

الحجية الإثباتية لمخرجات تحليل البلوك تشين في تتبع المعاملات المرتبطة بجرائم العملات المشفرة: دراسة

تحليلية في التشريع الإماراتي

د. هدى خلفان سالم الشامسي¹

Dr. Huda Khalfan Salem Alyan Alshamsi

دكتورة في القانون العام الدولي

جامعة عجمان، الإمارات العربية المتحدة

alshamsi_2000_ad@hotmail.com

DOI: <https://doi.org/10.65040/remeye.2026.11.v02n30.02>

This work is licensed under a Creative Commons Attribution 4.0 International License

<https://creativecommons.org/licenses/by/4.0/>

الملخص:

تبحث هذه الدراسة الحجية الإثباتية للنتائج التقنية المستخلصة من تحليل معاملات البلوك تشين المرتبطة بجرائم العملات المشفرة، وتهدف إلى تحديد مركزها القانوني والضوابط اللازمة لقبولها وتقدير قوتها في الإثبات الجنائي وفق التشريع الإماراتي. واعتمدت المنهج التحليلي من خلال دراسة النصوص المنظمة للدليل الرقمي والإجراءات الجزائية، إلى جانب الأدبيات القانونية والفنية وبعض التطبيقات المقارنة. وخلصت الدراسة إلى أن تتبع حركة القيمة لا يعني بذاته إسناد المعاملة إلى شخص محدد، لأن السجل قد يكشف المعاملة والعنوان دون الهوية القانونية للمسيطر عليه. كما تبين ضرورة التمييز بين البيانات الأصلية القابلة للتحقق والاستنتاجات الناتجة عن التجميع والإسناد ودرجات المخاطر. وأكدت الدراسة أن القوة الإثباتية لهذه النتائج تتوقف على مشروعية الحصول على البيانات، وسلامة استخراجها وحفظها، وتوثيق سلسلة الحيازة، وموثوقية الأداة والمنهج، وقابلية النتائج للمراجعة والمناقشة، مع بقاء تقدير كفايتها لسلطة القاضي وضمان حق الدفاع في اختبار أساسها الفني. وأوصت بوضع إطار إجرائي وفني موحد وتعزيز الاستعانة بأدلة مستقلة خارج السلسلة.

¹ باحثة قانونية في مركز شرطة المراجعة - فرع البلاغات والتحقيق بمدينة العين. حاصلة على درجة الدكتوراه في القانون العام الدولي من جامعة عجمان عام 2025، ودرجة الماجستير في العلوم الجنائية من جامعة العين للعلوم والتكنولوجيا عام 2024، ودرجة الماجستير في القانون العام من الجامعة ذاتها عام 2017. تتمتع بخبرة مهنية في مجال البحث القانوني، ودراسة الملفات والقوائم القانونية، وتحليل التشريعات الاتحادية والمحلية واللوائح التنظيمية، وإعداد المذكرات والتقارير القانونية. كما سبق لها العمل باحثة قانونية في قسم تنفيذ الأحكام بالمؤسسة الإصلاحية والعقابية في العين. وتركز اهتماماتها البحثية على القانون الجنائي، والأدلة الرقمية، والتقنيات الحديثة في الإثبات، والجرائم المرتبطة بالأصول الافتراضية. ومن أبحاثها: "الحجية الإثباتية لمخرجات تحليل البلوك تشين في تتبع المعاملات المرتبطة بجرائم العملات المشفرة: دراسة تحليلية في التشريع الإماراتي".

الكلمات المفتاحية: البلوك تشين، العملات المشفرة، الدليل الرقمي، الإسناد الجنائي، سلسلة الحيازة، الحجية الإثباتية.

Abstract

This study examines the evidentiary value of technical outputs derived from blockchain analysis in cryptocurrency-related crimes. It aims to determine their legal status and the requirements governing their admissibility and probative weight under UAE law. Using an analytical approach, the study reviews relevant provisions on digital evidence and criminal procedure, alongside legal and technical literature and selected comparative practices. It finds that tracing the movement of value does not, by itself, establish attribution to a specific person, as the blockchain may reveal a transaction and address without identifying the legal person controlling it. The study also distinguishes between directly verifiable blockchain data and analytical inferences based on clustering, attribution, and risk scoring. Their evidentiary weight depends on lawful data acquisition, integrity of extraction and preservation, chain of custody, methodological reliability, and reviewability. The study recommends a unified procedural and technical framework and greater reliance on independent off-chain evidence.

Keywords: Blockchain, cryptocurrency, digital evidence, criminal attribution, chain of custody, evidentiary value.

المقدمة:

أفرز التطور المتسارع في استخدام الأصول الرقمية والعملات المشفرة أنماطاً جديدة من المعاملات المالية العابرة للحدود، كما أتاح في المقابل توظيف هذه التقنيات في بعض صور النشاط الإجرامي، ولا سيما غسل الأموال والاحتيال وتمويل الأنشطة غير المشروعة. وقد أدى ذلك إلى تزايد أهمية أدوات التحليل التقني القادرة على تتبع حركة القيمة عبر شبكات السجل الموزع، والكشف عن الروابط بين المعاملات والعناوين والمخاف. غير أن القيمة القانونية لهذه الأدوات لا تقف عند حدود قدرتها التقنية على التتبع، بل تثير إشكالاً أكثر تعقيداً يتعلق بمدى إمكان الاستناد إلى مخرجاتها في الإثبات الجنائي، وبخاصة عند الانتقال من إثبات حركة أصل رقمي إلى إسنادها إلى شخص أو كيان محدد.

وتزداد أهمية هذه الإشكالية لأن مخرجات التحليل لا تتمتع بدرجة واحدة من اليقين؛ فبعضها يعيد عرض بيانات مثبتة على السلسلة، بينما يقوم بعضها الآخر على قواعد استدلالية وبيانات خارجية وعمليات تجميع وإسناد وتصنيف للمخاطر. ومن ثم، يثور التساؤل حول طبيعتها القانونية، وشروط قبولها، وقوتها الإثباتية، وحدود سلطة القاضي في تقديرها، وضمانات الدفاع في فحص أساسها الفني. وفي هذا الإطار، تتجه الدراسة إلى تحليل هذه المسائل في ضوء التشريع الإماراتي، بما يسهم في بناء تصور قانوني يوازن بين فاعلية التحقيق الجنائي ومتطلبات المحاكمة العادلة.

أهمية البحث:

الأهمية العلمية: تنبع الأهمية العلمية للدراسة من معالجتها لمسألة لم تحظَ بقدر كافٍ من التحليل القانوني، وهي الطبيعة الإثباتية للمخرجات التحليلية الناتجة عن فحص المعاملات الرقمية، مع التمييز بينها وبين البيانات الأصلية المسجلة على السلسلة وتقرير الخبر والأدلة الخارجية المرتبطة بالإسناد. وتسهم الدراسة في تأصيل التفرقة بين ما يثبت السجل مباشرة وما تستنتج أدوات التحليل، وبيان أثر درجة الاستنتاج ومصادر البيانات ومنهج الأداة في القوة الإثباتية للنتيجة، بما يضيف إطارًا تحليليًا أكثر دقة لدراسة الدليل الرقمي في البيئة الجنائية.

الأهمية العملية: تتمثل الأهمية العملية للدراسة في تقديم إطار يمكن أن يفيد جهات التحقيق والخبراء والمحكم في التعامل مع المخرجات التحليلية بصورة أكثر دقة، من خلال بيان ضوابط الحصول على البيانات واستخراجها وحفظها، وتوثيق سلسلة الحياة، وفحص موثوقية الأداة والمنهج، وتقدير مدى كفاية النتيجة للإسناد الجنائي. كما تساعد الدراسة في تعزيز التوازن بين فاعلية التحقيق في الجرائم المرتبطة بالمعاملات الرقمية وبين ضمانات المحاكمة العادلة، ولا سيما حق الدفاع في فحص الأساس الفني للنتيجة ومناقشتها.

