برخی مشاغل مانند صرافی‌های ارز دیجیتال نیز ملزم به رعایت چارچوب‌های مقابله با پولشویی هوشمند گردند.

بحث و نتیجه گیری

پولشویی هوشمند به عنوان یکی از پیچیده‌ترین چالش‌های نظام‌های مالی و امنیتی در عصر دیجیتال مطرح است. مجرمان یقه طلایی با بهره‌گیری از فناوری‌های پیشرفته مانند ربات‌های معامله‌گر و هوش مصنوعی، روش‌های

1. Distributed Ledger Technology (DLT)

2. Bank for International Settlements (BIS)

3. Basel AML Index report

4. <https://index.baselgovernance.org/downloads>

سنتی پولشویی را متحول کرده‌اند. این افراد که معمولاً دارای تحصیلات عالی، دانش فنی پیشرفته و ارتباطات سیاسی-اقتصادی قوی هستند، با استفاده از الگوریتم‌های پیچیده، شناسایی و پیگرد قانونی جرائم مالی را دشوارتر ساخته‌اند. پولشویی هوشمند در سه مرحله اصلی انجام می‌شود بدین نحو که ابتدا وجوه غیرقانونی وارد سیستم مالی می‌شوند، سپس با تراکنش‌های پیچیده و چندلایه ردپای مالی مخفی می‌شود و در نهایت پول‌های شسته‌شده به صورت قانونی وارد اقتصاد می‌گردند. ربات‌های معامله‌گر با انجام هزاران تراکنش خرد در کسری از ثانیه، شناسایی منشأ پول را غیرممکن می‌سازند. هوش مصنوعی نیز با تحلیل الگوهای بازار، بهترین مسیرهای پولشویی را شناسایی و اجرا می‌کند. در این راستا ارزش‌های دیجیتال به دلیل ماهیت نیمه‌ناشناس و غیرمتمرکز، به ابزاری ایده‌آل برای پولشویی تبدیل شده‌اند. مجرمان با استفاده از صرافی‌های غیرمتمرکز و ترکیب ارزش‌های دیجیتال، ردگیری تراکنش‌ها را دشوار می‌کنند. این در حالی است که بسیاری از مؤسسات مالی هنوز از سیستم‌های قدیمی برای شناسایی فعالیت‌های مشکوک استفاده می‌کنند که در مقابل الگوریتم‌های پیشرفته پولشویی هوشمند ناتوان هستند. قوانین فعلی ضد پولشویی نیز عمدتاً برای روش‌های سنتی طراحی شده‌اند و پوشش کاملی برای جرائم دیجیتال ندارند. عدم تعریف دقیق پولشویی هوشمند در قوانین کیفری و ماهیت فرامرزی این پدیده، اجرای عدالت پیرامون آن را با مشکل مواجه کرده است. برای مقابله با این چالش‌ها، به‌روزرسانی فناوری‌های نظارتی، تقویت چارچوب‌های قانونی و همکاری بین‌المللی ضروری است. همچنین استفاده از هوش مصنوعی و یادگیری ماشین برای شناسایی الگوهای پیچیده پولشویی، توسعه سیستم‌های تحلیل شبکه‌ای تراکنش‌های مالی و یکپارچه‌سازی داده‌های مؤسسات مالی از جمله راهکارهای فناورانه هستند. از سوی دیگر، جرم‌انگاری صریح پولشویی هوشمند، الزام صرافی‌های ارز دیجیتال به رعایت مقررات شناسایی مشتری و ایجاد نهادهای تخصصی برای بررسی جرائم مالی دیجیتال از اقدامات حقوقی ضروری محسوب می‌شوند. همکاری‌های اطلاعاتی بین نهادهای مالی و پلیس‌های بین‌المللی و تدوین استانداردهای جهانی برای نظارت بر تراکنش‌های ارزهای دیجیتال نیز از اهمیت ویژه‌ای برخوردار است. نتایج پژوهش نشان می‌دهد که گسترش فناوری‌های مالی، به‌ویژه هوش مصنوعی و ربات‌های معامله‌گر، موجب تحول در شیوه‌های ارتکاب پولشویی شده است. در چنین فضایی، مجرمان یقه‌طلایی با بهره‌گیری از دانش تخصصی و دسترسی به ابزارهای پیشرفته، قادرند فرآیندهای پیچیده‌ای از انتقال، لایه‌بندی و یکپارچه‌سازی وجوه غیرقانونی را طراحی کنند، به گونه‌ای که بسیاری از این فعالیت‌ها در ظاهر با رفتارهای عادی بازارهای مالی تفاوت چندانی ندارند. همین امر سبب شده است که شیوه‌های سنتی نظارت مالی و مبارزه با پولشویی در بسیاری از موارد کارایی کمتری در شناسایی الگوهای نوین پولشویی هوشمند داشته باشند. به نظر می‌رسد نظام حقوقی ایران در حوزه مبارزه با پولشویی نیازمند بازنگری و تکمیل مقررات موجود است. قوانین فعلی مبارزه با پولشویی عمدتاً بر شیوه‌های سنتی انتقال وجوه متمرکز بوده و در زمینه ابزارهای نوین مالی، از جمله معاملات الگوریتمی و فعالیت در بستر رمزارزها، با خلأهای تقنینی مواجه است. از سوی دیگر، روش‌های کشف جرم نیز باید با بهره‌گیری از تحلیل داده‌های مالی، رصد هوشمند تراکنش‌ها و همکاری میان نهادهای نظارتی و قضایی تقویت شود تا امکان شناسایی الگوهای پیچیده پولشویی فراهم گردد. در حوزه دادرسی نیز تخصصی‌تر شدن

