جرائم غسيل الأموال الرقمية بالعملات المشفرة: دراسة تحليلية قانونية وتقنية في ضوء التشريعات الدولية والوطنية

م.م. ميادة محمد راضي
طالبة دكتوراه في جامعة طهران / مجمع الفارابي
كلية الحقوق
Meada1234556@gmail.com

د. مير خليلي
ا.د. في جامعة طهران / مجمع الفارابي/ كلية الحقوق
mirkhalili@ut.ac.ir

الكلمات المفتاحية: جرائم ، غسيل الاموال ،العملات الرقمية، العملات المشفرة ، المشرع، المحلي والدولي.

كيفية اقتباس البحث

راضي ، ميادة محمد، مير خليلي ، جرائم غسيل الأموال الرقمية بالعملات المشفرة: دراسة تحليلية قانونية وتقنية في ضوء التشريعات الدولية والوطنية ،مجلة مركز بابل للدراسات الانسانية، شباط ٢٠٢٦، المجلد:١٦ ،العدد:٢ .

هذا البحث من نوع الوصول المفتوح مرخص بموجب رخصة المشاع الإبداعي لحقوق التأليف والنشر (Creative Commons Attribution) تتيح فقط للآخرين تحميل البحث ومشاركته مع الآخرين بشرط نَسب العمل الأصلي للمؤلف، ودون القيام بأي تعديل أو استخدامه لأغراض تجارية.

مفهرسة في Indexed
IASJ

مسجلة في Registered
ROAD

Cryptocurrency Money Laundering Crimes: A Legal and Technical Analytical Study in Light of International and National Legislation

Assistant lecturer
Mayada Mohammed Radhi
PhD student at Tehran University / Farabi Complex, Faculty of Law

Dr. Mir Khalili
Professor at the University of Tehran / Farabi Complex / Faculty of Law

Keywords : Crimes, money laundering, digital currencies, cryptocurrencies, legislator, local and international.

How To Cite This Article
Radhi, Mayada Mohammed, Mir Khalili, Cryptocurrency Money Laundering Crimes: A Legal and Technical Analytical Study in Light of International and National Legislation,Journal Of Babylon Center For Humanities Studies, February 2026,Volume:16,Issue 2.

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Abstract:

The rapid expansion of cryptocurrency use has led to the emergence of new types of economic crimes, most notably organized, cross-border digital money laundering. This crime relies on a complex technical architecture that utilizes tools that enable anonymity, multi-stage disguise, and instant cross-border transfers. This makes it difficult for judicial and regulatory authorities to trace suspicious funds or accurately establish their true and real source. This study aims to provide a comprehensive analytical treatment of cryptocurrency money laundering from a legal and technical perspective, by deconstructing the stages of the crime and identifying the methods used by perpetrators to

conceal criminal proceeds, such as smart contracts, currency mixing services, and unregulated trading platforms. The study also discusses shortcomings in national legislative structures, challenges associated with weak international cooperation, and the absence of effective digital proof systems compatible with the decentralized nature of cryptocurrencies. The study pays particular attention to the intersection of law and modern technology, and the ability of traditional legal texts to adapt to rapid digital transformations. It also addresses the risks associated with the misuse of these currencies to finance terrorism and transnational crimes. The study concludes that the current legal framework is insufficient to combat this type of crime. This requires the development of modern, flexible legislation and the expansion of the concept of criminal liability to include digital intermediaries, developers, and technical facilitators. The study calls for the development of a specialized national system to combat crypto-money laundering, based on the integration of blockchain analysis tools, the training of legal and technical personnel, and the promotion of cross-border cooperation. The study concludes that addressing digital money laundering cannot be effective unless traditional legislative approaches are reconsidered and the technical dimension is integrated into legal frameworks, in a delicate balance between protecting digital rights and maintaining the country's economic security.

الملخص:

أدى التوسع السريع في استخدام العملات المشفرة إلى نشوء أنماط جديدة من الجرائم الاقتصادية، أبرزها غسيل الأموال الرقمي المنظم والعابر للحدود الجغرافية. تستند هذه الجريمة إلى بنية تقنية معقدة تعتمد على أدوات تتيح إخفاء الهوية، والتمويه متعدد المراحل، والتحويلات الفورية العابرة للحدود، وهو ما يصعّب على الأجهزة القضائية والرقابية تعقّب الأموال المشبوهة أو إثبات مصدرها الفعلي والواقعي بشكل دقيق. تهدف هذه الدراسة إلى تقديم معالجة تحليلية شاملة لجريمة غسيل الأموال بالعملات المشفرة من منظور قانوني وتقني، من خلال تفكيك مراحل الجريمة، وتحديد الوسائل التي يستخدمها الجناة لإخفاء العائدات الإجرامية، كالعقود الذكية، وخدمات خلط العملات، ومنصات التداول غير المنظمة. كما يناقش البحث أوجه القصور في البنية التشريعية الوطنية، والتحديات المرتبطة بضعف التعاون الدولي، وغياب منظومات إثبات رقمية فعّالة تتلاءم مع الطبيعة اللامركزية للعملات المشفرة. ويولي البحث اهتمامًا خاصًا بتقاطع

القانون مع التكنولوجيا الحديثة، ومدى قدرة النصوص القانونية التقليدية على التكيف مع التحولات الرقمية السريعة، مع التطرق إلى المخاطر المرتبطة بإساءة استخدام هذه العملات في تمويل الإرهاب والجرائم العابرة للحدود. وقد توصلت الدراسة إلى أن الإطار القانوني الحالي غير كافٍ لمجابهة هذا النوع من الجرائم، مما يتطلب تطوير تشريعات حديثة مرنة، وتوسيع مفهوم المسؤولية الجنائية ليشمل الوسطاء الرقميين، والمطورين، والميسّرين التقنيين. وتدعو الدراسة إلى بناء منظومة وطنية متخصصة لمكافحة غسيل الأموال المشفّر، ترتكز على دمج أدوات تحليل سلاسل الكتل، وتدريب الكوادر القانونية والفنية، وتعزيز التعاون العابر للحدود. وتؤكد الدراسة في خاتمتها أن معالجة غسيل الأموال الرقمية لا يمكن أن تكون فعالة ما لم يُعاد النظر في مناهج التشريع التقليدية، ويُدمج البعد التقني ضمن الأطر القانونية، في توازن دقيق بين حماية الحقوق الرقمية، وصيانة الأمن الاقتصادي للدولة.

المقدمة:

في ظل التقدم المتسارع في مجال التقنية المالية والرقمنة العالمية، أصبحت العملات المشفرة (Cryptocurrencies) واحدة من أبرز الابتكارات المالية المثيرة للجدل في القرن الحادي والعشرين. هذه العملات، وعلى رأسها البيتكوين والإيثيريوم، شكّلت نقلة نوعية في مفاهيم التعاملات النقدية، إذ أتاحت إمكانيات غير مسبوقة لإجراء التحويلات المالية عبر شبكة الإنترنت دون الحاجة إلى مؤسسات مالية تقليدية، وضمن بيئة رقمية مفتوحة، لا مركزية، وآمنة تقنيًا من جهة، ولكنها غامضة ومجهولة الهوية من جهة أخرى.

رغم الفوائد الاقتصادية التي بشّرت بها هذه الأدوات، إلا أن الوجه المظلم لها لم يتأخر في الظهور، فقد أصبحت العملات المشفرة أداة مفضلة لشبكات الجريمة المنظمة، وغسيل الأموال، وتمويل الإرهاب، والاتجار بالبشر، والابتزاز الرقمي، وغيرها من الجرائم العابرة للحدود. ويُعزى ذلك بشكل رئيس إلى السمات التقنية الخاصة بهذه العملات: اللامركزية، إخفاء الهوية، صعوبة التتبع، قابلية التبادل السريع، وتعدد المنصات التي تتيح التداول بلا ضوابط قانونية.