مشكلة البحث:

تتمثل مشكلة الدراسة في أن قابلية معاملات العملات المشفرة للرصد والتتبع على شبكات البلوك تشين لا تعني بالضرورة إمكان إسنادها إلى أشخاص محددين، إذ قد يكشف السجل حركة القيمة والعناوين المرتبطة بها دون أن يكشف بذاته الهوية القانونية لمن يسيطر على تلك العناوين. ومع تطور أدوات تحليل البلوك تشين، لم يعد التحقيق يقتصر على قراءة البيانات المسجلة على السلسلة، وإنما أصبح يعتمد على مخرجات تحليلية تتدرج من تتبع مسار المعاملة وتجميع العناوين إلى إسنادها إلى كيانات معينة وتصنيفها وفق درجات للمخاطر، وهي مخرجات تختلف في مصدرها ومنهج إنتاجها ومقدار الاستنتاج الذي تتضمنه. وقد أكد البحث نفسه ضرورة الفصل بين البيانات الأصلية المسجلة على السلسلة وبين النتائج التي تستخلصها أدوات التحليل منها.

ومن هنا تثار الإشكالية القانونية بشأن المركز الإثباتي لهذه المخرجات في التشريع الإماراتي: فهل تعامل جميعها بوصفها أدلة رقمية ذات قوة واحدة، أم تختلف طبيعتها وقيمتها بحسب قربها من البيانات الأصلية ودرجة الاستنتاج التي تتضمنها؟ وما الشروط القانونية والفنية اللازمة لقبولها؟ وإلى أي مدى يجوز التعويل عليها في إسناد المعاملة إلى المتهم، خاصة عندما تعتمد

على قواعد تجميع أو إسناد أو بيانات خارجية أو أدوات تجارية مغلقة؟ كما تمتد المشكلة إلى حدود سلطة القاضي في تقدير هذه النتائج والضمانات التي يجب أن تتاح للدفاع لفحص الأساس الذي بنيت عليه ومناقشته.

السؤال الرئيسي للبحث:

ما مدى الحجية الإثباتية لمخرجات تحليل البلوك تشين في تتبع المعاملات المرتبطة بجرائم العملات المشفرة في التشريع الإماراتي، وما الضوابط التي تحكم قبولها وتقدير قوتها والتعويل عليها أمام القضاء الجنائي؟
أسئلة البحث الفرعية:

1. ما الخصائص التي تميز العملات المشفرة وتؤثر في إمكان تتبع معاملاتهما، وما أبرز أنماط استخدامها الإجرامي ذات الصلة بالتتبع الجنائي؟
 2. ما مصادر بيانات معاملات العملات المشفرة وتقنيات تحليل البلوك تشين ومخرجاتها، وكيف يتم الانتقال من تتبع المعاملة إلى إسنادها إلى أشخاص أو أنشطة إجرامية محددة؟
 3. ما التكييف القانوني لمخرجات تحليل البلوك تشين في التشريع الإماراتي، وما الضوابط القانونية والفنية اللازمة لقبولها في الإثبات الجنائي؟
 4. ما العوامل المؤثرة في القوة الإثباتية لمخرجات تحليل البلوك تشين، وما نطاق سلطة القاضي وضمانات الدفاع في تقدير هذه المخرجات والتعويل عليها؟
- أهداف البحث:

1. بيان خصوصية العملات المشفرة من حيث خصائصها المؤثرة في إمكان التتبع، وتحليل أنماط استخدامها الإجرامي التي تجعل تتبع حركة الأصول المشفرة ذا أهمية في التحقيق الجنائي.
2. تحليل مصادر بيانات معاملات العملات المشفرة وتقنيات تحليل البلوك تشين ومخرجاتها، وبيان المراحل التي تنتقل من تتبع المعاملة والعنوان إلى إسنادها إلى كيان أو شخص أو نشاط إجرامي محدد.
3. تحديد التكييف القانوني لمخرجات تحليل البلوك تشين في ضوء التشريع الإماراتي، وبيان الضوابط القانونية والفنية اللازمة لقبول هذه المخرجات في الإثبات الجنائي.
4. تقييم العوامل التي تحدد القوة الإثباتية لمخرجات تحليل البلوك تشين، وبيان حدود سلطة القاضي وضمانات الدفاع في فحصها ومناقشتها وتقدير مدى كفايتها للتعويل عليها في الإسناد الجنائي.

نطاق البحث:

ينحصر النطاق الموضوعي للدراسة في المخرجات الناتجة عن تحليل المعاملات المرتبطة بالعملات المشفرة، وبخاصة تتبع التدفقات، وتجميع العناوين، وإسنادها إلى كيانات أو أشخاص، ودرجات المخاطر، دون التوسع في دراسة التقنية ذاتها إلا بالقدر اللازم لفهم أثرها الإثباتي. أما النطاق المكاني فيتركز على التشريع الإماراتي، مع الاستئناس المحدود ببعض التطبيقات المقارنة عند

الحاجة. ويمتد النطاق الزمني إلى التشريعات والمصادر والتطبيقات المتاحة حتى تاريخ إعداد الدراسة في عام 2026، بما يسمح بتقييم الموضوع في ضوء الإطار القانوني والفني المعاصر.

منهجية البحث:

اعتمدت الدراسة **المنهج التحليلي** بوصفه المنهج الرئيس، من خلال تحليل النصوص التشريعية الإماراتية المنظمة للدليل الرقمي والإجراءات الجزائية والأصول الافتراضية، واستقراء ما تثيره مخرجات التحليل من إشكالات تتعلق بطبيعتها القانونية وشروط قبولها وقوتها الإثباتية. كما استعانت الدراسة بالأدبيات القانونية والفنية ذات الصلة، وبعدد من التطبيقات القضائية المقارنة، لا بقصد إجراء دراسة مقارنة مستقلة، وإنما للاستئناس بها في تقييم مسائل الموثوقية وقابلية الفحص وشفافية الأدوات التجارية وحقوق الدفاع، وربط ذلك بالإطار القانوني الإماراتي.

هيكل البحث:

المبحث الأول: العملات المشفرة ومخرجات تحليل البلوك تشين في التتبع الجنائي.

المبحث الثاني: الحجية الإثباتية لمخرجات تحليل البلوك تشين وضوابط التعويل عليها.

المبحث الأول: العملات المشفرة ومخرجات تحليل البلوك تشين في التتبع الجنائي

يقوم التتبع الجنائي للمعاملات المرتبطة بالعملات المشفرة على مرحلتين مترابطتين: فهم الخصائص التقنية التي تحدد ما يمكن رصده على السلسلة، ثم تحليل البيانات الناتجة عنها للوصول إلى دلالات تتجاوز مجرد إثبات وقوع المعاملة. وتبرز الإشكالية حين تنتقل عملية التتبع من حركة قيمة ظاهرة إلى محاولة تحديد الكيان أو الشخص القائم وراء العنوان الرقمي. ومن ثم، يتناول هذا المبحث خصوصية العملات المشفرة وأنماط استخدامها الإجرامي ذات الصلة بالتتبع، ثم يبين مصادر بيانات البلوك تشين وتقنيات تحليلها وحدود إسناد مخرجاتها إلى أشخاص أو أنشطة محددة، تمهيداً لبحث حجيتها الإثباتية.