رسیدگی به جرایم مالی و استفاده از کارشناسان فناوری مالی می‌تواند به افزایش کارآمدی فرآیند رسیدگی کمک کند. همچنین با توجه به اینکه ربات‌های معامله‌گر در حال حاضر ابزارهایی تحت کنترل انسان محسوب می‌شوند، مسئولیت کیفری آنها مستقلاً قابل تصور نیست و مسئولیت متوجه طراحان، بهره‌برداران یا استفاده‌کنندگان از این سامانه‌ها خواهد بود. در نهایت، اتخاذ رویکردی پیشگیرانه از طریق تنظیم‌گری فعالیت صرافی‌های رمزارزی، ارتقای شفافیت تراکنش‌های مالی و توسعه سامانه‌های نظارتی مبتنی بر فناوری، می‌تواند نقش مهمی در کاهش زمینه‌های سوءاستفاده مجرمانه از فناوری‌های نوین ایفا کند.

منابع

- ارجمند نژاد، عبدالمهدی؛ حبیبی، رضا و بابائی کیایی، مسعود. (۱۴۰۳). به کارگیری روش شبکه‌های هوشمند عصبی در شناسایی و رتبه‌بندی رفتاری مشتریان مظنون به پول‌شویی (مورد مطالعه: بانک ملت). *مطالعاتی در مدیریت بانکی و بانکداری اسلامی*، ۱۰(۲)، ۳۸-۱.

https://jifb.ibi.ac.ir/article_206095.html

- پروین، خیراله و الهیاری فرد، علی. (۱۴۰۳). تنظیم‌گری دولت در حوزه مبارزه با پول‌شویی از طریق رمزارز: مطالعه تطبیقی نظام حقوقی جمهوری اسلامی ایران و ایتالیا. *مطالعات حقوق عمومی*، ۵۴(۳)، ۱۵۷۴-۱۵۴۹.

https://jpls.ut.ac.ir/article_97768.html

- پیوندی، سعیده و گل ارضی، غلامحسین. (۱۴۰۴). تبیین عوامل موثر در وقوع پولشویی. *پژوهش‌های تجربی حسابداری*، ۱۵(۱)، ۸۵-۱۱۴.

https://jera.alzahra.ac.ir/article_8010.html

- خرازی، علیرضا. (۱۴۰۴). الگوی بومی پیشگیری از اعتیاد با استفاده از هوش مصنوعی در شبکه‌های اجتماعی: رویکردی نوین برای آگاهی‌بخشی و کاهش گرایش به مواد مخدر. *پژوهش‌نامه مواد مخدر*، ۱۷(۶۴)، ۱۶-۱.

