إسناد المحفظة الرقمية في إثبات جرائم غسل الأموال المرتبطة بالعملات المشفرة: دراسة تحليلية مقارنة في ضوء التشريع المقارن ومعايير FATF

Digital Wallet Attribution in Proving Cryptocurrency-Related Money Laundering: A Comparative Analytical Study in Light of Comparative Legislation and FATF Standards

أ. **نوف عبدالله محمد الكواري:** أستاذة وباحثة قانونية، جامعة لوسيل، قطر.

Ms. Nouf Abdullah Mohammed Al-Kuwari: *Lecturer and Legal Researcher, Lusail University, Qatar.*

Email: Noof.Alkuwari@hotmail.com

DOI https://doi.org/10.56989/benkj.v6i10.2142

تاريخ الاستلام:	2026-08-11	تاريخ القبول:	2026-08-30	تاريخ النشر	2026-10-01

المستخلص:

تعالج هذه الدراسة إشكالية إسناد المحفظة الرقمية إلى شخص طبيعي محدد في إثبات جرائم غسل الأموال المرتبطة بالعملات المشفرة، مع التمييز بين ثبوت المعاملة تقنيًا على سجل البلوكشين، وثبوت إسنادها شخصيًا من الناحية القانونية. وتهدف الدراسة إلى تقييم كفاية الإطار القانوني القطري في ضوء التشريعين المصري والإماراتي والقضاء الفرنسي، مع الاستعانة بنموذج تطبيقي من القضاء الأمريكي والإطار التنظيمي الأوروبي، وبيان حدود دور معايير مجموعة العمل المالي (FATF) في المجال الإثباتي الجنائي. وتعتمد الدراسة المنهج التحليلي المقارن والتأصيلي، استنادًا إلى النصوص القانونية والقضائية والتنظيمية والمصادر التقنية ذات الصلة. وتخلص إلى أن القبول العام للدليل الرقمي لا يحسم مشكلة إسناد المحفظة، وأن الامتثال لمعايير مجموعة العمل المالي (FATF)، مهما بلغ تفصيله الرقابي، لا ينشئ بذاته قواعد وطنية لحجية الدليل أو إسناده. وتقترح الدراسة إطارًا إجرائيًا يميز بين عبء التقديم وعبء الإقناع، بحيث تقدم النيابة العامة أولًا حدًا أدنى كافيًا من الأدلة الرابطة بين المتهم والمحفظة، مع بقاء عبء الإقناع النهائي بثبوت الإسناد عليها طوال الدعوى، بما يوازن بين فعالية الملاحقة الجنائية وضمانات الدفاع.

الكلمات المفتاحية: الدليل الرقمي؛ العملات المشفرة؛ غسل الأموال؛ إسناد المحفظة الرقمية؛ مجموعة العمل المالي (FATF)؛ تحليل السلسلة؛ القانون القطري.

Abstract:

This study examines the issue of attributing a digital wallet to a specific natural person in proving money-laundering offenses involving cryptocurrencies, while distinguishing between the technical establishment of a transaction on the blockchain ledger and the legal attribution of that transaction to a particular individual. The study aims to assess the adequacy of the Qatari legal framework in light of Egyptian and Emirati legislation and French jurisprudence, drawing on an applied model from U.S. jurisprudence and the European regulatory framework, and to clarify the limits of the role of the Financial Action Task Force (FATF) standards in the field of criminal evidence. The study adopts an analytical, comparative, and foundational methodology based on relevant legal, judicial, regulatory, and technical sources. It concludes that the general admissibility of digital evidence does not resolve the issue of attributing a digital wallet to a specific person, and that compliance with FATF standards, regardless of the level of regulatory detail, does not in itself establish national rules governing the evidentiary weight or attribution of such evidence. The study proposes a procedural framework that distinguishes between the burden of production and the burden of persuasion, whereby the Public Prosecution must first present a sufficient minimum threshold of evidence linking the accused to the wallet, while the ultimate burden of persuasion as to the attribution remains with the prosecution throughout the proceedings, thereby balancing the effectiveness of criminal prosecution with the guarantees of the defense.

Keywords: Digital evidence; cryptocurrency; money laundering; digital wallet attribution; FATF; chain analysis; Qatari law.

المقدمة:

أصبح الدليل الرقمي مكوّنًا محوريًا في إثبات جرائم غسل الأموال المرتبطة بالعملات المشفرة؛ إذ يتخذ جانب جوهري من النشاط والأثر الإثباتي في هذه الجرائم صورة رقمية، ولا سيما حين تُستخدم العملات المشفرة في مراحل التحويل أو الإخفاء أو التمويه، مع استمرار أهمية الأدلة المادية التقليدية في بناء الإثبات الجنائي. وقد رافق الانتشار المتسارع للعملات المشفرة، بوصفها أداة مشروعة للتداول والاستثمار من جهة، وإمكان استخدامها في إخفاء منشأ الأموال غير المشروعة من جهة أخرى، تحوّلٌ موازٍ في طبيعة الأدلة التي تُبنى عليها الدعوى الجنائية؛ فأصبح الدليل الرقمي المستمد من سجلات المعاملات أحد أهم مكونات الإثبات في هذا النوع من القضايا، بما يتسم به من خصائص تقنية تثير مسائل إثباتية تختلف في بعض جوانبها عن الأدلة الرقمية التقليدية.

وتكتسب هذه المسألة أهمية خاصة بالنسبة لدولة قطر في ضوء عاملين متزامنين: أولهما انخراطها المؤسسي في منظومة مكافحة غسل الأموال وتمويل الإرهاب الدولية، بما يشمل عضويتها في مجموعة العمل المالي لمنطقة الشرق الأوسط وشمال أفريقيا (MENAFATF) وخضوعها لآليات التقييم المتبادل ذات الصلة؛ وثانيهما أن التشريع القطري، في حدود النصوص محل الدراسة، لا يتضمن تنظيمًا خاصًا بالأدلة المتولدة عن معاملات البلوكشين تحديدًا، وإنما تخضع هذه الأدلة للأطر القانونية العامة ذات الصلة بالدليل الرقمي والمعاملات الإلكترونية. ومن ثم، تبرز أهمية الدراسة في تقييم مدى كفاية هذا الإطار لاستيعاب الخصائص الإثباتية التي تفرضها الطبيعة التقنية لهذه الجرائم، ولا سيما التمييز بين ثبوت المعاملة تقنيًا على سجل البلوكشين وبين إسناد المحفظة الرقمية والنشاط المرتبط بها إلى شخص طبيعي محدد.

إشكالية الدراسة:

تتمحور الإشكالية الرئيسة لهذه الدراسة حول التساؤل الآتي :إلى أي مدى يوفر الإطار القانوني القطري ضمانات كافية لحجية الدليل الرقمي في إثبات جرائم غسل الأموال المرتبطة بالعملات المشفرة، ومدى كفاية الإطار الإجرائي المنظم لإثبات إسناد المحفظة الرقمية إلى المتهم؟

ويتفرع عن هذا التساؤل الرئيس التساؤلان الآتيان:

1. ما حدود الدور الذي تؤديه معايير مجموعة العمل المالي (FATF) في المجال الإثباتي الجنائي، وإلى أي مدى يمكن الاستناد إليها في معالجة مسائل مشروعية الدليل الرقمي وحجيته وإسناده؟
2. إلى أي مدى تؤثر الأطر التنظيمية الأكثر تفصيلًا في معالجة إشكالية إسناد المحفظة الرقمية، وهل تظل الفجوة الإثباتية الجنائية قائمة رغم زيادة درجة التفصيل الرقابي؟

أهداف الدراسة:

1. بيان مدى كفاية الإطار القانوني القطري لقبول الدليل الرقمي في جرائم غسل الأموال المرتبطة بالعملات المشفرة، ومقارنته بالنظامين المصري والإماراتي.
2. التمييز بين الثبات التقني للمعاملة على سجل البلوكشين وثبوت الإسناد الشخصي لصاحب المحفظة، استنادًا إلى فهم منهجيات تحليل السلسلة وحدودها الاستدلالية.
3. تحديد حدود الدور الذي تؤديه معايير مجموعة العمل المالي (FATF) في المسائل المتصلة بالإثبات الجنائي، وتمييزه عن الدور الذي تؤديه القواعد الإجرائية الوطنية.
4. اختبار مدى استمرار الفجوة الإثباتية رغم اختلاف درجة التفصيل الرقابي، من خلال نموذج تطبيقي موجز من القضاء الأمريكي وإشارة مركزة إلى الإطار التنظيمي الأوروبي، دون توسيع النطاق المقارن الأساسي للدراسة.
5. اقتراح إطار إجرائي جنائي لتنظيم تقديم أدلة إسناد المحفظة الرقمية، يميز بين عبء التقديم وعبء الإقناع، بما يوازن بين فعالية الملاحقة الجنائية وضمانات المحاكمة العادلة، وتطبيقه على حالة افتراضية متكاملة.