إن ما يزيد من تعقيد هذه المسألة هو الفجوة التشريعية الكبيرة على الصعيدين الوطني والدولي، وضعف التعاون بين الدول، وغياب منظومة قانونية موحّدة قادرة على ضبط هذا المجال شديد السيولة.

جريمة غسيل الأموال، التي طالما اعتُبرت تحديًا حيويًا للمنظومات الاقتصادية، دخلت الآن طورًا جديدًا عبر بوابة العملات المشفرة. حيث أضحى بالإمكان تحويل الأموال الإجرامية

إلى عملات رقمية، ومزجها في محافظ رقمية متعددة، ثم إعادتها إلى النظام الاقتصادي الرسمي دون أن تترك خلفها أثرًا يُعتد به من الناحية القانونية.

من هنا تبرز أهمية تناول هذه المسألة بالبحث والتحليل؛ إذ إنها لا ترتبط فقط بجوانب اقتصادية أو تقنية، بل تمس جوهر السيادة القانونية للدول، وتضع المنظومات العدلية أمام اختبارات غير مسبوقة، تتطلب أدوات تشريعية وأمنية من طراز جديد.

وهذا ما تسعى إليه هذه الدراسة: تحليل جريمة غسيل الأموال الرقمية باستخدام العملات المشفرة، من حيث نشأتها، وسائل تنفيذها، العوامل المحفزة لها، وسبل الوقاية منها.

تنبع أهمية هذه الدراسة من تناولها لموضوع حديث ومعقد يتجاوز نطاق القانون الجنائي التقليدي، ويتمثل في جريمة غسيل الأموال باستخدام العملات المشفرة، بما يفرض تحديات جديدة على الصعيدين القانوني والتقني.

فعلى الصعيد القانوني، تكشف الدراسة عن قصور واضح في التشريعات الوطنية في مواكبة تطورات العملات المشفرة، حيث تبقى النصوص القانونية التقليدية غير قادرة على ضبط الأصول الرقمية المشفرة، مما يستدعي تطوير الأطر القانونية القائمة أو سن تشريعات متخصصة.

أما على المستوى التقني، فتوفر الدراسة فهماً معمقاً لطبيعة العملات المشفرة وآليات استخدامها في غسيل الأموال، وتسعى إلى سد الفجوة المعرفية بين القانون والتكنولوجيا من خلال تحليل منهجي يجمع بين المفاهيم التقنية والسلوك الإجرامي.

وفيما يتعلق بالأبعاد الأمنية والاقتصادية، تبرز خطورة هذه الظاهرة في تهديدها للاقتصاد الوطني، وتيسيرها لعمليات تمويل غير مشروع بطرق يصعب تتبعها، مما يجعل التصدي لها ضرورة لتعزيز الأمن المالي والاستقرار الاقتصادي.

وأخيراً، على الصعيد الأكاديمي، تسعى الدراسة إلى الإسهام في سد النقص في البحوث القانونية العربية المتخصصة في هذا المجال، وتوفير أساس علمي يدعم الباحثين والمشرعين في فهم الظاهرة ومواجهتها.

تتمحور الإشكالية الرئيسة لهذه الدراسة حول التوتر القائم بين حرية التقنية الرقمية المتمثلة في العملات المشفرة، ومتطلبات النظام القانوني والسيادة المالية. فبينما توفر هذه العملات نظامًا ماليًا لامركزيًا يتيح حرية عالية في التحويلات دون رقابة مركزية، فإنها تطرح في المقابل تحديات قانونية وأمنية جسيمة، أبرزها إمكانية استغلالها في أنشطة إجرامية مثل غسيل الأموال.

تتعارض البنية التقنية للعملات المشفرة مع أسس القانون الجنائي المالي، مثل الشفافية، إمكانية التتبع، والمسؤولية القانونية، ما يجعلها بيئة خصبة لعمليات "غسيل الأموال المشفر" التي تتسم بصعوبة الاكتشاف، وغياب الأثر الورقي، والعابرية للحدود، مما يُضعف فعالية الرقابة الوطنية والدولية.

كما تكشف الدراسة عن قصور التشريعات الحالية في مواكبة هذه الظاهرة، وضعف التعاون الدولي في مكافحتها، مما يطرح سؤالاً مركزياً: كيف يمكن مواجهة غسيل الأموال باستخدام العملات المشفرة في ظل محدودية الأطر القانونية والتقنية القائمة؟

ويتفرع عن هذا السؤال مجموعة من التساؤلات الفرعية، منها: مدى كفاية التشريعات الجنائية الحالية، كيفية التوفيق بين الخصوصية الرقمية والشفافية المالية، دور الجهات التنظيمية، وآليات تطوير أدوات قانونية وتقنية فعّالة في بيئة لامركزية.

وتسعى الدراسة إلى تحليل هذه الإشكاليات في ضوء التحولات الرقمية المتسارعة، واقتراح حلول متوازنة تضمن الأمن المالي دون المساس بالحقوق الرقمية الأساسية.

بناءً على الإشكالية المركزية، تسعى هذه الدراسة للإجابة عن سؤال رئيس يتمحور حول آليات غسيل الأموال باستخدام العملات المشفرة وفعالية الأطر القانونية في مكافحتها. ويُعد هذا السؤال مدخلاً لفهم الجريمة في بيئة رقمية لا مركزية، واستكشاف تحديات الرقابة والتنظيم.

ويتفرع عن هذا السؤال الرئيسي عدد من الأسئلة الفرعية تشمل:

١.الخصائص التقنية للعملات المشفرة التي تجعلها مناسبة لغسيل الأموال، مثل التشفير وإخفاء الهوية.:

٢.المراحل العملية للجريمة وأدواتها، مثل خلاطات العملات والمنصات اللامركزية.

٣. العوامل المؤسسية والتشريعية التي تسهم في تفشي الظاهرة، كضعف الإطار القانوني وغياب التنظيم الدولي.

٤.فعالية الإجراءات الوقائية كآليات التتبع، وتطبيقات KYC و AML، والتعاون الدولي.

٥.مدى ملاءمة العقوبات التقليدية للجريمة الرقمية، والحاجة إلى نظام قانوني جديد للتعامل مع الأصول المشفّرة.

تشكل هذه الأسئلة الإطار المنهجي للدراسة، وتوجه تحليلها المفاهيمي والتقني والقانوني للوصول إلى نتائج دقيقة وتوصيات عملية قابلة للتطبيق.

تنطلق فرضية هذه الدراسة من أن السمات التقنية للعملات المشفرة، مثل اللامركزية، وإخفاء الهوية، وصعوبة التتبع، إلى جانب القصور التشريعي والرقابي على المستويين الوطني والدولي، تهيئ بيئة مواتية لارتكاب جرائم غسيل الأموال الرقمية. وتفترض الدراسة أن فعالية مكافحتها تتطلب تطوير تشريعات متخصصة، وتفعيل أدوات الرقابة التقنية، وتعزيز التعاون الدولي.

وتُبنى هذه الفرضية على عدة مبررات تحليلية، أبرزها:

١.الطبيعة التقنية للعملات المشفرة تتيح استخدامها كأدوات تمويه مالي تتجاوز الحدود القانونية للدول، مما يحدّ من قدرة الجهات القضائية على تتبعها.

٢.قصور المنظومة القانونية القائمة في تعريف العملات المشفرة وتوصيف الجرائم المرتبطة بها، إضافة إلى غياب آليات إثبات رقمية فعّالة.