http://dles.jrl.police.ir/article_104746.html

- جمالی حاجانی، امیر؛ عبدالحی، اسماعیل و میرزایی، احمد. (۱۴۰۳). استانداردهای FATF در اتخاذ رویکرد ریسک‌محور (RBA) در ساختار نظارتی - کنترلی ضد پول‌شویی و موضع تقنینی ایران. *پژوهش‌های حقوقی*، ۲۳(۵۸)، ۲۱۷-۲۵۲.

https://jlr.sdil.ac.ir/article_171486.html

- سبجانی، حسین. (۱۴۰۴). رویکرد ریسک‌پایه ناظر بر عوائد مجرمانه در پرتو مطالعه تطبیقی و استانداردهای FATF. *مطالعات حقوقی*، ۱۷(۱)، ۱۵۷-۲۰۰.

https://jls.shirazu.ac.ir/article_8090.html

- شاکری بهبهانی، مهدی. (۱۳۹۸). *کشف پولشویی با روش‌های هوشمند در سیستم بانکی*. چاپ اول. پژوهندگان راه دانش.

- رشیدی، جاسم؛ شاملو، باقر و سایبانی، علیرضا. (۱۳۹۹). اثبات جرم پولشویی و معیار تشخیص آن در اسناد بین‌المللی و داخلی ایران. *پژوهش‌های بین‌الملل*، ۱۰(۳۸)، ۳۲۷-۳۵۶.

https://www.iisajournals.ir/article_163066.html

- رستمی، هادی. (۱۳۹۸). *تحصیل مال از طریق نامشروع در پرتو مقررات پولشویی، مطالعات حقوق کیفری و جرم‌شناسی*، ۴۹(۲)، ۳۹۷-۴۱۷.

https://jqclcs.ut.ac.ir/article_76130.html

- رضوی فرد، بهزاد. (۱۳۹۸). پول شویی. در دانشنامه علوم جنایی اقتصادی. به کوشش امیرحسن نیازپور. چاپ دوم. بنیاد حقوقی میزان.

- زر نشان، شهرام؛ شجاعی نصرآبادی، محمد. (۱۳۹۶). ضرورت جرم انگاری پولشویی مستقل از جرم منشاء، آموزه های حقوق کیفری، ۱۴ (۱۴)، ۲۰۰-۱۷۳.

https://cld.razavi.ac.ir/article_492.html

- دارابی، شهرداد. (۱۳۹۷). پیشگیری از جرایم خونین یقه سرخ ها. پژوهشنامه حقوق کیفری، ۹ (۲)، ۱۳۳-۱۵۴.

https://jol.guilan.ac.ir/article_3139.html

- علیمردادی دوکوهی، هدایت و نوروزی، عرفانه. (۱۴۰۳). مروری بر روش های هوشمند داده کاوی جهت مبارزه با پول شویی و استقرار حاکمیت داده در شبکه بانکی. سامانه های پردازشی و ارتباطی چند رسانه ای هوشمند، ۵۸ (۴)، ۴۷-۵۸.

<https://sanad.iau.ir/Journal/impcs/Article/903603>

- قاسمی، ابوالفضل؛ جوادی نیاکانی، حسن و جواهری، مهدی. (۱۴۰۳). شناسایی چالش های فراجا در مقابله با خرید و فروش مواد مخدر از طریق رمز ارزها. پژوهش نامه مواد مخدر، ۱۶ (۶۲)، ۴۸-۳۱.

http://dles.jrl.police.ir/article_104296.html

- نجفی ابرندآبادی، علی حسین. (۱۴۰۳). تحولات جرم شناسی بزهکاری یقه سفیدها دیباچه در: بزهکاری یقه سرخ ها. شهرداد دارابی. چاپ دوم. بنیاد حقوقی میزان.

- نجفی ابرندآبادی، علی حسین. (۱۳۸۵). تحلیل جرم شناختی جرایم اقتصادی. تعالی حقوق، ۱ (۶)، ۱۹-۱۵.

- نجفی ابرندآبادی، علی حسین. (۱۳۹۱). ز جرم یقه سفیدی تا جرم اقتصادی. دیباچه در: سمپسون و دیگران. جرایم یقه سفیدی؛ رویکردی فرصت مدار. ترجمه: اسماعیل رحیمی نژاد. چاپ اول. بنیاد حقوقی میزان.