أهمية الدراسة:

تنبع أهمية الدراسة من معالجتها إحدى أدق الإشكالات التي يثيرها الإثبات الجنائي في جرائم غسل الأموال المرتبطة بالعملات المشفرة، والمتمثلة في الانتقال من إثبات وجود المعاملة أو النشاط على سجل البلوكشين إلى إثبات إسناد المحفظة الرقمية والنشاط المرتبط بها إلى شخص طبيعي محدد. وتتجلى أهميتها العلمية في التمييز بين ثلاث مسائل مترابطة ومستقلة في آثارها القانونية، هي: مشروعية الحصول على الدليل الرقمي، وقيمته الفنية في الإثبات، وإسناده الشخصي. كما تبرز أهميتها التطبيقية في السعي إلى بناء إطار إجرائي يمكن الاستناد إليه في تقييم أدلة إسناد المحفظة الرقمية، مع الاستفادة من النماذج المقارنة والحالة الافتراضية في اختبار مدى استمرار الفجوة الإثباتية، رغم اختلاف الأطر القانونية والتنظيمية.

حدود الدراسة:

تقتصر الدراسة موضوعيًا على الجانب الإثباتي الجنائي للأدلة المرتبطة بالعملات المشفرة، وبخاصة إسناد المحفظة الرقمية، دون تناول الاختصاص القضائي الدولي أو تسليم المجرمين أو استرداد الأصول عبر الحدود. ويتركز نطاقها المقارن على قطر، ومصر، والإمارات، وفرنسا، مع الاستعانة بصورة محدودة بالقضاء الأمريكي والإطار الأوروبي لاختبار فرضية الدراسة. أما فنيًا،

فتستند الدراسة إلى منهجيات تحليل سلسلة الكتل المتاحة وقت إعدادها، مع مراعاة ما قد يطرأ عليها من تطورات تقنية تؤثر في موثوقية إسناد المحفظة الرقمية.

منهج الدراسة:

تعتمد الدراسة المنهج التحليلي المقارن، من خلال تحليل النصوص القانونية والقضائية والتنظيمية ذات الصلة ومقارنتها في الأنظمة محل الدراسة، مع الاستعانة بالمصادر التقنية اللازمة لفهم طبيعة الأدلة المستمدة من البلوكشين وآليات تحليلها. كما تستند إلى المنهج القانوني التأصيلي التحليلي (Doctrinal Legal Research)، بالرجوع إلى المصادر القانونية الأصلية، والاستعانة بالمصادر الفقهية المتخصصة بالقدر اللازم لتفسيرها وتحليلها.

هيكل الدراسة:

تنقسم الدراسة إلى خمسة مطالب؛ يتناول المطلب الأول الإطار المفاهيمي للدليل الرقمي وخصوصية أدلة البلوكشين، ويبحث المطلب الثاني حجية الدليل الرقمي والسلطة التقديرية للقاضي الجنائي، ويتناول المطلب الثالث مشروعية الدليل الرقمي وأثر صفة القائم بالحصول عليه، ويُخصَّص المطلب الرابع لبيان حدود دور معايير مجموعة العمل المالي (FATF) في المجال الإثباتي، بينما يعرض المطلب الخامس الإطار الإجرائي المقترح لإثبات إسناد المحفظة الرقمية وتطبيقه على حالة افتراضية.

الدراسات السابقة والفجوة البحثية:

تناولت أدبيات عربية سابقة موضوع الدليل الرقمي في الإثبات الجنائي بعمومه، ومن أبرزها دراسة (موسى، 2024)، وهي دراسة تعالج حجية الدليل الرقمي وسلطة القاضي التقديرية في الإطار العام، دون التوقف عند خصوصية الأدلة المتولدة عن سجل البلوكشين. وفي جانب العملات المشفرة تحديدًا، تناولت دراسة وفاء صقر دور العملات الافتراضية المشفرة في جريمتي غسل الأموال وتمويل الإرهاب من زاوية موضوعية–جنائية (أركان الجريمة وصورها)، دون الخوض في مسألة الإثبات وقواعده (Meiklejohn et al., 2013).

وعلى الصعيد الأجنبي، تنتمي هذه الدراسة إلى تقاطع منهجي بين حقلين يظهر، في حدود الأدبيات العربية التي أمكن الاطلاع عليها، أن الربط بينهما لا يزال محدودًا: القانون الجنائي المقارن من جهة، وأدبيات علوم الحاسوب المتخصصة في تحليل سلسلة الكتل (Blockchain Forensics) من جهة أخرى. وتُعد دراسة ميكلجون وآخرين لعام 2013 حول تجميع عناوين البتكوين وربطها بمستخدميها من الدراسات التقنية المبكرة والمؤثرة في تطوير منهجيات هذا الحقل (صقر، 2024).

وهي دراسة تقنية بحتة لا تناقش المسائل القانونية، لكن فهم منهجيتها ضروري لأي تحليل قانوني دقيق لحجية أدلة الإسناد؛ لأنها توضح أن ربط عنوان بمستخدم يتم عبر استدلال احتمالي (heuristics)، لا عبر يقين تقني مباشر، وهذا بالذات هو جوهر الإشكالية الإثباتية التي يعالجها هذا البحث من الزاوية القانونية. ويُلاحظ، في حدود الأدبيات العربية التي أمكن الاطلاع عليها في هذه الدراسة، حضور محدود للتحليل التقني التفصيلي لمنهجيات تحليل السلسلة وحدودها الاستدلالية، وهي فجوة بين الحقلين تُعد جزءًا من الفجوة البحثية التي يسعى هذا البحث إلى سدها.

ولم تقف الدراسة، في حدود الأدبيات العربية التي أمكن التحقق منها والاطلاع عليها، على دراسة تُفرد معالجة مستقلة لمسألة إسناد المحفظة الرقمية إلى شخص طبيعي محدد بوصفها مسألة إثباتية متمايزة عن مسألة حجية الدليل الرقمي العام، ولا دراسة تختبر بدقة حدود الدور الذي تلعبه معايير مجموعة العمل المالي (FATF) – أو الأطر التنظيمية الأكثر تفصيلًا كالإطار الأوروبي – في هذا السياق الإجرائي الجنائي تحديدًا، بالتمييز عن دورها الرقابي–الوقائي المعروف. وهذه هي الفجوة التي يسعى هذا البحث إلى معالجتها، عبر تقديم إطار تحليلي يفصل بوضوح بين ثلاث مسائل غالبًا ما تُخلط: مشروعية جمع الدليل الرقمي، وحجيته الفنية العامة، وإسناده الشخصي إلى صاحب المحفظة.

المطلب الأول: الإطار المفاهيمي للدليل الرقمي وخصوصيته في جرائم العملات المشفرة

الفرع الأول: الإطار التشريعي المقارن لمفهوم الدليل الرقمي وحجيته

لم يضع المشرع القطري حتى الآن تعريفًا تشريعيًا صريحًا لمصطلح (الدليل الرقمي) بذاته، لكن قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014 (المعدَّل بالقانون رقم (11) لسنة 2025) يتضمن نصًا مؤداه عدم جواز استبعاد أي دليل ناتج عن وسيلة من وسائل تقنية المعلومات أو أنظمتها أو شبكاتها لمجرد طبيعته الرقمية (قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014، المادة 15).