المطلب الأول: العملات المشفرة وخصوصيتها في مجال التتبع الجنائي

أدى انتشار العملات المشفرة إلى نشوء معاملات مالية ذات خصائص تقنية تختلف عن وسائل انتقال القيمة التقليدية، بما انعكس على أساليب ارتكاب بعض الجرائم المالية والتحقيق فيها. وتبرز أهمية هذه الخصائص في إمكان رصد حركة الأصول المشفرة عبر الشبكات المرتبطة بها، مع ما يثيره ذلك من صعوبات في تحديد الأشخاص القائمين وراء العناوين الرقمية. ومن ثم، يتناول هذا المطلب الخصائص المؤثرة في التتبع، ثم أنماط الاستخدام الإجرامي التي تجعل من تتبع حركة الأصول ضرورة للتحقيق الجنائي.

الفرع الأول: مفهوم العملات المشفرة وخصائصها المؤثرة في إمكان التتبع

تُعد العملات المشفرة أحد أبرز صور الأصول الرقمية القائمة على تقنيات التشفير، وهي لا تمثل الفئة الكاملة للأصول الافتراضية، وإنما تندرج ضمن نطاق أوسع يشمل صوراً أخرى من الأصول والرموز الرقمية. وتوضح الأدبيات الحديثة أن العملات المشفرة أصول رقمية تعتمد على تقنيات التشفير في تأمين المعاملات والتحقق منها، لكنها لا تستوعب جميع صور الأصول

الافتراضية⁽¹⁾. ويكتسب هذا التمييز أهمية قانونية في البحث؛ لأن التشريع الإماراتي يستخدم اصطلاح "الأصول الافتراضية" بصياغة أوسع، إذ يعرفها بأنها تمثيل رقمي للقيمة يمكن تداوله أو تحويله رقميًا واستخدامه لأغراض الدفع أو الاستثمار، مع استبعاد التمثيل الرقمي للعمليات الورقية والأوراق المالية وغيرها من الأموال⁽²⁾. وعليه، يستخدم البحث اصطلاح "العمليات المشفرة" عند الحديث عن محل الدراسة تحديدًا، بينما يُستخدم اصطلاح "الأصول الافتراضية" عند الإحالة إلى النصوص الإماراتية التي اعتمدت هذا المفهوم الأوسع.

وترتبط العمليات المشفرة في صورتها الشائعة بتقنية السجل الموزع، وعلى رأسها البلوك تشين، التي تقوم على تسجيل المعاملات داخل سجل موزع بين عدد من العقد بدلاً من الاحتفاظ بها لدى جهة مركزية واحدة. وقد عزف قرار مجلس الوزراء الإماراتي رقم (111) لسنة 2022 تقنية السجل الموزع بأنها قاعدة بيانات رقمية عامة أو خاصة تُسجل من خلالها التصرفات الواقعة على الأصول الافتراضية وتُنشأ وتُحفظ وتُشارك عبر شبكة من العقد، وتشمل تقنية البلوك تشين⁽³⁾. وتؤثر هذه البنية مباشرة في إمكان التتبع؛ لأن حركة الأصل تُسجل على السلسلة في صورة معاملات مترابطة يمكن الرجوع إليها وتحليل مسار انتقال القيمة بينها.

وتُجرى المعاملات في شبكات البلوك تشين العامة باستخدام عناوين رقمية مرتبطة بمحافظ تُدار من خلال مفاتيح تشفيرية، ويتيح المفتاح الخاص التحكم في إجراء التصرفات المرتبطة بالأصول الموجودة في المحفظة⁽⁴⁾. ومن ثم، لا تعني معرفة عنوان المحفظة معرفة الشخص الذي يسيطر عليها، وهو ما يفسر وصف هذا النموذج بأنه يقوم على "الهوية المستعارة" (Pseudonymity) لا على إخفاء كامل للمعاملة. فالبيانات المتعلقة ببعض الشبكات العامة، مثل وقت المعاملة وقيمتها والعناوين المرسل والمستقبل، تكون ظاهرة وقابلة للفحص، بينما تبقى الهوية الحقيقية الكامنة خلف العنوان غير ظاهرة مباشرة⁽⁵⁾. وتنشأ من ذلك مفارقة ذات أهمية جنائية؛ فالبنية اللامركزية والهوية المستعارة قد تعقدان عملية التعرف على الشخص الحقيقي، إلا أن علانية السجل ومقاومته للتعديل، مع إمكان التحقق اللاحق من المعاملات المسجلة عليه، تتيح في المقابل تتبع مسار انتقال الأصول وتحليل الروابط بين العناوين. ومن ثم، تكمن المعضلة الجنائية في أن السجل قد يكشف حركة القيمة من دون أن يكشف بذاته هوية القائم بها، الأمر الذي يفرض الفصل بين تتبع المعاملة وبين إسنادها إلى شخص محدد.

¹ - عائشة فضيل وعلي بناني الخير، "غسل الأموال والأصول المشفرة بين الخطر الواقعي وضرورة التقنين"، مجلة القانون والأعمال الدولية، الإصدار رقم 64، يونيو

DOI: 10.63585/RPDM9639, 2026

² - المرسوم بقانون اتحادي رقم (10) لسنة 2025 في شأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل انتشار التسلح، المادة (1).

³ - قرار مجلس الوزراء رقم (111) لسنة 2022 بشأن تنظيم الأصول الافتراضية ومزودي خدماتها، المادة (1).

⁴ - هيئة تنظيم الأصول الافتراضية بدبي (VARA)، كتاب قواعد التكنولوجيا والمعلومات، القسم (د): "المفاتيح التشفيرية وإدارة محافظ الأصول الافتراضية"، 2025.

⁵ - وجدان الصالبي، "غسل الأموال باستخدام العملات المشفرة في ضوء التشريع الجنائي المغربي ومستجدات مشروع قانون الأصول المشفرة"، مجلة القانون والأعمال الدولية، المجلد 11، العدد 4، الإصدار 65، أغسطس 2026، ص 772-791.

ويؤكد الإطار التشريعي الإماراتي الرأهن أهمية هذا البعد؛ إذ أدرج المرسوم بقانون اتحادي رقم (10) لسنة 2025 بشأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل انتشار التسلح الأصول الافتراضية صراحة ضمن نطاق تطبيقه، وأخضع مزودي خدماتها لجملة من الالتزامات الرقابية، من أبرزها تدابير العناية الواجبة، والتحقق من هوية العميل والمستفيد الحقيقي، والإبلاغ عن العمليات المشبوهة⁽¹⁾. وتكتسب هذه الالتزامات أهمية خاصة في سياق التتبع؛ لأنها توفر بيانات يمكن الاستعانة بها في الربط بين حركة الأصل المسجلة على السلسلة وبين الأشخاص أو الجهات المرتبطة بها خارج السلسلة، وهو ما يوفر مصدراً تنظيمياً خارج السلسلة يمكن الاستعانة به لاحقاً في عملية الإسناد.

ويستفاد من ذلك أن قابلية التتبع نتاج تفاعل بين البيانات الظاهرة على السلسلة والمعلومات التنظيمية المتاحة خارجها. وتظل الفجوة بين العنوان الرقمي والهوية القانونية هي الحد الفاصل بين مجرد تتبع المعاملة وإسنادها، وهي المسألة التي يبنى عليها البحث لاحقاً تقدير الحجية الإثباتية لمخرجات التحليل.