- نوروزی، میثم؛ اسکندری خوشگو، مهدی و ابوالقاسمی، ساناز. (۱۴۰۳). بررسی رویکرد نهادهای مالی بین المللی در پیشگیری و مقابله با پولشویی. مطالعات بین المللی، ۲۱ (۱)، ۷۳-۵۵.

https://www.isjq.ir/article_191125.html

- Alhajeri, R., & Alhashem, A. (2023). Using artificial intelligence to combat money laundering. *Intelligent Information Management*, 15(4), 284-305.

<https://doi.org/10.4236/iim.2023.154014>

- Bergström, M. (2024). *The EU's fight against money laundering and terrorist financing in a digital and fragmented world. In The Borders of the European Union in a Conflictual World: Interdisciplinary European Studies* (pp. 177-203). Cham: Springer Nature Switzerland.

- Bichler, G., Malm, A., & Cooper, T. (2017). Drug supply networks: a systematic review of the organizational structure of illicit drug trade. *Crime Science*, 6(2), 1-23.

<https://link.springer.com/article/10.1186/s40163-017-0063-3>

- Brants, C. (2007). *Gold-collar crime: The peculiar complexities and ambiguities of war crimes, crimes against humanity, and genocide. In International handbook of white-collar and corporate crime* (pp. 309-326). Boston, MA: Springer US.

- Buchanan, B. (2004). Money laundering—a global obstacle. *Research in International Business and Finance*, 18(1), 115-127.

<https://doi.org/10.1016/j.ribaf.2004.02.001>

- Cassella, S. D. (2018). Toward a new model of money laundering: Is the “placement, layering, integration” model obsolete?. *Journal of Money Laundering Control*, 21(4), 494-497.

doi: 10.1108/JMLC-09-2017-0045

- Davis, M. (2024). *Scamageddon: Pt 10 (Gold-collar Crime)*. Published in Dreamocracy. <https://dreamocracy.ai/>
- Dionysopoulos, L., Marra, M., & Urquhart, A. (2024). Central bank digital currencies: A critical review. *International Review of Financial Analysis*, 91, 103031. <https://doi.org/10.1016/j.irfa.2023.103031>
- FATF (Financial Action Task Force). (2018, July). *Professional money laundering*. Paris, France: Financial Action Task Force. <https://www.fatf-gafi.org/en/publications/Methodsandtrends/Professional-money-laundering.html>
- Gilmour, N. (2016). Understanding the practices behind money laundering—A rational choice interpretation. *International Journal of Law, Crime and Justice*, 44, 1-13. <https://doi.org/10.1016/j.ijlcj.2015.03.002>
- Hendriyetty, N., & Grewal, B. S. (2017). Macroeconomics of money laundering: effects and measurements. *Journal of Financial Crime*, 24(1), 65-81. <https://doi.org/10.1108/JFC-01-2016-0004>
- Ilker, K. A. R. A., & Aydos, M. (2020). Cyber fraud: Detection and analysis of the crypto-ransomware. *11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference*. <https://ieeexplore.ieee.org/abstract/document/9298128>
- Isolauri, E. A., & Ameer, I. (2023). Money laundering as a transnational business phenomenon: a systematic review and future agenda. *Critical Perspectives on International Business*, 19(3), 426-468. <https://www.emerald.com/cpoib/article/19/3/426/28439>
- 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*, 12(4), 54-80. <https://doi.org/10.37745/ejaaf.2013/vol12n45480>
- Julius Otusanya, O. (2012). An investigation of the financial criminal practices of the elite in developing countries: Evidence from Nigeria. *Journal of financial crime*, 19(2), 175-206. <https://www.emerald.com/jfc/article/19/2/175/214380>
- Levi, M., & Soudijn, M. (2020). Understanding the laundering of organized crime money. *Crime and Justice*, 49(1), 579-631. <https://www.journals.uchicago.edu/doi/abs/10.1086/708047>
- Maggetti, M. (2014). Promoting corporate responsibility in private banking: Necessary and sufficient conditions for joining the Wolfsberg Initiative against money laundering. *Business & Society*, 53(6), 787-819. doi: 10.1177/0007650312439448.
- Makarov, I., & Schoar, A. (2022). Cryptocurrencies and decentralized finance (DeFi). *Brookings Papers on Economic Activity*, 2022(1), 141-215. <https://muse.jhu.edu/pub/1/article/872595/summary>
- Mallik, S. K., Islam, M. R., Uddin, I., Ali, M. A., & Trisha, S. M. (2025). Leveraging artificial intelligence to mitigate money laundering risks through the detection of cyberbullying patterns in financial transactions. *Global Journal of Engineering and Technology Advances*, 22(01), 094-115. <https://doi.org/10.30574/gjeta.2025.22.1.0015>
- Marriott, L. (2017). The construction of crime: the presumption of blue-collar guilt and white-collar innocence. *Social Policy and Society*, 16(2), 237-251. <https://doi.org/10.1017/S1474746416000063>
- Mer, A., Singhal, K., & Viridi, A. S. (2024). A review of the role of artificial intelligence in banking and stock market trading. *Finance Analytics in Business*, 175-198. <https://doi.org/10.1108/978-1-83753-572-920241009>