كما أوجب هذا القانون على مزود الخدمة، بمقتضى المادة (5/21)، أن يتعاون مع الجهة المختصة ويساعدها في جمع أو تسجيل المعلومات والبيانات الإلكترونية وبيانات المرور، بناءً على أمر صادر إليه من الجهات القضائية، وهو التزام يقع، بحسب صريح النص، على مزود الخدمة تنفيذًا لأمر قضائي، لا تخويلًا مباشرًا للنيابة العامة بإصدار أمر الجمع والتسجيل ابتداءً، خلافًا لما قد يوحي به اختصار هذا النص في بعض الكتابات (قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014، المادة 21، البند 5).

ولا يقتصر الإطار القطري ذو الصلة على قانون مكافحة الجرائم الإلكترونية، إذ يتضمن مرسوم بقانون رقم (16) لسنة 2010 بشأن المعاملات والتجارة الإلكترونية قواعد عامة تتصل بحجية البيانات الإلكترونية. فقد قررت المادة (25) منه عدم استبعاد المحرر أو المستند أو المعاملة من الإثبات لمجرد وروده في شكل رسالة بيانات، ولو لم يكن في شكله الأصلي، إذا كان هو الدليل الوحيد الذي يمكن أن يحصل عليه الشخص المتمسك به؛ بينما أوجبت المادة (26)، عند تقدير حجيته، مراعاة ظروف إنشائه وتخزينه وتوصيله، ومدى المحافظة على سلامته، والظروف التي جرى في ظلها تحديد منشئ رسالة البيانات (مرسوم بقانون رقم (16) لسنة 2010 بإصدار قانون المعاملات والتجارة الإلكترونية، المادتان 25–26).

ومع ذلك، تظل هذه الأحكام عامة ولا تعالج بصورة خاصة إسناد عنوان أو محفظة على شبكة بلوكشين إلى شخص طبيعي معين.

ويجدر التمييز بين هذا الإطار العام للدليل الرقمي وبين قانون مكافحة غسل الأموال وتمويل الإرهاب الصادر بالقانون رقم (20) لسنة 2019، المعدَّل بالمرسوم بقانون رقم (19) لسنة 2021، ثم بالقانون رقم (18) لسنة 2025، وهو القانون الذي يحدد الركن الشرعي لجريمة غسل الأموال ذاتها؛ وتتكامل هذه التشريعات، في حدود نطاق تطبيق كل منها، في تكوين الإطار القانوني ذي الصلة بالدليل الرقمي في هذا النوع من الجرائم، بينما يظل قانون مكافحة غسل الأموال وتمويل الإرهاب هو التشريع الموضوعي الذي يحدد جريمة غسل الأموال وأحكامها. وكل هذه الأطر عامة بطبيعتها، ولا يتضمن أيٌّ منها تعريفًا مستقلًا للدليل الرقمي المتولد عن دفتر الأستاذ الموزع تحديدًا (قانون مكافحة غسل الأموال وتمويل الإرهاب رقم (20) لسنة 2019).

وفي المقابل، عرّف القانون المصري رقم (175) لسنة 2018، في المادة (1)، الدليل الرقمي بأنه المعلومات الإلكترونية ذات القوة أو القيمة الثبوتية والمخزنة أو المنقولة أو المستخرجة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها. كما قررت المادة (11) من القانون ذاته للأدلة المستمدة أو المستخرجة من الوسائل التقنية القيمة والحجية المقررة للأدلة الجنائية المادية متى استوفت الشروط الفنية المنصوص عليها في اللائحة التنفيذية (قانون مكافحة جرائم تقنية المعلومات رقم (175) لسنة 2018).

أما المشرع الإماراتي، فلم يضع في المرسوم بقانون اتحادي رقم (34) لسنة 2021 تعريفًا مستقلًا للدليل الرقمي على غرار المشرع المصري، وإنما تناول حمايته من العبث أو الإخفاء؛ إذ جرّمت المادة (18) إخفاء الأدلة الرقمية أو العبث بها بقصد إعاقة عمل جهات البحث والتحري أو التحقيق أو الجهات المختصة الأخرى (المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية).

أما في قطر، فلا يتضمن الإطار القانوني تعريفًا صريحًا ومستقلًا للدليل الرقمي على غرار التشريع المصري، ولا نصًا عقابيًا خاصًا بحمايته من التلاعب على نحو ما قرره التشريع الإماراتي؛ دون أن يحول ذلك دون قبوله في الإثبات استنادًا إلى عموم النصوص ذات الصلة ومبدأ حرية الإثبات، على النحو الذي سيُبيَّن في المطلب الثاني.

الفرع الثاني: البنية التقنية لسجل البلوكشين وأنواع المحافظ الرقمية

يقتضي البحث في حجية الأدلة المرتبطة بالعملات المشفرة فهمًا واضحًا لبنيتها التقنية وآليات عملها؛ ذلك أن خصائصها الإثباتية ترتبط ارتباطًا وثيقًا بالطريقة التي تُنشأ بها المعاملات وتُسجّل وتُتحقق من صحتها على شبكة البلوكشين، بما يجعل الإحاطة بهذه البنية مدخلًا ضروريًا لتقدير قيمتها القانونية في الإثبات الجنائي. فسجل البلوكشين يقوم، في صورته العامة، على سجل موزع تُجمع فيه المعاملات في كتل مترابطة باستخدام دوال التجزئة التشفيرية (Cryptographic Hash Functions)، بحيث يؤدي تغيير بيانات كتلة سابقة إلى تغير بصمتها التجزئية والإخلال بترابطها مع الكتل اللاحقة، الأمر الذي يجعل تعديل السجل بعد تأكيده شديد الصعوبة عمليًا وفقًا لبنية الشبكة وآلية الإجماع التي تعتمدها.

وتمنح هذه الخاصية سجل البلوكشين درجة مرتفعة من مقاومة التلاعب (Tamper Resistance)، ويشار إليها عادة في الأدبيات التقنية بخاصية الثبات (Immutability). غير أن قيمتها الإثباتية ينبغي ألا تُفهم على أنها قرينة بذاتها على صحة جميع الوقائع المرتبطة بالمعاملة؛ فهي تعزز، في المقام الأول، الثقة في سلامة البيانات المسجلة وعدم تعديلها بعد تثبيتها، ولا تثبت وحدها هوية الشخص الذي أجرى المعاملة أو الظروف الخارجية التي أحاطت بها. وهنا يظهر الفارق الجوهري بين ثبات المعاملة على السلسلة وإسنادها إلى شخص معين.

ويقصد بإسناد المحفظة الرقمية، لأغراض هذا البحث، إقامة رابطة إثباتية كافية بين شخص معين وبين سيطرته الفعلية على وسائل التصرف في الأصول المرتبطة بالمحفظة أو العنوان الرقمي وقت المعاملة محل الاتهام، بما يسمح بإسناد التصرف إليه، دون أن يستلزم ذلك بالضرورة إثبات ملكيته القانونية للمحفظة.

فالمعاملات المسجلة على شبكات البلوكشين العامة لا تظهر، في الأصل، بأسماء الأشخاص، وإنما ترتبط بعناوين رقمية (Addresses) تُستخدم في إرسال الأصول الرقمية واستقبالها، وتقوم السيطرة على الأصول عادة على حيازة المفاتيح أو بيانات الاعتماد اللازمة للتصرف فيها. ولهذا توصف كثير من شبكات البلوكشين بأنها ذات هوية مستعارة (Pseudonymous) لا مجهولة الهوية بالضرورة، إذ يمكن في بعض الحالات ربط العناوين بهويات حقيقية من خلال معلومات خارج السلسلة (Off-chain Data) ووسائل التحليل الفني.

وفي هذا السياق، يكتسب التمييز بين المحافظ الحاضنة (Custodial Wallets) والمحافظ الذاتية أو غير الحاضنة (Non-Custodial / Self-Hosted Wallets) أهمية إثباتية خاصة. ففي الحالة الأولى، يتولى مقدم خدمة (كمنصة تداول أو مزود خدمات أصول افتراضية) حفظ المفاتيح أو التحكم في الأصول نيابة عن العميل، وقد يخضع، بحسب النظام القانوني المنطبق عليه، لالتزامات التعرف على العميل والتحقق من هويته (KYC) والاحتفاظ ببياناته. ومن ثم قد تتوافر لديه معلومات خارج السلسلة تساعد جهات التحقيق على الربط بين نشاط معين وحساب مستخدم محدد، دون أن يعني ذلك بالضرورة أن كل عنوان ظاهر على البلوكشين مخصص حصريًا لذلك المستخدم.