الفرع الثاني: أنماط الاستخدام الإجرامي للعملة المشفرة ذات الصلة بالتتبع

تتعدد صور الاستخدام الإجرامي للعملة المشفرة، إلا أن أهميتها في هذا البحث لا ترجع إلى مجرد كونها وسيلة حديثة لارتكاب الجريمة، وإنما إلى أن حركة القيمة الرقمية تخلف مساراً يمكن تحليله وربطه تدريجياً بالنشاط غير المشروع. وتبرز جريمة غسل الأموال في مقدمة هذه الاستخدامات؛ إذ قد تُستغل العملة المشفرة في نقل العائدات عبر محافظ متعددة، ومنصات مختلفة، وعمليات تحويل متتابعة تهدف إلى إبعاد الأموال عن مصدرها الإجرامي، كما قد تُستخدم خدمات المزج والمحافظ غير المستضافة ونقاط التحويل إلى النقد لطمس الصلة بين الأصل المشفر ومصدره الحقيقي⁽²⁾. ومن ثم، يصبح تتبع حركة الأصل عبر السلسلة وسيلة أساسية لإعادة بناء مسار الأموال وكشف مراحل التمويه والدمج، بدل الاكتفاء برصد المعاملة النهائية منفصلة عن سياقها. وتؤكد الدراسات القانونية الحديثة أن تحدي مكافحة لا يقتصر على تجريم السلوك، بل يمتد إلى القدرة على تتبع الأصل المشفر وضبطه ومصادرته وربط تدفقاته بالفاعل الحقيقي، وهو ما يجعل التتبع جزءاً من البنية الإثباتية للتحقيق ذاته⁽³⁾.

ويمتد الاستخدام الإجرامي إلى تمويل الإرهاب وغيره من أنماط التمويل غير المشروع، حيث تتيح الأصول المشفرة تحويل القيمة عبر الحدود بسرعة ومن دون المرور دائماً بوسيط مالي تقليدي. وقد أكدت تقارير حديثة لمجموعة العمل المالي أن المخاطر المرتبطة بالأصول الافتراضية تشمل إساءة استخدام المحافظ غير المستضافة، والمعاملات من نظير إلى نظير، وبعض مقدمي

¹ - المرسوم بقانون اتحادي رقم (10) لسنة 2025 في شأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل انتشار التسلح، المواد (18) و(19).

² - فضيل وبناني، "غسل الأموال والأصول المشفرة"، ص 8.

³ - الصالبي، "غسل الأموال باستخدام العملات المشفرة"، ص 772-791.

الخدمات العاملين خارج نطاق الرقابة الفعالة، وهي بيئات قد تُستغل في غسل الأموال وتمويل الإرهاب وتمويل أنشطة غير مشروعة أخرى⁽¹⁾.

وعلى المستوى الإماراتي، رصدت الجهات الرقابية في الدولة، في تقييمها الحديث للمخاطر الناشئة المرتبطة بمزودي خدمات الأصول الافتراضية، تزايد المخاطر المتصلة بالتدفقات المالية القائمة على العملات المستقرة، ولا سيما تلك المرتبطة بعملة (USDT)، فضلاً عن استخدام الجسور بين الشبكات (Cross-chain Bridges)، وخدمات المزج (Mixers)، وموجهات منصات التداول اللامركزية (DEX Routers)، والتعامل مع مزودي خدمات الأصول الافتراضية غير المرخصين، ومعاملات الند للند (P2P).⁽²⁾ وأشارت الورقة إلى ارتباط هذه الأنماط بمخاطر غسل الأموال وتمويل الإرهاب وتمويل انتشار التسليح والاحتيال وتخرب العقوبات، بما يكشف عن حضور فعلي لهذه المخاطر ضمن أولويات الرقابة الإماراتية ويؤكد الحاجة إلى أدوات قادرة على تحليل مسارات انتقال القيمة عبر البيئات والمنصات المختلفة. وتزداد أهمية التتبع هنا لأن التحقيق لا يقتصر على إثبات وجود تحويل مالي، بل يهدف إلى تحديد تسلسل التحويلات والجهات أو المحافظ التي انتقلت بينها القيمة وصولاً إلى المستفيد النهائي أو نقطة التسييل.

كما ترتبط العملات المشفرة بجرائم الاحتيال والاستيلاء على الأصول الرقمية، سواء من خلال مشاريع استثمارية وهمية أو اختراق المحافظ والمنصات أو خداع المستخدمين لتحويل أصولهم إلى عناوين يسيطر عليها الجناة. وتبين الدراسات الحديثة أن أدوات التحليل الجنائي للبلوك تشين تُستخدم لتتبع تدفقات العملات المسروقة ورصد العلاقات بين العناوين، بما يساعد على كشف حركة العائد الإجرامي حتى بعد نقله عبر عدة محافظ⁽³⁾. وينطبق الأمر ذاته على جرائم الفدية الإلكترونية، التي يطلب فيها الجاني سداد الفدية بأصول مشفرة، إذ يصبح تتبع المدفوعات اللاحقة وسيلة للكشف عن المحافظ المرتبطة بالنشاط الإجرامي وربطها بخدمات أو منصات يمكن أن تكشف بيانات إضافية عن المستخدمين⁽⁴⁾.

¹-Financial Action Task Force (FATF), *Targeted Report on Stablecoins and Unhosted Wallets – Peer-to-Peer Transactions*, Paris, 3 March 2026.

²- اللجنة الوطنية لمواجهة غسل الأموال ومكافحة تمويل الإرهاب وتمويل انتشار التسليح، اللجنة الفرعية للجهات الرقابية، "مزودو خدمات الأصول الافتراضية: المخاطر والتهديدات ونقاط الضعف الناشئة المتعلقة بغسل الأموال وتمويل الإرهاب وتمويل انتشار التسليح في دولة الإمارات المرتبطة بالعملات المستقرة"، دولة الإمارات العربية المتحدة، ديسمبر 2025، ص4.

³-Oluleye M. Adewuyi, "The Double-Edged Ledger: Cryptocurrency, Financial Crime, and the Potential of Blockchain Forensics," *International Journal of Research and Innovation in Social Science (IJRISS)*, Vol. 9, Issue 5, 2025, pp. 5739–5742, DOI: 10.47772/IJRISS.2025.905000442.

⁴-Jelena Gjorgjev, M. F. Fajar Ramadhan & Sonny Dhamayana, "Blockchain Forensics – Unmasking Anonymity in Dark Web Transactions," *International Journal of Criminology and Sociology*, Vol. 14, 2025, pp. 68–75, DOI: 10.6000/1929-4409.2025.14.07.

وتتضح الحاجة إلى التتبع بصورة أكبر عند لجوء الجناة إلى التحويلات المتكررة وخدمات المزج والتداول من نظير إلى نظير والمنصات غير المنظمة؛ فهذه الوسائل لا تمحو بالضرورة الأثر الرقمي، لكنها تزيد تعقيد مساره وتوزعه عبر شبكات ومنصات متعددة. كما أن تعدد المنصات والولايات القضائية قد يجعل الوصول إلى بيانات المستخدم أو المستفيد النهائي مرهوناً بالتعاون مع مقدمي خدمات الأصول الافتراضية والسلطات المختصة⁽¹⁾. وعليه، فإن تتبع العملات المشفرة لا يمثل مجرد أداة تقنية مساعدة، بل يشكل حلقة أساسية في كشف النمط الإجرامي، وإعادة بناء حركة العائدات، والانتقال من عنوان رقمي مجرد إلى قرائن يمكن أن تسهم في إسناد النشاط إلى أشخاص أو كيانات محددة، وهو ما يمهد لاحقاً لبحث القيمة الإثباتية لمخرجات هذا التحليل.