- Mooij, A. (2023). *Currency (layering). In Regulating the Metaverse Economy: How to Prevent Money Laundering and the Financing of Terrorism*. Cham: Springer Nature Switzerland.
- Nweze, M., Avickson, E. K., & Ekechukwu, G. (2024). The role of AI and machine learning in fraud detection: enhancing risk management in corporate finance. *Int J Res Publicat Rev*, 5(10), 2812-2830.
<https://www.researchgate.net/profile/Eli-Avickson-2/publication/385098322>
- Ozer, Aleaddin & Aydos, Murat (2025) Fraud Detection Framework for Blockchain Finance: Tackling Arbitrage, Liquidity Exploits, and Money Laundering, *International Journal of Intelligent Systems*, V.2026.
- Rania A.M., Adrian, T., Laxton, M. D., & Obstfeld, M. M. (2018). *Advancing the frontiers of monetary policy*. International Monetary Fund.
- Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937
- Ris, K., Stankovic, Z., & Avramovic, Z. (2020). Implications of implementation of artificial intelligence in the banking business with correlation to the human factor. *Journal of Computer and Communications*, 8(11), 130.
https://www.scirp.org/html/10-1731429_104472.htm
- Samanta, S., Mohanta, B. K., Pati, S. P., & Jena, D. (2019). A framework to build user profile on cryptocurrency data for detection of money laundering activities. *International Conference on Information Technology (ICIT)*.
<https://ieeexplore.ieee.org/abstract/document/9031941/>
- Scholl, H. J., & Bolívar, M. P. R. (2019). Regulation as both enabler of technology use and global competitive tool: The Gibraltar case. *Government Information Quarterly*, 36(3), 601-613. <https://doi.org/10.1016/j.giq.2019.05.003>
- Tiemann, M. (2025). Digital money laundering: threats and EU regulatory reform. *EUI; RSC; Working Paper; 2025/08; Centre for a Digital Society*. <https://hdl.handle.net/1814/78073>
- Tiwari, M., Ferrill, J., & Allan, D. M. (2025). Trade-based money laundering: a systematic literature review. *Journal of Accounting Literature*, 47(5), 1-26.
<https://www.emerald.com/jal/article/47/5/1/1267437>
- Tiwari, M., Gepp, A., & Kumar, K. (2020). A review of money laundering literature: the state of research in key areas. *Pacific Accounting Review*, 32(2), 271-303.
<https://doi.org/10.1108/PAR-06-2019-0065>
- Villányi, B. (2021). Money laundering: History, regulations, and techniques. In *Oxford Research Encyclopedia of Criminology and Criminal Justice*.
<https://doi.org/10.1093/acrefore/9780190264079.013.708>
- Zakaria, P. (2023). *Financial inclusion to digital finance risks: A commentary on financial crimes, money laundering, and Fraud. In Financial Technologies and DeFi: A Revisit to the Digital Finance Revolution*. Cham: Springer International Publishing.