أما في المحافظ الذاتية، فيتولى المستخدم بنفسه الاحتفاظ بوسائل التحكم في أصوله الرقمية، دون وجود جهة حاضنة تحتفظ ببيانات هويته استنادًا إلى علاقة تعاقدية معه. ومن ثم، يصبح الانتقال من إثبات إجراء معاملة بواسطة عنوان معين على شبكة البلوكشين إلى إثبات أن شخصًا طبيعيًا محددًا كان يسيطر على ذلك العنوان وقت تنفيذها مسألة أكثر تعقيدًا؛ إذ قد يتطلب إثبات هذا الإسناد الجمع بين نتائج تحليل السلسلة وأدلة أخرى مستقلة من خارجها. وتزداد صعوبة الإسناد في بعض البيئات اللامركزية، وكذلك عند استخدام تقنيات تعزيز الخصوصية، تبعًا لطبيعة كل تقنية وبنيتها وآلية عملها.

الفرع الثالث: تقنيات تحليل السلسلة وحدود الإسناد الشخصي

تمثل تقنيات تحليل السلسلة (Chain Analysis) إحدى الوسائل المستخدمة لمعالجة صعوبة تحديد هوية أصحاب عناوين البلوكشين، إذ تعتمد على تحليل أنماط المعاملات والعلاقات بين العناوين لتجميع ما يُرجح خضوعه لسيطرة كيان واحد. وتظل نتائجها احتمالية لا يقينية، لاعتمادها على مؤشرات استدلالية قابلة للتقييم، لا على إثبات مباشر للهوية، وقد أرست الدراسة التأسيسية في هذا الحقل قاعدتين استدلاليتين رئيستين شكّلتا أساسًا مبكرًا ومؤثرًا في تطوير منهجيات تحليل معاملات البتكوين (Meiklejohn et al., 2013).

وإن تطورت أدوات التحليل اللاحقة وأضيفت إليها منهجيات وبيانات مساندة أخرى: الأولى تقوم على افتراض أن العناوين التي تُستخدم معًا كمدخلات في المعاملة الواحدة تخضع لسيطرة كيان واحد، لأن توقيع المعاملة يستلزم حيازة المفاتيح الخاصة لجميع هذه العناوين في آن واحد، والثانية تقوم على تتبع (عناوين الباقي) التي قد تنشئها برمجيات المحافظ لاستقبال الفارق بين قيمة المدخلات والقيمة المحولة، والتي يُرجَّح عودتها إلى المرسل الأصلي نفسه. ويمكن باستخدام هذه الاستدلالات، إلى جانب منهجيات وبيانات مساندة أخرى، تجميع عدد من العناوين في مجموعات يُرجح خضوعها لسيطرة كيان واحد، ثم محاولة ربط بعض هذه المجموعات بكيانات معروفة من خلال معلومات خارج

السلسلة، بما في ذلك البيانات المتاحة لدى مزودي الخدمات الخاضعين لالتزامات التعرف على العميل.

تظل القيمة الإثباتية لهذه المنهجيات محكومة بطبيعتها الاستدلالية الاحتمالية؛ إذ قد تتراجع دقتها عند استخدام تقنيات الخلط وتعزيز الخصوصية، مثل (CoinJoin)، أو عند اختلاف أنماط المعاملات عن الافتراضات التي تقوم عليها استدلالات السيطرة المشتركة وعنوان الباقي. كما تزداد صعوبة الإسناد في المحافظ الذاتية والمنصات اللامركزية التي لا تخضع لالتزامات «اعرف عميلك»، وإن أمكن استكماله بعناصر فنية أو خارجية، كضبط جهاز يحمل مفتاحًا خاصًا. ومن ثم، فإن ثبوت المعاملة على سجل البلوكشين لا يستتبع بذاته ثبوت إسنادها إلى شخص معين، ما لم تدعمه أدلة كافية تربط النشاط به.

المطلب الثاني: حجية الدليل الرقمي والسلطة التقديرية للقاضي الجنائي

الفرع الأول: مبدأ حرية الإثبات وخضوع الدليل الرقمي له

يخضع الدليل الرقمي في الأنظمة التي تأخذ بمبدأ حرية الإثبات الجنائي، ومنها النظام القطري، للسلطة التقديرية للقاضي في قبوله وتقييمه، مع مراعاة الضمانات الإجرائية التي تكفل للدفاع الاطلاع عليه ومناقشة أساسه الفني والطعن فيه. وتكتسب الخبرة الفنية أهمية خاصة في أدلة البلوكشين؛ نظرًا إلى الطبيعة الاحتمالية لمنهجيات تحليل السلسلة، بما يستلزم تقييم منهجية التحليل ودرجة موثوقيتها، لا الاكتفاء بنتيجتها النهائية. وفي حين تخضع الخبرة في قطر للقواعد العامة دون تنظيم خاص بخبرة تحليل البلوكشين، ربط المشرع المصري حجية الدليل الرقمي باستيفاء الشروط الفنية المقررة في اللائحة التنفيذية للقانون رقم (175) لسنة 2018. ويكشف ذلك عن أهمية وضع معايير أكثر تحديدًا لتأهيل الخبرة المتخصصة في تحليل سلسلة الكتل، بما يعزز موثوقية الدليل وضمانات مناقشته أمام القضاء.

ويقدم القضاء الأمريكي نموذجًا تطبيقيًا دالًا على قوة أدلة البلوكشين حين تقترن بدليل مادي مساند؛ ففي قضية الولايات المتحدة ضد روس أولبريخت، مؤسس ومدير منصة «طريق الحرير» (Silk Road) المظلمة، التي أيدت فيها محكمة الاستئناف الفيدرالية للدائرة الثانية الإدانة، United States v. Ulbricht (2017).

اعتمدت النيابة الفيدرالية على تحليل سجل البلوكشين لربط مدفوعات بالبتكوين بمحافظ رقمية عُثر عليها فعليًا على حاسوب المتهم الشخصي عند إلقاء القبض عليه وهو ظرف عزّز الإسناد الشخصي بدرجة كبيرة، إذ لم يعد الاستدلال قائمًا على تحليل السلسلة مجردًا، وإنما اقترن بعناصر رقمية ومادية تربط المتهم بالنشاط محل الاتهام. وتبرز القضية من هذه الزاوية أهمية تضافر تحليل

السلسلة مع أدلة مستقلة خارجها عند بناء الإسناد الشخصي. ولا تُستحضر هذه القضية بوصفها مصدرًا لقاعدة عامة في إسناد المحافظ الرقمية، وإنما كنموذج تطبيقي يبين أهمية تضافر الدليل التقني مع الأدلة الرقمية والمادية الأخرى في بناء الإسناد الشخصي، فالقوة الإثباتية في هذه القضية لم تكن مصدرها تحليل السلسلة وحده، بل اقترانه بدليل مادي مستقل. وتبقى الحالة الأصعب حيث يقتصر الدليل على تحليل السلسلة دون سند مادي مساند، وهي الحالة التي لم يقف البحث، في حدود النصوص والأحكام المنشورة التي أمكن الاطلاع عليها في الأنظمة الثلاثة محل المقارنة، على معيار خاص واضح لمعالجتها – محل المعالجة التفصيلية في المطلب الخامس من هذه الدراسة.

المطلب الثالث: مشروعية الدليل الرقمي وأثر صفة القائم بالحصول عليه

الفرع الأول: مضمون شرط المشروعية

تخضع مشروعية الدليل الذي تحصل عليه سلطات التحقيق أو الضبط للضمانات الإجرائية المقررة قانونًا، ويترتب على مخالفتها الأثر الذي يحدده النظام القانوني في قبول الدليل أو حجيته. وتبرز الإشكالية في الدليل الرقمي عند استخدام الإكراه لفك التشفير أو الكشف عن المفتاح الخاص، أو تجاوز صلاحيات الضبط بالدخول إلى المحفظة أو منصة التداول دون إذن لازم. وتزداد أهميتها في المحافظ الذاتية (Non-Custodial)، التي قد يتطلب الوصول إليها الحصول على المفتاح الخاص أو عبارة الاسترداد (Seed Phrase)، بما يثير مسألة الحق في عدم تجريم النفس (Privilege Against Self-Incrimination).