المطلب الثاني: آليات تحليل البلوك تشين ومخرجاتها في تتبع معاملات العملات المشفرة

إذا كان إمكان رصد حركة العملات المشفرة يتيح تتبع مسار المعاملة، فإن تحويل هذا المسار إلى معلومات ذات دلالة جنائية يتطلب إخضاع بيانات البلوك تشين لعمليات تحليل تتجاوز مجرد قراءتها. وتبرز هنا ضرورة التمييز بين البيانات الأصلية المسجلة على السلسلة وبين الاستنتاجات التي تنتجها أدوات التحليل من خلال ربط المعاملات والعناوين والأنماط المختلفة. ولا تتساوى هاتان الفئتان من حيث مصدر المعلومة وطريقة استخلاصها أو درجة اليقين التي تعكسها. ومن ثم، يتناول هذا المطلب مصادر بيانات معاملات العملات المشفرة وتقنيات تحليلها، ثم يبحث كيفية الانتقال من تتبع المعاملة إلى إسنادها إلى أشخاص أو أنشطة محددة.

الفرع الأول: مصادر بيانات معاملات العملات المشفرة وتقنيات تحليلها

تبدأ عملية تحليل معاملات العملات المشفرة من البيانات المسجلة أصلاً على البلوك تشين، وهي بيانات تنشأ مع تنفيذ المعاملة وتوثيقها في السجل الموزع. وتشمل، بحسب بنية الشبكة محل التحليل، معرف المعاملة أو بصمتها الرقمية (Transaction Hash)، وعناوين الإرسال والاستقبال، وقيمة التحويل، والبيانات الزمنية المرتبطة بتسجيل المعاملة، وما ينشأ عن ترابط هذه العناصر من مسار يمكن تمثيله في صورة شبكة من العقد والروابط. وقد أظهرت الدراسات الحديثة أن تمثيل معاملات البتكوين في صورة رسم بياني زمني يسمح بتحليل العلاقات بين العناوين وتتبع حركة القيمة عبر أعداد كبيرة من المعاملات، بما يجعل بيانات السلسلة المادة الأولية للتحليل الجنائي، لا النتيجة النهائية له⁽²⁾.

وتتمثل إحدى الوظائف الأساسية للتحليل في تتبع المعاملات (Transaction Tracing)، أي إعادة بناء حركة الأصل المشفر من عنوان إلى آخر عبر سلسلة من التحويلات. ولا يضيف التتبع، في صورته الأساسية، واقعة جديدة إلى السجل بقدر ما يعيد تنظيم الوقائع المسجلة وربطها زمنياً ومالياً للكشف عن اتجاه التدفق والعلاقات القائمة بين العناوين⁽³⁾. غير أن

¹ - فضيل وبناي، "غسل الأموال والأصول المشفرة"، ص 11.

² -Hugo Schnoering & Michalis Vazirgiannis, "Bitcoin Research with a Transaction Graph Dataset," *Scientific Data*, Vol. 12, Article 404, 2025, pp1-3 DOI: 10.1038/s41597-025-04684-8.

³ -Noor Hazfalinda Hamzah, Khairul Osman, Qi Wei Kong, Atikah Mohd Nasir & Nur Mahiza Md Isa, "Forensic Analysis of Cryptocurrencies: A Comprehensive Overview," *Asia-Pacific Journal of*

التحليل ينتقل إلى مستوى أكثر استنتاجاً عند استخدام تجميع العناوين أو المحافظ (Wallet/Address Clustering)، حيث تطبق قواعد استدلالية على أنماط المعاملات لتقدير ما إذا كانت عدة عناوين تخضع لسيطرة كيان واحد. وهنا ينبغي التمييز بين "العنوان المسجل في المعاملة" بوصفه حقيقة يمكن الرجوع إليها في السلسلة، وبين "انتماء عدة عناوين إلى مستخدم واحد" بوصفه نتيجة تحليلية. وقد بينت دراسة حديثة في الأدلة الجنائية الرقمية أن الطبيعة الاستدلالية لعمليات التجميع قد تفضي إلى ضم عناوين لا تعود في الواقع إلى الكيان ذاته، بما يفرض الحذر عند التعامل مع هذه النتائج⁽¹⁾.

ويزداد الطابع الاستنتاجي عند الانتقال إلى إسناد العناوين (Address Attribution)، الذي يهدف إلى ربط عنوان أو مجموعة عناوين بكيان معلوم، كمنصة تداول أو خدمة أو شخص ذي صلة بالتحقيق. ولا يتحقق هذا الانتقال من بيانات السلسلة وحدها، بل قد يستلزم دمجها ببيانات خارجية (Off-chain Data)، وقد تشمل هذه البيانات، بحسب سياق التحقيق، الآثار المستخرجة من الأجهزة وقواعد البيانات وسجلات التطبيقات وبيانات التصفح وغيرها من المصادر الرقمية⁽²⁾. ومن ثم، فإن الإسناد لا يمثل مجرد قراءة للسجل، بل عملية دمج بين بيانات السلسلة ومصادر بيانات خارجية تختلف في مصدرها ودرجة موثوقيتها.

كما تتيح تقنيات تحليل الشبكات والعلاقات تمثيل حركة الأموال بين المحافظ والكيانات في صورة روابط مترابطة، في حين تستخدم بعض منصات التحليل التجارية درجات للمخاطر (Risk Scoring) لتقدير مدى ارتباط عنوان أو معاملة بكيانات مصنفة عالية المخاطر، سواء عبر تعامل مباشر أو من خلال معاملات وسيطة⁽³⁾. غير أن درجة المخاطر، بخلاف قيمة المعاملة أو عنوانها، ليست معلومة مثبتة أصلاً على البلوك تشين؛ وإنما هي تقييم مشتق من قواعد التصنيف وبيانات الإسناد والمنهج الذي تتبعه الأداة.

وعليه، يرى البحث أن مخرجات تحليل البلوك تشين لا تمثل فئة واحدة متجانسة؛ إذ يتعين الفصل بين البيانات الأصلية القابلة للتحقق مباشرة من السجل، وبين العلاقات التي يعيد التحليل بناءها، والاستنتاجات الناتجة عن التجميع والإسناد والتصنيف. وهذه التفرقة تتجاوز أهميتها الجانب التقني، لأن الخلط بين "ما سجله البلوك تشين" و "ما استنتجته أداة التحليل" قد

Information Technology and Multimedia, Vol. 14, No. 2, 2025, pp. 585–594, DOI: 10.17576/apjitm-2025-1402-15.

¹-Yanan Gong, Kam Pui Chow & Siu Ming Yiu, "Improved Bitcoin Simulation Model and Address Heuristic Method," *Forensic Science International: Digital Investigation*, Vol. 53, Supplement, 2025, Article 301935, pp. 2–3 DOI: 10.1016/j.fsidi.2025.301935.

²-Abhishek Bhattarai et al., "Cryptocurrency Forensics Automation: A Deep Learning and NLP-Based Approach for Mobile Platforms," *Discover Computing*, Vol. 28, Article 123, 2025.

³-Chainalysis, "What is Blockchain Analytics?", sections on Entity Attribution, Graph Analysis and Risk Scoring, accessed 2026.

يؤدي إلى منح النتيجة الاستنتاجية قوة لا تستمدّها من السجل ذاته. ومن هنا تتميز هذه الدراسة عن الأدبيات التي انصبت أساساً على القيمة الإثباتية لسجلات البلوك تشين، إذ تتجه إلى بحث الطبيعة المستقلة للمخرجات التحليلية تمهيداً لتقييم حجيتها الإثباتية⁽¹⁾.