٣.ضعف البنية المؤسسية والتقنية في التعامل مع الجرائم المشفّرة، نتيجة نقص التدريب والأدوات التحليلية والربط الدولي.

٤.الحاجة إلى مقاربة شاملة للمواجهة، لا تقتصر على العقوبات، بل تشمل الوقاية القانونية والتقنية، وإلزام منصات التداول بمتطلبات مكافحة غسل الأموال، وتعزيز التنسيق العابر للحدود.

تشير هذه الفرضية إلى أن معالجة الظاهرة تتطلب استجابة متعددة الأبعاد تشمل التشريع، الرقابة، والتعاون الدولي الفعّال.

يعتمد هذا البحث منهجية متعددة الأدوات، تستجيب للطبيعة المعقدة لجريمة غسيل الأموال المشفرة، من خلال الجمع بين التحليل القانوني، التقني، والاقتصادي. وقد تم توظيف أربعة **مناهج رئيسية:**

١.**المنهج الوصفي التحليلي:** لتفكيك الظاهرة عبر تحليل مفاهيمها القانونية والتقنية، وأساليب ارتكاب الجريمة، وأدوات التمويه، والواقع التشريعي القائم، مع التركيز على الجوانب البنيوية للجريمة الرقمية.

٢.**المنهج المقارن:** لمقارنة التشريعات الوطنية والدولية في التعامل مع غسيل الأموال المشفر، واستعراض نماذج قانونية ناجحة (مثل الولايات المتحدة، ألمانيا، وسنغافورة) بهدف استنباط حلول قابلة للتطبيق محليًا.

٣.**منهج دراسة الحالة:** لتحليل قضايا واقعية تثبت أنماط الجريمة الرقمية وآليات مكافحتها، مما يعزز البُعد التطبيقي للبحث ويدعم نتائجه بتجارب عملية.

٤.**المنهجان الاستنباطي والاستقرائي:** حيث جرى الاستنباط من المبادئ القانونية العامة لفهم خصائص الجريمة المشفّرة، والاستقراء من تقارير دولية وتحقيقات جنائية لاستخلاص الاتجاهات والأساليب الشائعة.

كما استند البحث إلى مصادر موثوقة، من بينها الاتفاقيات الدولية، توصيات مجموعة العمل المالي (FATF)، القوانين الوطنية، والدراسات المحكمة، بما يضمن موضوعية النتائج وموثوقية التحليل.

تعتمد هذه الدراسة منهجًا منظمًا في عرض وتحليل موضوعها، من خلال تقسيم محكم إلى أربعة مباحث رئيسة، يُفصَّل كل واحد منها إلى مطالب محددة، بما يتيح تناول الظاهرة من زوايا متعددة، قانونية وتقنية وواقعية، وصولًا إلى تحقيق أهداف البحث والإجابة على إشكاليته المحورية.

وفيما يلي عرض تفصيلي لهندسة الدراسة:

المبحث الأول: المفاهيم والمباحث التاريخية، يُعالج هذا المبحث الإطار النظري الأولي، من خلال توضيح المفاهيم الأساسية لجريمة غسيل الأموال، وبخاصة في البيئة الرقمية. كما يستعرض نشأة العملات المشفرة وتطورها التاريخي، وعلاقتها التدريجية بنشاطات غير مشروعة.

وينقسم إلى:

المطلب الأول: التعريف بجريمة غسيل الأموال.

المطلب الثاني: نشأة العملات المشفرة وتطور استخدامها في البيئات الإجرامية.

المبحث الثاني: كيفية ارتكاب جريمة غسيل الأموال بالعملات المشفرة.

ينتقل هذا المبحث من التأطير المفاهيمي إلى التوصيف العملي، من خلال تحليل مراحل الجريمة الرقمية، والأساليب المستخدمة من قبل مرتكبيها، مثل خدمات المزج، والعقود الذكية، والمحافظ غير الحافظة.

ويتضمن:

المطلب الأول: مراحل غسيل الأموال المشفر (الإيداع – التغطية – الدمج)

المطلب الثاني: أبرز الأدوات والتقنيات المستخدمة (Mixers – DEX – Privacy Coins – NFTs)

المبحث الثالث: عوامل ارتكاب جريمة غسيل الأموال بالعملات المشفرة ، يسلط هذا المبحث الضوء على الأسباب والعوامل التي تساعد في تفشي هذه الجريمة، سواء كانت قانونية (مثل ضعف التشريعات)، أو تقنية (مثل عدم إمكانية التتبع)، أو اقتصادية واجتماعية.

ويتفرع إلى:

المطلب الأول: العوامل القانونية والرقابية.

المطلب الثاني: العوامل التكنولوجية والاقتصادية والاجتماعية.

المبحث الرابع: سبل الوقاية الظرفية والعقابية من جريمة غسيل الأموال المشفرة.

يعرض هذا المبحث مقترحات الوقاية والمكافحة، من خلال الإجراءات التقنية (مثل أدوات تحليل البلوك تشين)، والتشريعية (مثل سن قوانين متخصصة)، والعقابية (مثل تطوير المنظومة الزجرية وتجريم الأفعال الرقمية).

ويتضمن:

المطلب الأول: التدابير الوقائية الظرفية (تقنية، تنظيمية، تشريعية).

المطلب الثاني: العقوبات الزجرية والتدابير الجنائية المرافقة.

تُختتم الدراسة بعرض شامل لأهم النتائج التي توصّل إليها الباحث، إضافة إلى تقديم توصيات عملية ومقترحات تشريعية وتقنية قابلة للتطبيق، بما يسهم في تعزيز القدرة المؤسسية للدولة على مواجهة هذه الجريمة الحديثة والمعقدة.

المبحث الأول

المفاهيم والمباحث التاريخية

يُعد فهم المفاهيم الأساسية المرتبطة بجريمة غسيل الأموال بالعملات المشفرة شرطًا جوهريًا لبناء إدراك علمي سليم لبنية هذه الجريمة، وتطورها، وتداخلاتها. كما أن تتبع المسار التاريخي لظهور العملات المشفرة وتطور علاقتها بالأنشطة غير المشروعة يساعد على إدراك الخلفية الزمنية والفكرية التي تمكّن الجريمة من الظهور والتبلور في صورتها الرقمية الراهنة.

ينقسم هذا المبحث إلى مطلبين:

المطلب الأول: الإطار المفاهيمي لجريمة غسيل الأموال الرقمية بالعملات المشفرة.

المطلب الثاني: نشأة العملات المشفرة وتطور استخدامها في البيئات الإجرامية.

المطلب الأول

الإطار المفاهيمي لجريمة غسيل الأموال الرقمية بالعملات المشفرة

أولاً– مفهوم غسيل الأموال في التشريعات الوطنية والدولية:

يُعد غسيل الأموال من الجرائم المالية الكبرى ذات الطابع العالمي، والتي ترتبط ارتباطًا وثيقًا "بالفساد والجريمة المنظمة والتهرب الضريبي وتمويل الإرهاب"[١]، وهو" فعل إجرامي يهدف

إلى إخفاء المصدر غير المشروع للأموال وإعادة إدخالها في النظام المالي كأنها أموال مشروعة"[٢].

وقد تعددت تعريفات غسيل الأموال باختلاف الزاوية القانونية أو الاقتصادية أو الجنائية، ومن أبرزها:

"في التشريعات الدولية، عرّفت اتفاقية فيينا ١٩٨٨ غسيل الأموال بأنه: "تحويل الأموال مع العلم بأنها متحصلة من جريمة، بهدف إخفاء أو تمويه المصدر غير المشروع لتلك الأموال، أو لمساعدة أي شخص متورط في مثل هذه الأفعال على الإفلات من المسؤولية القانونية"[٣].