ولا تتضمن التشريعات القطرية والمصرية والإماراتية محل المقارنة نصًا خاصًا يحسم مدى جواز إلزام المتهم بالإفصاح عن مفتاحه الخاص أو عبارة الاسترداد، وما إذا كان ذلك يمس حقه في عدم تجريم نفسه. وتمثل هذه المسألة فجوة تشريعية تستحق معالجة مستقلة، وتكتفي الدراسة بالإشارة إليها دون تفصيل؛ التزامًا بنطاقها الموضوعي.

الفرع الثاني: صفة القائم بالحصول على الدليل وأثرها في تقدير مشروعيته

يتباين تقدير أثر عدم مشروعية وسيلة الحصول على الدليل في الفقه والقضاء المقارن تبعًا لصفة القائم بالحصول عليه؛ إذ يُميَّز في هذا السياق بين الدليل الذي تحصل عليه السلطة العامة في إطار مباشرتها لاختصاصاتها، والدليل الذي يحصل عليه فرد بصفته الخاصة ثم يقدمه إلى القضاء. ويترتب على هذا التمييز اختلاف في تقدير أثر عدم مشروعية وسيلة الحصول على الدليل ومدى انعكاسها على قبوله وقيمته الإثباتية. ويجد هذا التمييز تطبيقًا في القضاء الفرنسي؛ فقد قررت الغرفة الجنائية لمحكمة النقض الفرنسية، في حكمها الصادر في 15 يونيو 1993، عدم استبعاد الدليل الذي يقدمه الخصوم لمجرد الحصول عليه بطريقة غير مشروعة أو غير نزيهة، وإنما يخضع

لتقدير القاضي (Cour de cassation, chambre criminelle, 15 juin 1993, n° 92-82.509).

وأنه لا يوجد نص قانوني يجيز للقضاة الجنائيين استبعاد وسائل الإثبات التي يقدمها الخصوم لمجرد الحصول عليها بطريقة غير مشروعة أو غير نزيهة، وإنما عليهم تقدير قيمتها الثبوتية، عملًا بالمادة (427) من قانون الإجراءات الجنائية الفرنسي، التي تكرس مبدأ حرية الإثبات الجنائي واقتناع القاضي، مع اشتراط ألا يُبنى الحكم إلا على أدلة طُرحت في الجلسة ونوقشت حضوريًا (Code de procédure pénale, art. 427).

وأكدت المحكمة هذا الاتجاه في حكمها الصادر في 31 يناير 2012، مقررةً أن التسجيلات التي يحصل عليها فرد خاص لا تعد من أعمال التحقيق القابلة للبطلان، وإنما تخضع للمناقشة وتقدير قيمتها الإثباتية في القضية المعروفة إعلاميًا بتسجيلات كاتب منزل عائلة بيتنكور (Cour de cassation, chambre criminelle, 31 janvier 2012, n° 11-85.46).

وقضت المحكمة بأن التسجيلات التي يجريها فرد خاص لا تُعد من «أعمال أو أوراق التحقيق» القابلة للبطلان بمقتضى المادة (170) من قانون الإجراءات الجنائية ما دامت صادرة عن فرد لا عن سلطة عامة، وإنما هي وسيلة إثبات تخضع للمناقشة الحضورية كغيرها.

ولا يعني هذان الحكمان قصر شرط المشروعية على أدلة الإدانة دون البراءة، وإنما يقرران أن الدليل المقدم من فرد خاص لا يُستبعد لمجرد عدم مشروعية أو نزاهة طريقة الحصول عليه، سواء قُدم لمصلحة الاتهام أم الدفاع. ويرجع ذلك إلى اختلاف مركز الفرد عن السلطة العامة المقيدة في مباشرة صلاحياتها بالضمانات الإجرائية، مع بقاء دليل الفرد خاضعًا للمناقشة الحضورية وتقدير القاضي.

الفرع الثالث: تقييم نقدي في سياق جرائم العملات المشفرة

إن التمييز الفرنسي بين دليل السلطة العامة ودليل الفرد الخاص، رغم وجاهته في الإثبات الجنائي التقليدي، يحتاج إلى إعادة تقييم في جرائم غسل الأموال المرتبطة بالعملات المشفرة. فالإشكال في هذا السياق لا يقتصر على مشروعية الحصول على دليل قائم، وإنما يمتد إلى صعوبة الإسناد الشخصي؛ لأن سجل البلوكشين لا يكشف بذاته هوية أصحاب المحافظ، وقد يتطلب إثباتها بيانات تحتفظ بها منصات التداول أو جهات تحليل السلسلة، ولا تتاح عادةً للفرد بصورة مباشرة.

المطلب الرابع: الدور الفعلي لمعايير مجموعة العمل المالي (FATF)

الفرع الأول: طبيعة معايير FATF وتعريفاتها الأساسية

تعد مجموعة العمل المالي (FATF) منظمة حكومية دولية أُنشئت خلال قمة مجموعة السبع في باريس عام 1989، وتتمثل مهمتها في وضع معايير مكافحة غسل الأموال وتمويل الإرهاب وتعزيز التنفيذ الفعال لها. وقد عدّلت مجموعة العمل المالي التوصية رقم (15) في أكتوبر 2018 لتشمل صراحةً الأصول الافتراضية ومزودي خدماتها، واعتمدت في يونيو 2019 مذكرة تفسيرية معدلة توضح كيفية تطبيق معايير مكافحة غسل الأموال على هذا القطاع (Financial Action Task Force [FATF], n.d.).

وتعرّف هذه الوثائق (الأصل الافتراضي) (Virtual Asset) بأنه تمثيل رقمي للقيمة يمكن تداوله أو تحويله رقميًا واستخدامه لأغراض الدفع أو الاستثمار، و(مزود خدمات الأصول الافتراضية) (VASP) بأنه أي شخص طبيعي أو معنوي يزاول كنشاط تجاري واحدًا أو أكثر من أنشطة محددة (كالتبادل بين الأصول الافتراضية والعملات الورقية، أو نقل الأصول الافتراضية، أو حفظها وإدارتها) نيابة عن الغير (FATF, 2021).

ثم أصدرت المجموعة سلسلة من الإرشادات والتحديثات الدورية المتعلقة بتنفيذ معاييرها بشأن الأصول الافتراضية ومزودي خدماتها، وصولًا إلى التحديث السادس الصادر في 2025 والتحديث السابع الصادر في 2026 (FATF, 2021, 2022, 2024, 2025, 2026).

وتبين هذه الوثائق أن جانبًا رئيسًا من معايير FATF المتعلقة بالأصول الافتراضية يتركز على التنظيم والوقاية والإشراف، بما يشمل ترخيص أو تسجيل مزودي خدمات الأصول الافتراضية، والعناية الواجبة بالعملاء، وحفظ السجلات والإبلاغ عن المعاملات المشبوهة. ومع ذلك، يمتد إطار FATF الأوسع كذلك إلى وحدات المعلومات المالية وسلطات التحقيق وإنفاذ القانون والمصادرة والتعاون الدولي، دون أن يضع بذاته قواعد وطنية تفصيلية لقبول الدليل الجنائي أو تقدير حجيته أمام القضاء.

الفرع الثاني: قاعدة السفر (Travel Rule) وحدودها الإجرائية الجنائية

من أبرز الأدوات الرقابية التي استحدثتها INR.15 ما يُعرف بـ«قاعدة السفر» (Travel Rule)، ومؤداها إلزام مزودي خدمات الأصول الافتراضية بجمع وتبادل بيانات محددة عن مُرسِل ومستفيد التحويلات (كالاسم ورقم الحساب/عنوان المحفظة، وفي بعض الصياغات عنوان الإقامة أو رقم الهوية)، وفق المتطلبات والحدود التي يقررها الإطار التنظيمي المطبق، على غرار قاعدة مماثلة

معمول بها منذ عقود في التحويلات المصرفية التقليدية بموجب التوصية رقم (16) (FATF, 2021).