الفرع الثاني: إسناد معاملات العملات المشفرة إلى الأشخاص والأنشطة الإجرامية

يمثل إسناد المعاملة إلى شخص محدد مرحلة تختلف في طبيعتها عن مجرد تتبع حركة العملة على البلوك تشين؛ فالسلسلة قد تثبت انتقال قيمة معينة بين عنوانين، لكنها لا تسجل بذاتها الهوية المدنية لمن يقف وراءها. ومن ثم، يمكن تصور عملية الإسناد في مسار متدرج يبدأ من المعاملة (Transaction)، ثم العنوان (Address)، فالمحفظة أو مجموعة العناوين المترابطة (Wallet/Cluster)، ثم الكيان (Entity)، وصولاً إلى الشخص (Person). ولا تتساوى هذه المراحل من حيث مصدر المعلومة أو درجة الاستدلال؛ فكلما ابتعد التحليل عن البيانات المسجلة مباشرة على السلسلة، ازداد اعتماده على الاستنتاج وعلى مصادر معلومات إضافية ومستقلة، ولا سيما عند الانتقال من العنوان إلى الكيان ثم إلى الشخص.

وتكتسب بيانات منصات تداول الأصول الافتراضية وإجراءات "اعرف عميلك" (KYC) أهمية خاصة عند الانتقال من الكيان إلى الهوية؛ إذ يمكن أن تكشف بيانات الحساب، وعناوين الإيداع والسحب، وبيانات العميل عن الصلة بين عنوان ظهر في مسار التتبع وحساب معلوم لدى مقدم خدمة خاضع لمتطلبات التعرف على العملاء. وقد خلصت دراسة حديثة إلى أن إمكان ربط النشاطات المشبوهة بأشخاص أو جهات معينة يتعزز عند تقاطع معاملات مع منصات أو هيئات تطبق إجراءات⁽²⁾ KYC. ويكتسب ذلك أهمية إضافية في البيئة الإماراتية في ضوء إنشاء المنصة الرقمية "اعرف عميلك" بموجب المرسوم بقانون اتحادي رقم (30) لسنة 2024، وإصدار لائحته التنفيذية بقرار مجلس الوزراء رقم (55) لسنة 2026، بما يؤسس لإطار منظم بما يؤسس لإطار منظم لجمع بيانات «اعرف عميلك» وحفظها وتحليلها وتبويبها واستخدامها وتداولها وحمايتها وتنظيمها وإصدار التقارير بشأنها⁽³⁾.

وتبرز كذلك نقاط التحويل بين العملات التقليدية والأصول المشفرة (Fiat On/Off-Ramps) بوصفها نقاط التقاء مهمة بين البيئة اللامركزية والنظام المالي المنظم؛ فعند شراء الأصل المشفر بأموال تقليدية أو إعادة تحويله إلى نقد أو حساب مصرفي، قد تظهر بيانات مصرفية أو بيانات لدى شركات الصرافة أو مزودي خدمات الدفع أو منصات الأصول الافتراضية

¹ - عمر عبد المجيد مصبح، "القيمة الإثباتية لسجلات البلوك تشين في نظام العدالة الجنائية: دراسة تحليلية مقارنة"، *المجلة الدولية للقانون*، المجلد 15، العدد 1، 2026، ص 37. DOI: 10.29117/irl.2026.0361.

² - الحسين زروال، *البلوك تشين وجريمة غسل الأموال: بين المخاطر التنظيمية وفرص المكافحة*، مجلة القانون والأعمال الدولية، الإصدار 66، مارس 2026، ص 79. DOI: 10.63585/UWRW9962.

³ - المرسوم بقانون اتحادي رقم (30) لسنة 2024 بشأن المنصة الرقمية "اعرف عميلك"؛ وقرار مجلس الوزراء رقم (55) لسنة 2026 بإصدار اللائحة التنفيذية للمرسوم بقانون اتحادي رقم (30) لسنة 2024 بشأن المنصة الرقمية "اعرف عميلك"؛ قرار مجلس الوزراء رقم (55) لسنة 2026، المادة (2).

تساعد في استكمال مسار الإسناد. وقد رصدت الجهات الرقابية الإماراتية حديثاً احتمال تقاطع التدفقات عالية المخاطر مع المؤسسات المالية الخاضعة للرقابة، ولا سيما عند نقاط الدخول والخروج بين النظامين التقليدي والافتراضي⁽¹⁾. ولا يتوقف الإسناد على بيانات المنصات؛ فقد تتداخل معه أدلة رقمية مستمدة من الهواتف والحواسيب والحسابات وسجلات التطبيقات والاتصالات وبيانات الدخول وغيرها من المصادر الخارجية. وتؤكد الدراسات الإماراتية أن إثبات الجريمة لا يقتصر على التحقق من وقوعها، وإنما يستلزم كذلك وجود دليل يربطها بشخص معين⁽²⁾. وفي الإطار الإجرائي، أجاز المشرع الإماراتي لعضو النيابة العامة تفتيش الأجهزة والشبكات والمعدات والوسائط والنظم المعلوماتية وبرامج الحاسب متى استوجبت مقتضيات التحقيق ذلك، كما أجاز له تكليف الخبراء أو المختصين بالقيام بهذا الإجراء⁽³⁾. وتدعم دراسة تقنية حديثة لعام 2026 هذا الاتجاه من خلال بيان إمكان تضييق فجوة الإسناد بين الشخص والمحفظة عبر الربط المنهجي بين آثار البلوك تشين والبيانات الوصفية المستمدة من مصادر رقمية أخرى⁽⁴⁾.

غير أن مجرد ارتباط الحساب أو الجهاز أو العنوان باسم شخص لا يكفي دائماً لإثبات أنه المسيطر فعلياً على المحفظة أو أنه هو من نفذ المعاملة محل التحقيق؛ فقد تكون العناوين خاضعة لخدمة حفظ، أو لمحفظة تديرها منصة نيابة عن عدد كبير من العملاء، وهو ما يفرض التمييز بين مجرد الارتباط الاسمي أو التقني بالمحفظة وبين السيطرة الفعلية عليها وقت إجراء المعاملة. وتؤكد الممارسات المهنية الحديثة في تحليل البلوك تشين أن Address Attribution يعتمد على الجمع بين البيانات الموجودة على السلسلة والأدلة الخارجية، وأن نسبة العنوان إلى كيان معين يجب ألا تعامل باعتبارها حقيقة مطلقة منفصلة عن مصدر الإسناد ودرجة الثقة فيه⁽⁵⁾.

وعليه، يرى البحث أن ثبوت حركة العملات إلى عنوان معين لا يساوي بذاته ثبوت أن المتهم هو صاحب ذلك العنوان أو المسيطر عليه وقت إجراء المعاملة. فالإسناد الجنائي السليم يقتضي بناءً تراكمياً يجمع بين سجل المعاملة، ونتائج التحليل، وبيانات المنصات، وبيانات KYC، والآثار الرقمية المستمدة من الأجهزة والحسابات، وغيرها من القرائن المستقلة. ويتفق ذلك

¹ - اللجنة الوطنية لمواجهة غسل الأموال ومكافحة تمويل الإرهاب وتمويل انتشار التسليح، مزودو خدمات الأصول الافتراضية، مرجع سابق، ص4.

² -Ayman Nawwaf Alhawawsheh et al., "Digital Evidence as a Means of Proof in Criminal Proceedings in the UAE," *Access to Justice in Eastern Europe*, Vol. 8, No. 3, 2025, pp. 1-20, 10.33327/AJEE-18-8.3-a000111.

³ - المرسوم بقانون اتحادي رقم (38) لسنة 2022 بإصدار قانون الإجراءات الجزائية، المادة (1/73).