أما اتفاقية باليرمو، ٢٠٠٠ "الخاصة بمكافحة الجريمة المنظمة، فقد وسّعت مفهوم الجريمة ليشمل الإخفاء والتمويه والتحويل، وعرفت الأموال بأنها تشمل جميع الممتلكات، المادية منها وغير المادية، المنقولة وغير المنقولة"[٤].

في القانون الفرنسي، نصت المادة ٣٢٤-١ من قانون العقوبات على أن:

"غسيل الأموال هو تسهيل التبرير الكاذب لمصدر الأموال أو الدخل الناتج مباشرة أو غير مباشرة من جريمة، أو المشاركة في نقل أو تحويل أو استخدام العائدات لإخفاء مصدرها غير المشروع"[٥].

ويجمع بين هذه التعريفات أنها تشترك جميعًا في ثلاثة عناصر جوهرية:

١. وجود مال متحصل من جريمة أصلية (predicate offense).

٢. نية مرتكب الجريمة في إخفاء أو تمويه المصدر غير المشروع.

٣. سلسلة من الأفعال تهدف إلى إدماج المال في النظام المالي المشروع[٦].

ثانيًا: ماهية العملات المشفرة (Cryptocurrencies)

العملات المشفرة هي شكل من أشكال الأصول الرقمية، التي تستخدم تقنيات التشفير لتأمين المعاملات، والتحقق منها، والتحكم في إنشاء وحدات جديدة من العملة[٧]. وهي تعتمد بشكل أساسي على تقنية سلسلة الكتل (Blockchain)، وتتميز بأنها لا مركزية، وغير خاضعة لأي سلطة حكومية أو مصرف مركزي [٨].

ومن أبرز العملات المشفرة الرائجة:

Bitcoin(BTC): أول وأشهر عملة مشفرة، أُطلقت عام ٢٠٠٩ على يد شخصية مجهولة تُدعى ساتوشي ناكاموتو[٩].

Ethereum(ETH): "ثاني أكبر عملة مشفرة، تعتمد على تقنية العقود الذكية"[١٠].

Monero XMR(وZEC) (Zcash): عملات تركز على الخصوصية، ويُصعب تتبع حركتها[١١].

تتمتع العملات المشفرة بعدة خصائص تجعلها مثالية للأنشطة المالية المجهولة، منها:

الشفافية المشروطة: حيث تكون المعاملات مفتوحة، ولكن هوية المستخدمين غير معروفة.

السرعة: إذ تُنقل الأموال عالميًا في ثوانٍ.

انخفاض التكاليف: مقارنة بالتحويلات البنكية التقليدية.

صعوبة التتبع القانوني: خصوصًا مع استخدام أدوات مثل الـMixers و DEXs [١٢].

ثالثًا– دمج المفهومين – غسيل الأموال المشفّر:

ينشأ ما يُسمى بـ "غسيل الأموال المشفّر" عندما تُستخدم العملات المشفرة كوسيلة لإخفاء أو تمويه مصادر الأموال غير المشروعة، بدلاً من الطرق التقليدية مثل شراء العقارات أو استخدام شركات واجهة[١٣]. وتتم هذه العمليات عادة عبر ثلاث مراحل:

١. الإيداع (Placement): تحويل الأموال النقدية إلى عملات مشفرة.

٢. التمويه (Layering): استخدام المحافظ والعقود الذكية والمنصات اللامركزية لإخفاء الأثر.

٣. الإدماج (Integration): تحويل الأموال مرة أخرى إلى نقود أو استثمارها في مشاريع قانونية[١٤].

هذا النمط الجديد من الجريمة يتجاوز التعريفات القانونية التقليدية لغسيل الأموال، لأنه:

لا يعتمد على النظام المصرفي.

لا يترك أدلة ورقية.

يُنفذ عبر الإنترنت بالكامل، وعبر منصات غير خاضعة لأي سلطة[١٥].

المبحث الثاني

كيفية ارتكاب جريمة غسيل الأموال بالعملات المشفرة

لقد أفرز التطور الرقمي والتكنولوجي الهائل في القرن الحادي والعشرين منظومة مالية بديلة، لا تعتمد على الوسائل المصرفية التقليدية، بل تتخذ من العملات المشفرة وسيطًا رئيسًا للتعاملات المالية العابرة للحدود، والمجهولة الهوية، واللامركزية[١٦]. وعلى الرغم من الفرص الاقتصادية التي أتاحتها هذه البيئة الجديدة، إلا أنها وفّرت في ذات الوقت تربة خصبة لنمو جريمة غسيل الأموال، حيث أتاح الفضاء الرقمي أدوات وتقنيات غير مسبوقة لتعقيد عملية التتبع، وإخفاء الأثر الجرمي [١٧].

إن جريمة غسيل الأموال المشفّر باتت اليوم واحدة من أخطر صور الجريمة الاقتصادية الحديثة، وذلك لاعتمادها على تقنيات تخترق منطق الرقابة، وتتجاوز السيادة القانونية للدول[١٨]. وهي تختلف في طابعها وآلياتها عن غسيل الأموال التقليدي، رغم أنها تحتفظ بذات الجوهر: إضفاء مشروعية على أموال متحصلة من مصدر غير مشروع. غير أن ما يميزها هو البيئة التكنولوجية التي تُرتكب فيها، والأدوات التقنية المتطورة التي تدعمها.

المطلب الأول: المراحل الفنية لجريمة غسيل الأموال بالعملات المشفرة.

تتبع جريمة غسيل الأموال، سواء في صورتها التقليدية أو الرقمية، نموذجًا ثلاثيًا كلاسيكيًا يتألف من:

١. مرحلة الإيداع (Placement)

٢. مرحلة التغطية أو التمويه (Layering)

٣. مرحلة الإدماج (Integration) [١٩].

لكن في السياق المشفّر، تتجلى هذه المراحل بصورة أكثر تعقيدًا، مدعومة بأدوات رقمية تجعل اكتشاف الجريمة وتتبّع خيوطها أكثر صعوبة بكثير مما هو معتاد في النظام المالي التقليدي[٢٠].

أولًا– مرحلة الإيداع (Placement):

تُمثل هذه المرحلة الخطوة الأولى في عملية غسل الأموال، حيث يسعى الجاني إلى إدخال الأموال غير المشروعة إلى النظام المالي الرقمي، وتحويلها من حالتها النقدية أو المصرفية إلى عملة مشفرة[٢١].

-طرق الإيداع تشمل:

١.شراء العملات المشفرة نقدًا من وسطاء خارج الإطار التنظيمي الرسمي.

٢.استخدام البطاقات مسبقة الدفع أو بطاقات الهدايا لتحويل الأموال إلى حسابات على منصات التداول.

٣.الاستفادة من منصات تداول غير خاضعة للتنظيم، والتي لا تطلب من المستخدمين تقديم إثباتات هوية (No–KYC Exchanges) [٢٢].

استخدام حسابات مزيفة أو مستعارة أو حتى ما يُعرف بـ "الهويات المسروقة الرقمية"[٢٣].

ثانيًا– مرحلة التمويه أو التغطية (Layering)

تهدف هذه المرحلة إلى فصل الأموال المغسولة عن مصدرها غير المشروع عبر سلسلة من العمليات المعقدة التي تُصمم خصيصًا لتشويش عملية التتبع الرقابي، سواء عبر شبكة البلوك تشين أو الأنظمة التنظيمية[٢٤].