غير أن قاعدة السفر –رغم أهميتها الرقابية البالغة في تعزيز إمكانية التتبع– تبقى، من حيث طبيعتها القانونية، التزامًا إداريًا يقع على عاتق مزود الخدمة تجاه الجهة الرقابية المختصة، لا قاعدة إثبات جنائي بالمعنى الدقيق؛ فهي لا تنشئ بذاتها حجية قانونية للبيانات المتبادلة أمام القضاء الجنائي، ولا تحدد من يتحمل عبء إثبات صحة هذه البيانات أو نفيها إذا أنكر المتهم صلته بالمحفظة المعنية. وهذا هو بالضبط موضع الفجوة الإجرائية الجنائية التي يعالجها هذا البحث: التزام رقابي فعّال (قاعدة السفر) لا يقابله بالضرورة معيار إثباتي جنائي واضح على المستوى الوطني.

الفرع الثالث: التمييز بين المستويات القانونية ذات الصلة بمعايير FATF

يقتضي التحليل القانوني لجرائم العملات المشفرة التمييز بين ثلاثة مستويات: الالتزامات الرقابية المقررة وفق معايير مجموعة العمل المالي (FATF) لمزودي خدمات الأصول الافتراضية، وصلاحيات جهات التحقيق الوطنية في تتبع الأصول الرقمية وجمع المعلومات عنها، وقواعد قبول الدليل وحجيته أمام القضاء الجنائي. فالمستوى الأول ذو طبيعة رقابية، بينما يستند المستويان الثاني والثالث أساسًا إلى التشريعات الإجرائية والإثباتية الوطنية، وإن استفادا من أطر التعاون والمعايير التي تدعمها FATF.

ويؤدي الخلط بين هذه المستويات إلى إسناد قواعد إثباتية مباشرة إلى معايير FATF دون سند صريح منها؛ فمشروعية الحصول على الدليل وحجيته تستندان إلى النظام القانوني الوطني المختص، وإن اتفقتا مع الإطار العام الذي تدعمه تلك المعايير. ومن ثم، يختلف توافق القاعدة الوطنية مع معايير FATF عن اشتقاق القاعدة الإثباتية مباشرةً منها.

الفرع الرابع: الفجوة بين الامتثال الرقابي القطري والحجية القضائية للدليل

يوفر قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014 ومرسوم بقانون المعاملات الإلكترونية رقم (16) لسنة 2010، في تكاملهما مع أحكام قانون مكافحة غسل الأموال وتمويل الإرهاب رقم (20) لسنة 2019، أساسًا تشريعيًا عامًا صالحًا، من حيث المبدأ، لقبول الدليل الرقمي المستمد من تحليل معاملات العملات المشفرة.غير أن هذا الإطار يبقى – في تقدير هذا البحث – قاصرًا عن معالجة خصوصية أدلة العملات المشفرة من وجهين: غياب إطار إجرائي واضح لتنظيم إثبات إسناد المحفظة الرقمية إلى المتهم؛ وغياب تنظيم إجرائي خاص يراعي الخصائص الفنية للأدلة المستمدة من دفتر الأستاذ الموزع، ولا سيما سلامة الاستخراج وسلسلة العهدة ومنهجية التحليل. وهذه فجوة إجرائية جنائية داخلية لا يسدها الامتثال الرقابي لمعايير FATF مهما بلغت درجته؛ إذ لا تضع

معايير FATF، رغم امتدادها إلى مجالات الوقاية والرقابة والتحقيق المالي وإنفاذ القانون والتعاون الدولي، القواعد الوطنية التفصيلية التي تحكم قبول الدليل الجنائي أو حجيته أو إسناده أمام القضاء.

وتتأكد هذه الخلاصة عند النظر إلى أحد أكثر الأطر التنظيمية تفصيلًا في مجال الأصول المشفرة، إذ يتبين أن تطور التنظيم وتفصيله لا يكفيان، بذاتهما، لمعالجة الفجوة الإثباتية محل الدراسة وقد اعتمد الاتحاد الأوروبي لائحة نقل الأموال المعاد صياغتها رقم 1113/2023، التي تتضمن متطلبات تتعلق بالمعلومات المصاحبة لتحويلات بعض الأصول المشفرة (Regulation (EU) 2023/1113, 2023)

كما اعتمد لائحة أسواق الأصول المشفرة (MiCA) رقم 1114/2023، التي تنظم جوانب متعددة من أسواق الأصول المشفرة ومزودي خدماتها (Regulation (EU) 2023/1114, 2023).

وقد أصبحت أحكامها الخاصة بالعملات المستقرة واجبة التطبيق اعتبارًا من 30 يونيو 2024، فيما أصبحت غالبية باقي أحكامها – ومنها الإطار المتعلق بترخيص مزودي خدمات الأصول المشفرة – واجبة التطبيق اعتبارًا من 30 ديسمبر 2024. ومع ذلك، تكشف قراءة كلتا اللائحتين أن أيًّا منهما لا يتضمن قاعدة إثبات جنائي مباشرة تحدد كيفية إسناد محفظة رقمية إلى متهم بعينه، أو تنظم قبول هذا النوع من الأدلة وحجيته أمام القضاء الجنائي. وعلى الرغم من هذا التفصيل التنظيمي، لا تضع أي من اللائحتين معيارًا جنائيًا موحدًا لإسناد المحفظة الرقمية إلى شخص معين، ولا تحدد بذاتها كيفية إثبات هذا الإسناد أمام القضاء. ومن ثم، يبين النموذج الأوروبي أن زيادة التفصيل الرقابي لا تكفي بذاتها لمعالجة مسألة الإسناد الشخصي للمحفظة الرقمية.

المطلب الخامس: نحو إطار إجرائي لإثبات إسناد المحفظة الرقمية

الفرع الأول: التمييز بين عبء التقديم وعبء الإقناع

تفرّق نظرية الإثبات الجنائي المقارن عمومًا في تطبيقاتها الإجرائية على مسائل فرعية محددة كإثبات دفع أو واقعة عارضة، دون أن يمس ذلك بالقاعدة الأصولية العامة التي تظل بمقتضاها قرينة البراءة قائمة وعبء إثبات الإدانة على عاتق النيابة العامة في الدعوى الجنائية بأكملها بين مستويين من (عبء الإثبات) يفيد التمييز بينهما في صياغة آلية دقيقة ومتوازنة: عبء التقديم (Burden of Production)، ومؤداه الالتزام بتقديم حد أدنى من الأدلة الأولية على واقعة معينة بما يكفي لطرحها أمام المحكمة للمناقشة، دون أن يستلزم ذلك إثباتها إثباتًا قاطعًا؛ ويفيد التمييز بين عبء التقديم وعبء الإقناع في تنظيم بعض المسائل الإجرائية دون أن يستلزم ذلك نقل عبء إثبات

عناصر الجريمة من النيابة العامة، وهو تمييز يظهر في القضاء الأمريكي في Patterson v. (New York (1977)

ويبقى على سلطة الاتهام إثبات كل واقعة لازمة لتكوين الجريمة وفق معيار الإثبات الجنائي المقرر، وهو المبدأ الذي أكدته المحكمة العليا الأمريكية في (In re Winship (1970)

وتظل قرينة البراءة، بمقتضى هذا التمييز، سليمة تمامًا: فعبء الإقناع النهائي بثبوت التهمة بجميع أركانها – بما فيها إسناد المحفظة إلى المتهم – يبقى، ويجب أن يبقى، على عاتق النيابة العامة طوال الدعوى، وما تقترحه الآلية أدناه هو تنظيم لعبء التقديم الأولي فحسب، لا نقل لعبء الإقناع النهائي.