⁴ -Wei-Hsiang Lin & Che-Yen Wen, "A Lawful Metadata-Driven Framework for Linking Encrypted Communication Behavior and Cryptocurrency Wallet Activity in Digital Investigations," *Applied System Innovation*, Vol. 9, No. 4, 2026, Article 73, pp.1-4 DOI: 10.3390/asi9040073

⁵ -Chainalysis, "What is Wallet Attribution?", sections "Off-chain Evidence and Entity Attribution", "Assigning a Confidence Level", and "Risks and Common Misconceptions about Wallet Attribution", accessed 2026.

مع الاتجاه الذي يربط قيمة الدليل الإلكتروني بإثبات صلتها بالجريمة والمتهم، ويحذر من التعويل عليه منفردًا متى تعذر إثبات نسبته إلى الشخص محل الاتهام⁽¹⁾. ومن هنا تنتقل الدراسة من سؤال كيفية الوصول إلى الشخص إلى السؤال القانوني الأهم: ما الطبيعة القانونية لهذه المخرجات، وما مدى القوة الإثباتية التي يجوز منحها لكل منها؟

المبحث الثاني: الحجية الإثباتية لمخرجات تحليل البلوك تشين وضوابط التعويل عليها

ينتقل هذا المبحث من بيان كيفية إنتاج مخرجات تحليل البلوك تشين إلى بحث مركزها القانوني وقيمتها في الإثبات الجنائي. وتكمن أهمية هذه المرحلة في أن سلامة البيانات المسجلة على السلسلة لا تكفي بذاتها لإضفاء الحجية على كل نتيجة مشتقة منها، مما يقتضي بحث طبيعتها، وشروط قبولها، ومدى قوتها والرقابة القضائية عليها.

المطلب الأول: الطبيعة القانونية وشروط قبول مخرجات تحليل البلوك تشين

يقتضي تحديد مدى صلاحية مخرجات تحليل البلوك تشين للإثبات التمييز بين سجل المعاملة الأصلي، والمخرج التحليلي، وتقرير الخبر، والأدلة الخارجية المرتبطة بالإسناد. ومن ثم، يتناول هذا المطلب التكييف القانوني لهذه العناصر في ضوء التشريع الإماراتي، ثم يحدد الضوابط القانونية والفنية اللازمة لقبولها أمام القضاء الجنائي.

الفرع الأول: التكييف القانوني لمخرجات تحليل معاملات العملات المشفرة

لا يقتضي تحديد الطبيعة القانونية لمخرجات تحليل معاملات العملات المشفرة البحث عن وصف واحد ينطبق على جميع ما تنتجه عملية التحليل؛ إذ كشف المبحث السابق أن هذه العملية تتعامل مع عناصر تختلف من حيث مصدرها وطريقة إنتاجها ودرجة الاستنتاج التي تنطوي عليها. ولذلك يجب ابتداءً الفصل بين سجل المعاملة الأصلي على البلوك تشين، والمخرج الذي تولده أداة التحليل، والتقرير الفني الذي يفسر هذا المخرج، والأدلة الخارجية التي تربط العنوان أو المحفظة بشخص معين. ويترتب على هذا الفصل أثر قانوني مهم، هو أن ثبوت الطبيعة الرقمية لأحد هذه العناصر لا يعني بالضرورة تماثلها جميعًا في طبيعتها أو قوتها الإثباتية.

فبالنسبة إلى سجل المعاملة الأصلي، فإنه يمثل البيانات التي أثبتتها السلسلة ذاتها بشأن وقوع المعاملة وعناصرها المسجلة، كالتحويل والعناوين والقيمة والبيانات الزمنية بحسب بنية الشبكة. وقد تناولت الدراسات القانونية الحديثة هذا النوع من السجلات من زاوية سلامته وإمكان التحقق منه وقيمته في الإثبات الجنائي، وهو ما يظهر بوضوح في دراسة مصباح التي انصبت على "القيمة الإثباتية لسجلات البلوك تشين" في نظام العدالة الجنائية⁽²⁾. ومن ثم، فإن السجل الأصلي يمثل نقطة البدء الإثباتية التي يمكن الرجوع إليها للتحقق مما هو مثبت على السلسلة، لكنه يظل محتلفًا عن النتيجة التي تستخلصها أداة تحليلية عند ربط هذه البيانات أو تصنيفها أو الاستدلال منها.

¹ - فوزي لواتي وعبد القادر بوبكر، "حجية الدليل الإلكتروني في الإثبات الجنائي"، مجلة الفكر القانوني والسياسي، المجلد العاشر، العدد الأول، 2026، ص 354؛ ص 358.

² - مصباح، "القيمة الإثباتية لسجلات البلوك تشين في نظام العدالة الجنائية: ص 37 وما بعدها.

أما مخرجات تحليل البلوك تشين، فتثير إشكالات أدق. فقد عرّف المشرع الإماراتي "الدليل الرقمي" تعريفاً واسعاً يشمل المعلومات الإلكترونية ذات القوة أو القيمة الثبوتية المخزنة أو المنقولة أو المستخرجة أو المأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها، مع إمكان تجميعها وتحليلها بواسطة أجهزة أو برامج أو تطبيقات تكنولوجية خاصة؛ كما قررت المادة (65) أن للأدلة المستمدة أو المستخرجة من الوسائل والأنظمة والبرامج الإلكترونية حجية الأدلة الجنائية المادية في الإثبات الجنائي⁽¹⁾. ويتيح اتساع هذا التعريف، في تقدير البحث، إدراج المخرج التحليلي من حيث طبيعته الرقمية ضمن هذا الإطار متى كانت له قيمة في إثبات واقعة محل التحقيق. غير أن ذلك لا يبرر مساواة كل مخرج تحليلي بالبيانات الأصلية التي بُني عليها؛ فهناك فرق بين نتيجة تعيد عرض واقعة يمكن التحقق منها مباشرة من السلسلة، وبين نتيجة تستند إلى قواعد استدلالية، مثل تجميع العناوين أو إسنادها إلى كيان أو تصنيفها وفق درجة للمخاطر. وتدعم الدراسات الحديثة ضرورة هذا الحذر؛ إذ تميز بين سلامة البيانات التقنية وبين ما تنتجه الأنظمة الآلية من عمليات كشف وتصنيف وتفسير، بما قد يثير مسائل تتعلق بالشفافية والحياد وإمكان فحص النتيجة⁽²⁾.

ويتربط على ذلك أن وصف المخرج بأنه "دليل رقمي" لا يحسم بذاته وظيفته الإثباتية. فإذا اقتصر المخرج على إعادة عرض بيانات أو علاقات يمكن التحقق منها مباشرة من السجل، كانت دلالاته أقرب إلى البيانات الرقمية المشتقة مباشرة من المصدر. أما إذا كان يعبر عن احتمال أو استنتاج مستخلص من أنماط متعددة، فإن وظيفته تصبح أقرب إلى قرينة رقمية ذات طبيعة استنتاجية تحتاج إلى تقدير مدى صحة مقدماتها والمنهج الذي أنتجها. ولا يقصد البحث بذلك إنشاء فئة تشريعية مستقلة لم ينص عليها القانون الإماراتي، وإنما التمييز الوظيفي بين المعلومة الرقمية التي تثبت واقعة مسجلة وبين المخرج الذي يستدل منها على واقعة أخرى. وهذه التفرقة تحول دون افتراض أن الموثوقية المرتبطة بسلامة البيانات الأصلية تنتقل تلقائياً إلى كل استنتاج تحليلي مشتق منها. وتؤكد الدراسة الإماراتية الحديثة حول الدليل الرقمي أن الاعتراف بقيمته الإثباتية لا ينفصل عن شروط اليقين والمشروعية والسلامة وإمكان عرضه ومناقشته أمام الخصوم⁽³⁾.