-أبرز وسائل التمويه:

١.التحويل المتسلسل للعملات بين محافظ متعددة تابعة لأشخاص أو هويات وهمية.

٢.استخدام خدمات المزج (Mixers / Tumblers) [٢٥].

٣.التحويل بين أنواع متعددة من العملات، خاصة تلك التي تركّز على الخصوصية، كـ: Monero (XMR)، Dash، Zcash (ZEC) [٢٦].

٤.الاستعانة بالجسور البرمجية (Blockchain Bridges) [٢٧].

٥.استخدام حسابات روبوتية (Bots) تنفذ عمليات صغيرة متكررة[٢٨].

٦.ثالثًا: مرحلة الإدماج أو الدمج (Integration).

في هذه المرحلة، يسعى الجاني إلى إعادة دمج الأموال المغسولة في الدورة الاقتصادية الرسمية، وذلك من خلال استثمارات أو إنفاق ظاهر للعيان[٢٩].

-صور الإدماج الأكثر شيوعًا:

١.تحويل العملات المشفرة إلى عملات ورقية عبر وسطاء أو صرّافات مشفرة.

٢.شراء سلع عالية القيمة مثل العقارات، اليخوت، المجوهرات، أو السيارات الفاخرة.

٣.الاستثمار في مشاريع رقمية مثل NFTs، الألعاب الرقمية، أو العقود الذكية[٣٠].

٤.الاستخدام اليومي للعملات المغسولة عبر بطاقات دفع مشفرة[٣١].

المطلب الثاني

الأدوات والتقنيات المستخدمة في تنفيذ الجريمة

أولًا: خدمات خلط العملات (Crypto Mixers / Tumblers)

وهي أدوات رقمية تقوم بدمج الأموال المشفرة من مستخدمين مختلفين في محفظة واحدة، ثم توزيعها مرة أخرى بشكل عشوائي، ما يخلق طبقة عزل بين المصدر والمستلم[٣٢].

من أشهر هذه الخدمات: Tornado Cash، Wasabi Wallet [٣٣].

ثانيًا– العملات ذات الخصوصية العالية (Privacy Coins):

هي عملات مشفرة صُممت لتُعزز إخفاء هوية المستخدم بالكامل، مما يجعل من المستحيل تقريبًا تتبع معاملات المستخدم أو معرفة أرصدته[٣٤].

- Monero: تُعد الأكثر استخدامًا في غسيل الأموال.
- Zcash: توفر معاملات محمية باستخدام zk–SNARKs.
- Dash: تقدم خدمة PrivateSend [٣٥].

ثالثًا: المنصات اللامركزية (DEXs)

تُمكّن المستخدمين من التداول المباشر بين بعضهم دون وسطاء أو قيود تنظيمية[٣٦].

أمثلة: Uniswap، PancakeSwap، Sushiswap.

رابعًا- المحافظ غير الحافظة (Non-Custodial Wallets):

محافظ رقمية لا تتحكم بها أي جهة وسيطة، بل يتحكم بها المستخدم وحده، مثل MetaMask، Trust Wallet [٣٧].

خامسًا- بروتوكولات التمويل اللامركزي (DeFi Protocols):

تُستخدم هذه البروتوكولات في الإقراض والتداول دون وسيط[٣٨]، وتُعد من الأدوات المعقّدة التي يصعب تتبعها من قبل الأجهزة الرقابية[٣٩].

المبحث الثالث

الآثار القانونية لغسيل الأموال بالعملات المشفرة

تُعد العملات المشفرة من الابتكارات المالية الحديثة التي أحدثت ثورة في عالم الاقتصاد الرقمي، ولكنها في الوقت ذاته أوجدت تحديات قانونية وأمنية متعددة، من أبرزها استخدامها في عمليات غسيل الأموال. وتتمثل الآثار القانونية لهذه الجريمة في عدد من الجوانب، من أهمها:

أولاً- المسؤولية الجنائية لمُرتكبي جريمة غسيل الأموال المشفرة:

إن استخدام العملات المشفرة في عمليات غسيل الأموال يُعَدّ فعلاً مجرمًا وفقًا للعديد من التشريعات، حتى وإن لم يتم النص صراحة على "العملة المشفرة" كوسيط مالي، إذ تعتمد القوانين على مفاهيم أوسع تشمل الأدوات الرقمية والوسائل الحديثة التي يُمكن استخدامها في إخفاء مصدر الأموال غير المشروعة[٤٠]. وقد نصت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية (باليرمو ٢٠٠٠) على تجريم غسل الأموال بكل أشكاله، ما يتيح للدول تضمين الوسائل التكنولوجية الحديثة في نطاق التجريم [٤١] .

ثانيًا- التحديات القانونية في إثبات الجريمة:

تبرز صعوبات تقنية وقانونية في إثبات جريمة غسيل الأموال بالعملات المشفرة، لا سيما بسبب الطبيعة المجهولة وغير المركزية لهذه العملات[٤٢]. إذ يصعب تعقّب العمليات المرتبطة بها بسبب استخدام تقنيات التشفير، وإمكانية استخدام "المحافظ الساخنة والباردة" وخدمات "الخلط" (Mixers) لإخفاء مصادر الأموال[٤٣]. وهذا يشكل عائقًا كبيرًا أمام جهات التحقيق والادعاء العام في تتبع الجرائم الرقمية[٤٤].

ثالثًا– دور التشريعات الوطنية والدولية في مكافحة غسيل الأموال المشفرة:

اتجهت العديد من الدول إلى إدخال تعديلات تشريعية لتشمل العملات المشفرة ضمن أدوات غسيل الأموال، حيث أصدرت بعض الدول تنظيمات تلزم منصات التداول بالحصول على تراخيص، وتطبيق إجراءات "اعرف عميلك" (KYC) و"مكافحة تمويل الإرهاب"(AML/CFT)[٤٥]. كما أصدرت مجموعة العمل المالي الدولية (FATF) إرشادات تنظم التعامل مع الأصول المشفرة وتشدد على ضرورة خضوعها للرقابة القانونية[٤٦].

رابعًا– التعاون الدولي في مكافحة الجريمة:

نظراً للطبيعة العابرة للحدود لجريمة غسيل الأموال باستخدام العملات المشفرة، أصبح التعاون الدولي ضرورة حتمية لتبادل المعلومات وتنسيق التحقيقات، خاصة مع ازدياد الجرائم السيبرانية المنظمة[٤٧]. وتلعب منظمات مثل الإنتربول، ويوروبول، ومجموعة إغمونت دورًا محوريًا في التنسيق بين الدول وتعقب الشبكات الإجرامية التي تستغل التقنيات الحديثة في غسل الأموال[٤٨].

المبحث الرابع

طرق الوقاية الظرفية والعقابية لمكافحة جريمة غسيل الأموال بالعملات المشفرة

نظرًا لطبيعة غسيل الأموال المشفر التي تتسم بالسرعة والتعقيد واللامركزية، فإن مواجهتها لا تكفي عبر العقوبات التقليدية أو التشريعات القديمة. بل تتطلب استراتيجية متعددة الأبعاد تشمل الوقاية الظرفية والعقابية، بما يتوافق مع الخصوصيات الرقمية للجريمة.

أولًا– الوقاية الظرفية:

تهدف إلى الحد من فرص ارتكاب الجريمة قبل وقوعها، وتشمل:

١. الوقاية التقنية:

- استخدام أدوات تحليل سلسلة الكتل (Blockchain Forensics) مثل Chainalysis لكشف الأنماط المشبوهة [٤٩].
- فرض إجراءات "اعرف عميلك" (KYC) و"مكافحة غسل الأموال" (AML) على منصات التداول [٥٠].
- اعتماد تقنيات الذكاء الاصطناعي لرصد المعاملات غير الاعتيادية [٥١].