الفرع الثاني: الآلية المقترحة وشروط تطبيقها

1. المرحلة الأولى (عبء النيابة العامة في التقديم): إذا استندت النيابة العامة إلى دليل مستمد من البلوكشين لإسناد محفظة رقمية إلى متهم بعينه، وجب عليها أن تقدم حدًا أدنى كافيًا من عناصر الإسناد، يشمل بحسب طبيعة القضية: (أ) ما يثبت سلامة استخراج الدليل الرقمي وحفظه وتوثيق سلسلة عهدته، و(ب) تقريرًا فنيًا من مختص في تحليل بيانات البلوكشين يوضح منهجية التحليل المستخدمة وحدودها ومصادر احتمال الخطأ فيها ومستوى موثوقية الاستدلال، و(ج) ما يتوافر من بيانات خارج السلسلة، كبيانات اعرف عميلك وسجلات مزود الخدمة، أو أدلة رقمية أو مادية مستقلة تعزز إسناد السيطرة على المحفظة إلى المتهم.

2. المرحلة الثانية (انتقال عبء التقديم إلى المتهم): ومتى قدمت النيابة العامة هذا الحد الأولي الكافي من عناصر الإسناد، جاز للمتهم – دون أن يتحمل عبء إثبات براءته ودون مساس بقرينة البراءة – أن يقدم ما يكون في حوزته من عناصر محددة تنازع في صحة الإسناد أو تكشف عن احتمال بديل جدي، مع بقاء عبء الإقناع النهائي بثبوت الإسناد على عاتق النيابة العامة.

3. المرحلة الثالثة (استمرار عبء الإقناع النهائي على عاتق النيابة العامة): بصرف النظر عن نتيجة المرحلتين السابقتين، يبقى الاقتناع النهائي بثبوت الإسناد على درجة اليقين الجنائي المطلوب من اختصاص القاضي وحده، وعلى عاتق النيابة العامة إقناعه بذلك، بما يحفظ قرينة البراءة والضمانات الأساسية للمحاكمة العادلة، ويحول الآلية المقترحة إلى تنظيم إجرائي لترتيب تقديم الأدلة، لا إلى قرينة إدانة قائمة على مجرد وجود دليل بلوكشين.

الفرع الثالث: الضمانات الإجرائية للمتهم في الآلية المقترحة

تحرص هذه الآلية على تجنب عكس عبء الإثبات الجنائي بصورة تخل بضمانات المحاكمة العادلة، وذلك عبر ثلاثة ضوابط: أولها، اقتصار أثرها على مسألة فرعية محددة (إسناد المحفظة) دون أن تمتد إلى أركان الجريمة الأخرى (كالعلم بمصدر الأموال غير المشروع أو القصد الجنائي) التي تظل خاضعة للقواعد العامة لعبء الإثبات الجنائي دون أي تعديل؛ وثانيها، إلزام النيابة العامة بحد أدنى موضوعي وقابل للتحقق من التقديم (التقرير الفني وبيانات اعرفْ عميلك أو الدليل المادي المساند) قبل أن يُطلب من المتهم أي رد، بما يمنع استناد الاتهام إلى مجرد الإشارة العامة إلى «تحليل السلسلة» دون تفصيل منهجي، تفاديًا لما بيّنه الفرع الثالث من المطلب الأول من الطابع الاستدلالي الاحتمالي لا اليقيني لهذه التقنية؛ وثالثها، حفظ حق المتهم الكامل في مناقشة التقرير الفني وأساسه الفني وفق الضمانات الإجرائية المقررة، وتمكينه، عند تعذر قدرته المالية وفي الحالات التي تتوقف فيها فعالية الدفاع على الخبرة الفنية، من الاستعانة بخبرة مستقلة وفق الضمانات التي يقررها القانون، بما يكفل له فرصة فعلية لمناقشة الأساس الفني للدليل وتقديم رأي فني مضاد، وينسجم مع الشرط الإجرائي العام الذي بيّنه المطلب الثاني بشأن ضرورة تمكين الدفاع من مناقشة الدليل الرقمي وأساسه الفني وفق القواعد الإجرائية المقررة.

الفرع الرابع: تطبيق الآلية المقترحة على حالة افتراضية متكاملة

يفترض التطبيق العملي للآلية اتهام الشخص (م) بغسل أموال من خلال تحويل ما يعادل 300 ألف ريال قطري بعملة البتكوين من منصة تداول أجنبية إلى محفظة ذاتية–Non) (Custodial، ثم توزيعها على محافظ فرعية وإعادة تجميعها في محفظة يُشتبه في سيطرته عليها، دون ضبط جهاز أو مفتاح خاص مرتبط بها في حيازته.

في المرحلة الأولى، تقدم النيابة العامة تقريرًا فنيًا يبين منهجية تحليل السلسلة ودرجة موثوقيتها وحدودها، مدعومًا – متى أمكن – ببيانات «اعرف عميلك» وأدلة تربط مسار الأموال بالمحفظة النهائية. فإذا تعذر الحصول على هذه البيانات، وجب دعم الإسناد بدليل مستقل يربط المتهم بالمحفظة. ولا يكفي تحليل السلسلة وحده لنقل عبء التقديم إلى المتهم ما لم تؤيده عناصر إضافية تقدرها المحكمة.

وفي المرحلة الثانية، يجوز للمتهم منازعة الإسناد بإثارة احتمال بديل جدي، كاشتراك الغير في السيطرة على المحفظة أو وجود عيب في منهجية التحليل، وله الاستعانة بخبرة مضادة لفحص التقرير الفني ومنهجيته.

أما المرحلة الثالثة، فيقدّر القاضي مجموع الأدلة والدفوع؛ فإذا أثارت المنازعة شكًا معقولًا لم تدحضه النيابة العامة، تعين عدم ثبوت الإسناد، لبقاء عبء الإقناع النهائي عليها طوال الدعوى. أما الإنكار المجرد فلا يؤدي بذاته إلى الإدانة، التي تظل مشروطة باقتناع المحكمة بثبوت الإسناد وفق معيار الإثبات الجنائي المقرر.

ويزداد اختبار الآلية أهمية عند استخدام تقنيات الخلط، مثل(CoinJoin) ؛ إذ يتعين على النيابة بيان أثرها في منهجية التحليل ومدى موثوقية الربط بين المعاملات، أو تقديم دليل تكميلي مستقل. فإذا أغفل التقرير الفني أثر الخلط، جاز الطعن في كفايته لعدم استيفائه الحد الأدنى اللازم لإسناد المحفظة.

ويبين التطبيق أن الآلية المقترحة تنظم تسلسل تقديم أدلة الإسناد دون إنشاء قرينة إدانة جديدة؛ فلا يكفي الاستناد المجرد إلى تحليل السلسلة، كما لا يجوز تحميل المتهم عبء نفي الإسناد ابتداءً، وإنما يظل تقدير كفاية الأدلة خاضعًا لرقابة المحكمة مع بقاء عبء الإقناع النهائي على النيابة العامة.

الخاتمة:

خلصت الدراسة إلى أن التحدي الرئيس في إثبات جرائم غسل الأموال المرتبطة بالعملات المشفرة لا يكمن في ثبات المعاملة على سجل البلوكشين، وإنما في إسناد المحفظة الرقمية إلى شخص محدد؛ إذ لا يكفي الثبات التقني وحده لإثبات هذا الإسناد، ولا سيما مع الطبيعة الاحتمالية لتقنيات تحليل السلسلة. كما أظهرت المقارنة أن معايير مجموعة العمل المالي ((FATF، رغم أهميتها الرقابية ودورها في دعم التحقيق المالي والتعاون الدولي، لا تنشئ بذاتها قواعد وطنية لحجية الدليل الجنائي أو إسناده. ومن ثم، تبرز الحاجة إلى معالجة إجرائية وطنية تنظم تقديم أدلة الإسناد وتقييمها، مع التمييز بين عبء التقديم وعبء الإقناع. ويحقق الإطار المقترح توازنًا بين فعالية الملاحقة الجنائية وضمانات المحاكمة العادلة، مع بقاء عبء الإقناع النهائي على النيابة العامة وخضوع كفاية أدلة الإسناد لتقدير القضاء.

النتائج:

1. أظهرت الدراسة أن الأنظمة القطرية والمصرية والإماراتية تقبل الأدلة الرقمية من حيث الأصل، مع خضوع حجيتها وتقديرها للقواعد الوطنية للإثبات الجنائي والسلطة التقديرية للقاضي، في إطار الضمانات الإجرائية المقررة.

2. يوفر التشريع القطري أساسًا عامًا لقبول الدليل الرقمي، لكنه لا يتضمن تعريفًا تشريعيًا مستقلًا له على غرار التشريع المصري، ولا حماية عقابية مباشرة من العبث به على النحو الذي قرره التشريع الإماراتي، بما يكشف عن حاجة الإطار القطري إلى مزيد من التحديد في هذا الجانب.
3. أثبتت الدراسة أن الثبات التقني للمعاملة على سجل البلوكشين لا يستتبع ثبوت إسناد المحفظة إلى شخص معين؛ إذ تعتمد تقنيات تحليل السلسلة على استدلالات احتمالية تتفاوت موثوقيتها بحسب المنهجية المستخدمة والأدلة المساندة.
4. أظهر النموذج القضائي الأمريكي أن قوة إسناد المحفظة تزداد باقتران تحليل السلسلة بأدلة رقمية أو مادية مستقلة تربط المتهم بالنشاط محل الاتهام، بينما لم يتبين في الأنظمة العربية الثلاثة محل المقارنة وجود معيار خاص وواضح لمعالجة الإسناد القائم على تحليل السلسلة وحده.
5. كشف القضاء الفرنسي عن أهمية التمييز بين الدليل الذي تحصل عليه السلطة العامة والدليل الذي يقدمه الفرد الخاص، إلا أن هذا التمييز لا يعالج بمفرده صعوبة إسناد المحفظة الرقمية الناشئة عن الطبيعة التقنية واللامركزية للبلوكشين وعدم كشفه بذاته عن هوية أصحاب العناوين.
6. لا تنشئ معايير مجموعة العمل المالي (FATF) قواعد وطنية مباشرة لقبول الدليل الجنائي أو حجيته أو إسناده؛ إذ ينبغي التمييز بين الالتزامات الرقابية لمزودي خدمات الأصول الافتراضية، وصلاحيات جهات التحقيق الوطنية، وقواعد الإثبات التي يحكمها النظام القانوني الوطني.
7. أظهرت الدراسة أن زيادة التفصيل الرقابي، كما في الإطار الأوروبي، أو الامتثال لمعايير FATF لا يسدان بذاتهما الفجوة الإجرائية المتعلقة بإسناد المحفظة الرقمية، بما يؤكد الحاجة إلى إطار وطني يحدد متطلبات تقديم أدلة الإسناد مع بقاء عبء الإقناع النهائي على النيابة العامة.

التوصيات:

1. استحداث تنظيم إجرائي خاص، في قانون مكافحة الجرائم الإلكترونية أو في لائحة تنفيذية مستقلة، للأدلة المستمدة من تقنيات دفتر الأستاذ الموزع، يحدد متطلبات سلامة جمعها وحفظها وتوثيق سلسلة عهدتها، ويميّز بين المحافظ الحاضنة (Custodial) والمحافظ الذاتية أو غير الحاضنة (Non-Custodial)، ويضع معايير واضحة لتقييم أدلة إسناد المحافظ الرقمية إلى الأشخاص.
2. إقرار قاعدة إجرائية صريحة على غرار الآلية المقترحة في المبحث الخامس، تُلزم النيابة العامة، حين تستند إلى دليل مستمد من البلوكشين لإسناد محفظة رقمية إلى متهم، بإرفاق تقرير فني يبيّن منهجية تحليل السلسلة وحدودها، ودرجة موثوقية نتائجها، ومصادر احتمال الخطأ فيها، مدعومًا ببيانات (اعرف عميلك) أو بدليل مادي مساند، مع بقاء عبء الإقناع النهائي كاملًا على عاتق النيابة العامة.تعزيز آليات التنسيق المؤسسي بين الجهات الرقابية المعنية بمزودي

خدمات الأصول الافتراضية والنيابة العامة وجهات إنفاذ القانون، بما يكفل سرعة الحصول على بيانات العملاء والمعلومات ذات الصلة عند الحاجة إليها في التحقيق والإثبات الجنائي.

3. تعزيز التمييز في الكتابات القانونية العربية بين الدور الرقابي لمعايير FATF والأطر التنظيمية المشابهة، وبين اختصاص القانون الوطني بتنظيم قواعد الإثبات الجنائي، بما يحول دون نسبة قواعد إجرائية جنائية إلى وثائق دولية لا تتضمنها.
4. تدريب الخبراء القضائيين والمحققين على المنهجية الفعلية لتقنيات تحليل السلسلة (بما يشمل حدودها الاستدلالية، الاحتمالية) بدل الاكتفاء بالإشارة العامة إليها بوصفها أداة إثبات قاطعة، بما يعزز جودة الاقتناع القضائي المؤسَّس على أساس فني سليم.
5. استحداث قاعدة تأهيل إجرائية خاصة بخبراء تحليل سلسلة الكتل، تميزهم عن الخبراء المعلوماتيين العموميين، على أن تحدد معايير موضوعية للتأهيل تراعي المؤهلات العلمية والخبرة العملية في تحليل بيانات البلوكشين، والمعرفة بالمنهجيات المستخدمة وحدودها ومصادر الخطأ فيها، والقدرة على عرض نتائج التحليل بصورة قابلة للفحص والمناقشة القضائية.

قائمة المصادر والمراجع:

أولًا: التشريعات القطرية والعربية

1. قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014 (قطر)، المعدل بالقانون رقم (11) لسنة 2025.
2. قانون مكافحة غسل الأموال وتمويل الإرهاب رقم (20) لسنة 2019 (قطر)، المعدل بالمرسوم بقانون رقم (19) لسنة 2021 والقانون رقم (18) لسنة 2025.
3. مرسوم بقانون رقم (16) لسنة 2010 بإصدار قانون المعاملات والتجارة الإلكترونية (قطر).
4. قانون مكافحة جرائم تقنية المعلومات رقم (175) لسنة 2018 (مصر).
5. المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية (الإمارات العربية المتحدة).

ثانيًا: المراجع العربية

1. موسى، محمد محمد عبد الظاهر. (2024). القيمة الثبوتية للدليل الرقمي وضوابط اقتناع القاضي الجنائي. مجلة البحوث القانونية والاقتصادية، 36(2)، 226–336 . https://doi.org/10.21608/lsej.2024.255692.1064

2. صقر، وفاء محمد مصطفى. (2024). دور العملات الافتراضية المشفرة في جريمتي غسل الأموال وتمويل الإرهاب. مجلة البحوث الفقهية والقانونية، (46)، 1405–1503. https://doi.org/10.21608/jlr.2024.287819.1436

ثالثًا: تشريعات الاتحاد الأوروبي

1. Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849, Official Journal of the European Union, L 150, 1–39.
2. 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, Official Journal of the European Union, L 150, 40–205.

رابعًا: التشريع الفرنسي

1. Code de procédure pénale (France), art. 427.

خامسًا: المراجع الأجنبية والتقارير الدولية

1. Financial Action Task Force. (2019). International standards on combating money laundering and the financing of terrorism & proliferation: The FATF recommendations (Recommendation 15 and Interpretive Note to Recommendation 15).
2. Financial Action Task Force. (2021). Updated guidance for a risk-based approach to virtual assets and virtual asset service providers.
3. Financial Action Task Force. (2022). Targeted update on implementation of FATF's standards on virtual assets and virtual asset service providers.
4. Financial Action Task Force. (2024). Virtual assets: Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers.

5. Financial Action Task Force. (2025). Sixth targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers.
6. Financial Action Task Force. (2026). Seventh targeted update on implementation of the FATF standards on virtual assets/VASPs.
7. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A fistful of bitcoins: Characterizing payments among men with no names. In Proceedings of the 2013 Internet Measurement Conference (IMC '13) (pp. 127–140). Association for Computing Machinery. https://doi.org/10.1145/2504730.2504747

سادسًا: الأحكام القضائية

الأحكام الفرنسية:

1. Cour de cassation, chambre criminelle, 15 juin 1993, n° 92-82.509, Bulletin criminel, 1993, n° 210, p. 530.
2. Cour de cassation, chambre criminelle, 31 janvier 2012, n° 11-85.464.

الأحكام الأمريكية:

1. In re Winship, 397 U.S. 358 (1970).
2. Patterson v. New York, 432 U.S. 197 (1977).
3. United States v. Ulbricht, 858 F.3d 71 (2d Cir. 2017).