٢. الوقاية التنظيمية والإدارية:

- إنشاء وحدات متخصصة بالجرائم الرقمية في الجهات الأمنية والبنوك المركزية [٥٢].
- بناء قواعد بيانات وطنية ودولية للعناوين المشبوهة وتبادلها عبر اتفاقيات أمنية [٥٣].

٣. الوقاية التشريعية:

- سنّ قوانين حديثة تنظم الأصول المشفرة وتُجرّم غسيل الأموال المشفر بشكل مستقل [٥٤].
- إلزام المنصات الرقمية بالتسجيل والامتثال الرقابي [٥٥].
- تعزيز التعاون الدولي لتبادل المعلومات وتنفيذ الأحكام الجنائية العابرة للحدود[٥٦].

المطلب الثاني

الوقاية العقابية – التشريعات الزجرية والعقوبات الجنائية

تشكل العقوبة، إلى جانب الوقاية التقنية والتنظيمية، أداة مركزية في مواجهة جريمة غسيل الأموال باستخدام العملات المشفرة. لكنها، لكي تكون فعّالة، يجب أن تُكيَّف مع طبيعة الجريمة الرقمية، وأن تتجاوز الإطار العقابي التقليدي الذي لم يعد كافيًا لردع مرتكبي الجرائم في الفضاء السيبراني.

وتنقسم الوقاية العقابية إلى جانبين تكميليين:

- الجانب التشريعي (التجريم).
- الجانب الزجري (العقوبة والتدابير الجنائية الموازية).

أولًا– الجانب التشريعي – تجريم غسيل الأموال المشفر:

١.إدراج واضح في قوانين العقوبات وغسل الأموال لا بد من التنصيص صراحةً في القوانين الجنائية على أن استخدام العملات المشفرة في تمويه أو نقل الأموال المتحصلة من الجرائم يُعد جريمة غسل أموال رقمية [٥٧].

٢.ويجب الاعتراف بالعملات المشفرة كـ "أدوات مالية محتملة لارتكاب الجريمة"، دون اشتراط أن تكون معترفًا بها رسميًا كعملة قانونية [٥٨].

٣.تعديل مفاهيم "المتحصّل الإجرامي" و"وسائل الجريمة".

٤.يجب أن تتوسع المفاهيم القانونية التقليدية لتشمل الأموال الرقمية والعملات المشفرة ضمن قائمة "عوائد الجريمة"، وأدواتها كذلك [٥٩].

وهذا يتطلب إعادة تعريف "الأموال" و"الملكية" و"النقل" و"الإخفاء" في النصوص القانونية بطريقة تراعي الخصوصية التكنولوجية لهذه الأدوات [٦٠].

٥.توسيع نطاق المسؤولية الجنائية ليشمل ليس فقط المستخدم النهائي للعملات المشفرة في الجريمة، بل أيضًا:

- مطوّري أدوات التمويه (Mixers / Tumblers) إن ثبت علمهم بالاستخدام غير المشروع [٦١].
- مديري المنصات التي تمتنع عن الإبلاغ رغم علمها أو تجاهلها المتعمّد للنشاط المشبوه [٦٢].

ثانيًا– الجانب الزجري – العقوبات الجنائية والتدابير الموازية:

١. العقوبات السالبة للحرية:

ينصح بأن تتراوح عقوبة السجن في جرائم غسيل الأموال المشفّر بين(٥ – ٢٠) سنة، مع إمكانية تشديدها إذا اقترنت الجريمة بتمويل الإرهاب، أو تمت عبر شبكة منظمة [٦٣].

العقوبة ينبغي أن تُقرَن بظروف مشددة في حال:

استخدام أدوات تعقيد إلكتروني، أو تجاوز مبلغ معين، أو إذا تم تنفيذها عبر الحدود الدولية [٦٤].

٢. الغرامات المالية العالية:

- تفرض غرامات مضاعفة لقيمة الأموال المغسولة [٦٥].
- ويُشترط أن تشمل الأموال الرقمية وليس فقط الأصول التقليدية [٦٦].

٣. المصادرة والملاحقة المالية الرقمية

- يجب السماح قانونيًا بمصادرة:
- المحافظ الرقمية، العملات المشفرة، الأصول المشتراة بها [٦٧].
- وتُعد المصادرة أداة ردعية، ووسيلة لإضعاف الحافز الاقتصادي لدى مرتكبي الجريمة [٦٨].

٤. إدراج الجناة في القوائم السوداء:

منع الجناة من التعامل مع المنصات الرقمية مستقبلاً [٦٩].

حظر فتح محافظ أو إجراء معاملات مشفّرة لمدة زمنية محددة [٧٠].

٥. المسؤولية الجنائية للشخص الاعتباري

يمكن محاسبة المؤسسات الرقمية التي تُسهّل أو تتستر على الجريمة، سواء بالامتناع عن الإبلاغ أو بالإهمال التنظيمي [٧١].

وتشمل العقوبات: تعليق الترخيص، الغرامة، الإغلاق المؤقت أو النهائي [٧٢].

ومما تقدم نلخص الى إن الوقاية من جريمة غسيل الأموال المشفرة لا تُبنى فقط على الردع، بل تتطلب بيئة قانونية مرنة، تُعيد تعريف الأدوات والمفاهيم وفق المنطق الرقمي.

ولا يمكن مواجهة هذا النوع من الجرائم إلا عبر توازي الوقاية الظرفية والتقنية، مع الردع الزجري والعقابي المتطور، في إطار قانوني منسجم مع المعايير الدولية ومتجاوب مع التحولات التكنولوجية.

الخاتمة

في خضم التحولات التقنية والاقتصادية المتسارعة التي يشهدها العالم، برزت العملات المشفرة كظاهرة مالية عابرة للأنماط التقليدية، فرضت واقعًا جديدًا على الأنظمة القانونية والمؤسسات الرقابية، واستوجبت إعادة النظر في المفاهيم الكلاسيكية المتعلقة بالجريمة الاقتصادية. وقد جاءت هذه الدراسة لتسبر أغوار أحد أخطر مظاهر هذا الواقع الجديد، والمتمثل في جريمة غسيل الأموال الرقمية بالعملات المشفرة، باعتبارها تجلٍّ معقّد للجريمة المنظمة العابرة للحدود، والمتماهية مع الفضاء السيبراني المفتوح.

لقد سعت الدراسة، بمنهج تحليلي ومقارن، إلى تفكيك البنية التقنية والقانونية لهذه الجريمة، واستجلاء خصوصياتها، ورصد مواطن الضعف التنظيمي التي تُغذّي انتشارها، سواء على المستوى الوطني أو الدولي. وتبين من خلال المباحث المتتالية أن هذه الجريمة لا تُمارَس في فراغ، بل في بيئة رقمية تُعاني من قصور تشريعي، وتفاوت رقابي، وضعف في البنية التحتية القانونية والتقنية، ما يجعلها واحدة من أكثر الجرائم استعصاءً على الاكتشاف والمساءلة.

النتائج الرئيسة

١.تمثل العملات المشفرة بيئة مثالية لعمليات غسيل الأموال، بسبب بنيتها اللامركزية، وتوفر خاصية إخفاء الهوية، وغياب الرقابة التنظيمية في العديد من الدول، مما يصعّب من إمكانية تتبع العمليات المشبوهة أو إثباتها قانونيًا.

٢.تتسم جريمة غسيل الأموال المشفر بثلاث مراحل جوهرية (الإيداع، التمويه، الإدماج)، إلا أن هذه المراحل في الفضاء الرقمي تُنفذ بأدوات معقدة تتجاوز القدرة الإجرائية للنظم القانونية التقليدية، وهو ما يجعلها أكثر فاعلية وخفاء من مثيلاتها التقليدية.

٣.أظهرت الدراسة تنامي استخدام أدوات رقمية متقدمة مثل Mixers، DEXs، Privacy Coins، والمحافظ غير الحافظة، وهي أدوات تُستخدم بشكل متكرر في إخفاء مصدر الأموال وصعوبة ربطها بأي جريمة أصلية.

٤.أبرزت الدراسة مدى اتساع الفجوة بين الواقع التقني السريع، والاستجابة التشريعية البطيئة، ما أفرز بيئة غير متوازنة بين المشرع والجريمة، وأدى إلى بروز "ملاذات رقمية آمنة" يستغلها الجناة للتحصّن من الملاحقة.

٥.بيّنت الدراسة أن السياسات العقابية القائمة لا تكفي لمواجهة غسيل الأموال المشفّر، إذ تتطلب المواجهة إعادة تعريف المفاهيم الجنائية، وتوسيع نطاق التجريم، وتكييف العقوبات مع الواقع الرقمي المعاصر.

٦.خلصت الدراسة إلى أن غياب التنسيق الدولي وعدم وجود اتفاقيات إلزامية لتبادل البيانات والملاحقة القضائية يشكل عائقًا بنيويًا في مكافحة هذا النوع من الجرائم ذات الطبيعة العالمية.

التوصيات:

١.ضرورة تطوير إطار تشريعي وطني خاص بالأصول المشفرة، يتضمن توصيفًا دقيقًا لها كوسائل مالية محتملة للجريمة، ويحدد أدوات إثبات رقمية تتماشى مع خصوصيات البلوك تشين والعملات اللامركزية.

٢.وجوب إلزام منصات التداول الرقمية بتطبيق صارم لمعايير KYC و AML، وربطها بوحدات التحري المالي، وإخضاعها لرقابة مركزية مستمرة.

٣.إنشاء وحدات قضائية وأمنية متخصصة في الجرائم الرقمية والمالية، تُزود بالكفاءات البشرية والتقنية القادرة على التعامل مع طبيعة الجريمة المشفرة.

٤.سنّ عقوبات تتناسب مع خطورة الجريمة الرقمية، تتضمن السجن المشدد، الغرامات العالية، والمصادرة الرقمية للمحافظ والأصول المرتبطة بالجريمة.

٥.توسيع المسؤولية الجنائية لتشمل المؤسسات الرقمية والميسّرين التقنيين الذين يُثبت تورطهم أو تواطؤهم مع مرتكبي الجريمة، سواء بالفعل أو الامتناع.

٦.الدعوة إلى بلورة إطار قانوني دولي موحّد يهدف إلى تسهيل التعاون القضائي، وتنفيذ أحكام المصادرة، وتسليم المجرمين في جرائم العملات المشفرة.

٧.إطلاق حملات توعوية وطنية وإقليمية تُعرّف بمخاطر التعامل غير المنضبط بالعملات المشفرة، وتوضح للمجتمع الحدود القانونية الفاصلة بين الاستخدام المشروع وغير المشروع لها.

إن غسيل الأموال المشفّر لا يمثل مجرد جريمة مالية رقمية، بل هو تحدٍ بنيوي للسيادة القانونية، والعدالة الجنائية، والحوكمة الاقتصادية في العصر الرقمي. والتعامل معه لا يمكن أن يظل حبيس الأدوات القانونية القديمة، بل يجب أن يرتقي إلى مستوى التحوّلات التقنية والواقعية الراهنة.

وعليه، فإن بناء منظومة استجابة فعالة لهذه الجريمة يقتضي تحولًا في الفهم، وتجديدًا في التشريع، وتكاملاً في الجهد المحلي والدولي، لأن مستقبل الأمن المالي لا يمكن ضمانه إلا في ظل قدرة حقيقية على ضبط الفضاء الرقمي واحتوائه قانونيًا وأخلاقيًا.

هوامش البحث:

(1) United Nations Office on Drugs and Crime (UNODC), "Money-Laundering and Globalization", 2020.

([2]) Financial Action Task Force (FATF), "Glossary of the FATF Recommendations", 2022.

([3]) United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention), 1988.

([4]) United Nations Convention against Transnational Organized Crime (Palermo Convention), 2000.

([5]) Code pénal français, Article 324-1, édition 2021.

([6]) Masciandaro, D., "Economics of Money Laundering", Journal of Money Laundering Control, Vol. 17 No. 1, 2014.

([7]) Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008.

([8]) Tapscott, D. & Tapscott, A., "Blockchain Revolution", Penguin, 2016.

([9]) Ibid.

([10]) Buterin, V., "Ethereum White Paper", 2014.

([11]) Privacy Coin Guide, CoinCenter.org, 2021.

([12]) Europol, "Cryptocurrency and Money Laundering", Internet Organised Crime Threat Assessment (IOCTA), 2022.

([13]) Chainalysis, "Crypto Crime Report", 2023.

([14]) FATF, "Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing", 2020.

([15]) Europol, "Decrypting Financial Crime in the Darknet", 2021.

([16]) Tapscott, Don & Tapscott, Alex. Blockchain Revolution. Penguin, 2016.

([17]) Europol, IOCTA Report, 2022.

([18]) FATF, Virtual Assets and AML/CFT Measures, 2021.

([19]) United Nations Office on Drugs and Crime (UNODC), 2020.

([20]) Chainalysis, Crypto Crime Report, 2023.

([21]) Financial Action Task Force (FATF), 2020.

([22]) CoinDesk, "What is a No-KYC Exchange?", 2022.

([23]) Interpol Cybercrime Directorate, Digital Identity Theft, 2021.

([24]) Europol, Decrypting Financial Crime in the Darknet, 2021.

([25]) Chainalysis, Crypto Mixing and Crime, 2023.

([26]) Privacy Coins Comparative Analysis, CoinCenter.org, 2021.

([27]) DeFi Watch, “Cross-Chain Laundering Risks”, 2023.

([28]) AML Analytics, “Bot Activity in Blockchain Transactions”, 2022.

([29]) FATF, Red Flag Indicators Report, 2020.

([30]) Deloitte, Crypto Investment and AML Risk, 2022.

([31]) CipherTrace, Crypto Payment Cards, 2023.

([32]) Europol, Internet Organised Crime Threat Assessment (IOCTA), 2022.
([33]) Chainalysis, Tornado Cash Analysis, 2022.
([34]) Monero Project Documentation, 2021.
([35]) Zcash Foundation, "Privacy Technologies Overview", 2022.
([36]) DeFi Pulse, DEX Activity Trends, 2023.
([37]) Trust Wallet Documentation, 2022.
([38]) DeFi Protocol Guide, CoinGecko, 2023.
([39]) Interpol-FATF Joint Report, "Emerging Crypto Laundering Tactics", 2023.
([٤٠]) الصاوي، محمد. (٢٠٢١). "العملات الرقمية والتحديات القانونية المعاصرة". المجلة العربية للدراسات القانونية، مج٢، عدد ١، ص٦٧.
([٤١]) اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، ٢٠٠٠، المادة ٦.
([٤٢])حميد، عبد العزيز. (٢٠٢٢). "غسيل الأموال في العصر الرقمي: دراسة تحليلية". مجلة العلوم القانونية والاقتصادية، مج١٦، عدد ٤، ص٢١٣.
([43])Albrecht, C., & Payne, E. (2021). "Bitcoin laundering: An analysis of illicit flows into digital currency services". Journal of Financial Crime, Vol. 28, No. 3, pp. 742–757.
([٤٤]) الربيعي، فاضل. (٢٠٢٣). "تحديات الإثبات في الجرائم الرقمية". مجلة القانون الجنائي الحديث، عدد ٩، ص١٣٤.
([٤٥]) الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا). (٢٠٢٣). "تنظيمات التعامل مع الأصول الرقمية في المملكة". ص٢٢.
([46])FATF (2021). "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers". Paris: Financial Action Task Force.
([٤٧])عبيد، كمال. (٢٠٢٢). "الجريمة المنظمة العابرة للحدود وأثرها على الأمن القومي". المجلة الدولية للدراسات الأمنية، مج٤، عدد ٢، ص١٠٢.
([48])Europol (2022). "Cryptocurrency Crime Report". Retrieved from: www.europol.eu
([49])Chainalysis. (2023). Crypto Crime Report.
([50])FATF. (2022). Guidance on Risk-Based Approach to Virtual Assets.
([51])Ahmed, R. (2022). "AI in Anti-Money Laundering Compliance". Journal of FinTech Law, Vol. 5(2), p. 144.
([٥٢]) عبيد، كمال. (٢٠٢٢). "الوحدات الأمنية المتخصصة في الجرائم الرقمية". مجلة الدراسات الأمنية، ع٥، ص٨٨.
([٥٣]) مجموعة إغمونت. (٢٠٢١). "تبادل المعلومات بين وحدات التحريات المالية".
([٥٤]) وزارة العدل المغربية. (٢٠٢٣). مشروع قانون مكافحة الجرائم الرقمية.
([٥٥]) البنك المركزي الأوروبي. (٢٠٢٢). Regulations on Crypto-Asset Service Providers.
([56]) INTERPOL. (2021). Global Crypto Task Force Report.

(٥٧) النوري، خالد. (٢٠٢٣). "تجريم غسيل الأموال المشفّر". المجلة القانونية العربية، مج١٩، عدد ٣، ص١٢١.

(58) European Commission. (2021). Proposal for Regulation of Crypto-Assets (MiCA).

(٥٩) فتاح، حامد. (٢٠٢٢). "إعادة تعريف الأموال في البيئة الرقمية". مجلة القضاء المعاصر، ع٩، ص٩٧.

(60) Albrecht, C. (2021). Digital Assets and Criminal Law. Oxford Publishing.

(61) U.S. Department of Justice. (2023). Prosecution of Crypto Mixing Services.

(٦٢) مكتب مكافحة الجرائم الاقتصادية – فرنسا. (٢٠٢٢). التقصير التنظيمي في منصات التشفير.

(٦٣) قانون مكافحة غسل الأموال – تونس، الفصل ٣٦ مكرر (٢٠٢٣).

(64) FATF. (2020). Red Flags Indicators for Virtual Assets.

(65) OECD. (2022). Crypto Taxation and Enforcement Report.

(٦٦)مجلة الجريمة الاقتصادية. (٢٠٢٣). "غرامات على أساس القيمة الرقمية". عدد ٧، ص٥٥.

(٦٧)منظمة التعاون القضائي الأوروبي. (٢٠٢١). مصادرة الأصول الرقمية.

(68)Al Jazeera Investigates. (2022). "Crypto Crackdowns and Confiscations."

(69) Central Bank of UAE. (2023). Blacklist Guidelines for Crypto Offenders.

(٧٠)هيئة السوق المالية السعودية. (٢٠٢٢). حظر التعامل الرقمي للمخالفين.

(٧١)الأمم المتحدة. (٢٠٢٢). مسؤولية الشركات الرقمية في الجرائم السيبرانية.

(72)European Parliament. (2022). Corporate Liability in Financial Crime.

قائمة المصادر

أولاً- الاتفاقيات الدولية والتشريعات الوطنية:

١.المملكة العربية السعودية. (٢٠١٧). نظام مكافحة غسل الأموال السعودي، الصادر بالمرسوم الملكي رقم م/٢٠ بتاريخ ٥ صفر ١٤٣٩هـ.

2.Financial Action Task Force (FATF). (2019). Guidance for a Risk-Based

3.Approach to Virtual Assets and Virtual Asset Service Providers. Retrieved from https://www.fatf-gafi.org

4.Financial Action Task Force (FATF). (2021). Second 12-Month Review of the Revised FATF Standards on Virtual Assets and VASPs. Retrieved from https://www.fatf-gafi.org

5.United Nations Office on Drugs and Crime (UNODC). (2000). United Nations Convention against Transnational Organized Crime (Palermo Convention.)

6.United Nations. (1988). United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention.(

ثانيًا: كتب أكاديمية معتمدة

1.Choo, K. K. R. (2015). Cryptocurrency and Virtual Currency: Corruption and Money Laundering/Terrorism Financing Risks?. In D. Lee (Ed.), Handbook of Digital Currency (pp. 283–307). Elsevier.

2.Houben, R., & Snyers, A. (2018). Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion. European Parliament.

3.Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

4.Tapscott, D. (2020). Financial Services Revolution: How Blockchain is Transforming Money, Markets, and Banking. Toronto: Blockchain Research Institute.

5.Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World. Penguin.

ثالثًا- أبحاث ومقالات علمية محكمة:

1.Bryans, D. (2014). Bitcoin and money laundering: Mining for an effective solution. Indiana Law Journal, 89(1), 441–472.

2.Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? Review of Financial Studies, 32(5), 1798–1853. https://doi.org/10.1093/rfs/hhz015

3.Zohar, A. (2015). Bitcoin: under the hood. Communications of the ACM, 58(9), 104–113. https://doi.org/10.1145/2701411

4.Albrecht, C., Duffin, K., Hawkins, S., & Rocha, J. M. (2019). The use of crypto currencies in the money laundering process. Journal of Money Laundering Control, 22(2), 210–216.

5.Mariano, F. (2020). Anti-money laundering regulation of cryptocurrencies: A comparative approach. Journal of Financial Regulation and Compliance, 28(1), 85–102.

6.Ruhl, C. (2022). Cryptocurrency regulation: An international overview. Harvard International Law Journal Online, 63, 31–45.

7.Moore, T., & Christin, N. (2013). Beware the middleman: Empirical analysis of Bitcoin-exchange risk. In Financial Cryptography and Data Security (pp. 25–33). Springer.

رابعًا- تقارير دولية وتقنية متخصصة:

1.International Monetary Fund (IMF). (2021). The Rise of Crypto Assets: Implications for Financial Stability. Retrieved from https://www.imf.org

2.Chainalysis. (2022). The Crypto Crime Report 2022. Chainalysis Inc. https://www.chainalysis.com

3.Chainalysis. (2023). Crypto Crime Trends 2023. Chainalysis Inc. https://www.chainalysis.com

4.Europol. (2021). Cryptocurrencies: Tracing the Evolution of Criminal Finances. Europol. https://www.europol.europa.eu

5.G7 Finance Ministers. (2021). Statement on Digital Payments and Central Bank Digital Currencies. Retrieved from https://www.g7uk.org

6.Interpol. (2020). Cryptocurrency Crime and Anti-Money Laundering Handbook. Retrieved from https://www.interpol.int

7.U.S. Department of Justice. (2020). Cryptocurrency Enforcement Framework. Cyber-Digital Task Force.

8.World Economic Forum. (2022). Crypto Crime and Cybersecurity: Global Risks and Opportunities. Retrieved from https://www.weforum.org

ترجمة المصدر العربي:

- Kingdom of Saudi Arabia. (2017). Saudi Anti-Money Laundering Law, issued by Royal Decree No. M/20 dated 5 Safar 1439 AH.