ويجب كذلك عدم الخلط بين المخرج التحليلي وتقرير الخبر. فالمخرج ينتجه البرنامج أو الأداة نتيجة معالجة البيانات، أما الخبرة فهي نشاط إجرائي يقوم به شخص ذو اختصاص فني لتفسير مسألة تحتاج إلى معرفة متخصصة. وقد أجاز قانون

¹ - المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية، المادة (1)، تعريف "الدليل الرقمي"، والمادة (65)، بشأن حجية الأدلة المستمدة أو المستخرجة من الوسائل والأنظمة والبرامج الإلكترونية في الإثبات الجنائي.

² - محمد واجد النعمة، منى م. بالو، سلوى م. علي، "سلسلة الكتل (Blockchain) والذكاء الاصطناعي في الأدلة الرقمية: التحديات القضائية ومعايير القبول"،

DOI: 10.36371/port.2026.special.3، ص 20-33، 2026، *Journal Port Science Research*، المجلد 9، عدد خاص،

³ - Alhawawsheh et al., "Digital Evidence as a Means of Proof in Criminal Proceedings in the UAE," pp. 521-540.

الإجراءات الجزائية الإماراتي للنيابة العامة الاستعانة بخبير لإثبات واقعة معينة، وألزمه بتقديم تقرير مكتوب عن المهمة المكلف بها، كما أجاز للمحكمة ندب خبير أو أكثر واستدعاء الخبراء لمناقشتهم فيما قدموه من تقارير⁽¹⁾.

ومن ثم، فإن الرسم الشبكي، أو نتيجة تجميع العناوين، أو نتيجة إسناد العنوان إلى كيان معين، لا تتحول بذاتها إلى «خبرة» لمجرد صدورهما عن برنامج متخصص؛ وإنما قد تكون محلاً لتقرير في يوضح مصدر البيانات، ومنهج التحليل، ودلالة النتيجة، وحدود ما يمكن استخلاصه منها. ولا يعد كل تقرير في بذاته تقرير خبرة بالمعنى الإجرائي، إذ يتوقف اكتسابه هذه الصفة على صدوره في إطار خبرة أجريت وفقاً للقواعد الإجرائية المقررة قانوناً. كما أن تضمين المخرجات التحليلية في تقرير خبير لا يغير طبيعتها الأصلية، ولا يزيل ما قد يحيط بطريقة إنتاجها من طابع احتمالي أو درجة من عدم اليقين.

أما الأدلة الخارجية، كبيانات "اعرف عميلك"، وبيانات المنصات والحسابات والأجهزة وسجلات الدخول، فهي لا تعد جزءاً من سجل البلوك تشين ولا مجرد مخرج لأداة التحليل، وإنما تمثل مصادر إثبات مستقلة قد تؤدي وظيفة مختلفة، هي الربط بين النتيجة الرقمية والشخص محل الاتهام. ومن ثم، قد يثبت السجل انتقال العملة إلى عنوان معين، ويقترح التحليل ارتباط العنوان بمجموعة أو كيان، ثم تأتي بيانات مستقلة لتدعم أو تثبت، بحسب قوتها، الصلة بين ذلك الكيان والمتهم. ولهذا فإن الإسناد الجنائي لا يقوم في كثير من الحالات على دليل واحد، بل على تفاعل عدة عناصر تختلف في طبيعتها ومصدرها. ويختلف ذلك أيضاً عن الصورة التي تناولتها دراسات استخدام البلوك تشين في توثيق دليل رقمي آخر أو حفظ سلسلة حيازته؛ إذ تبحث تلك الدراسات سلامة الدليل الموثق، بينما يتعلق موضوع البحث الحالي بمركز المخرج التحليلي المستخلص من بيانات البلوك تشين نفسها⁽²⁾.

وعليه، يخلص البحث إلى أن التكييف القانوني لمخرجات تحليل البلوك تشين تكيف متدرج لا موحد؛ فسجل المعاملة الأصلي يمكن أن يمثل دليلاً رقمياً مصدره السلسلة، في حين يعد المخرج التحليلي معلومات رقمية مشتقة قد تقتصر على إعادة عرض بيانات قابلة للتحقق من المصدر، أو تحمل دلالة استنتاجية بحسب مقدار الاستدلال الذي تتضمنه، أما تقرير الخبير فهو الوعاء الفني والإجرائي الذي يفسر تلك المخرجات، وتظل الأدلة الخارجية عناصر مستقلة تدعم عملية الإسناد أو تنفيها. وعند اجتماع هذه العناصر لإثبات نسبة المعاملة إلى متهم معين، يستخدم البحث اصطلاح "البناء الإثباتي المركب" للدلالة على تضافر عناصر إثبات متعددة تختلف في مصدرها وطبيعتها، لا بوصفها فئة مستقلة قررها المشرع الإماراتي. وتظهر هنا جودة الدراسة؛ إذ انصبت الأدبيات السابقة بصورة أساسية على سجلات البلوك تشين أو استخدام التقنية في حفظ الأدلة وتوثيقها،

¹ - المرسوم بقانون اتحادي رقم (38) لسنة 2022 بإصدار قانون الإجراءات الجزائية، المواد (94)، (96)، (181).

² - هاجر الحمدوني، "حجية الدليل الرقمي الموثقة بالبلوكشين في الإثبات الجنائي"، مجلة القانون والأعمال الدولية، المجلد 11، العدد 4، الإصدار 65، أغسطس 2026، ص 406-424.

بينما ينصرف البحث الحالي إلى تحديد المركز القانوني للاستنتاج التحليلي ذاته قبل الانتقال إلى ضوابط قبوله، ثم إلى تقدير قوته الإثباتية أمام القضاء⁽¹⁾.

الفرع الثاني: الضوابط القانونية والفنية لقبول مخرجات التحليل

لا يكفي إضفاء وصف الدليل الرقمي أو الطبيعة القرائية على مخرجات تحليل البلوك تشين للقول بصلاحياتها للتعبيل عليها في الإثبات الجنائي؛ إذ يتوقف ذلك على سلامة المسار الذي يبدأ بالحصول على البيانات، ويمر باستخراجها وحفظها وتحليلها، وينتهي بإنتاج المخرج وتقديمه أمام القضاء. وانطلاقاً من الاعتراف التشريعي السابق بالدليل الرقمي وإمكان جمع البيانات وتحليلها بواسطة الوسائل والبرامج التقنية، فإن المسألة هنا لا تتعلق بمجرد الطبيعة الرقمية للمخرج، وإنما بسلامة المسار الذي أنتجه⁽²⁾. غير أن هذا الاعتراف لا يعني افتراض صحة كل نتيجة تنتجها أداة التحليل، وإنما يقتضي الفصل بين سلامة البيانات التي بُني عليها المخرج وموثوقية الطريقة التي أنتجته.

ويأتي شرط مشروعية الحصول على البيانات في مقدمة هذه الضوابط. فلا يستوي الاطلاع على بيانات معاملة متاحة أصلاً على سلسلة عامة مع الوصول إلى بيانات غير متاحة للجمهور محفوظة في جهاز أو حساب أو لدى منصة أو مزود خدمة. ويجد هذا الشرط أساساً دستورياً في كفالة سرية المراسلات ووسائل الاتصال وفقاً للقانون، كما أجاز قانون الإجراءات الجزائية لعضو النيابة العامة، متى اقتضى التحقيق، تفتيش الأجهزة والشبكات والمعدات والوسائط والنظم المعلوماتية وبرامج الحاسب، مع إمكان تكليف خبير أو مختص بذلك⁽³⁾. ومن ثم، فإن إمكان الوصول إلى البيانات تقنياً لا يغني عن مشروعية الطريق الإجرائي للحصول عليها، وبخاصة عند الانتقال من بيانات السلسلة العامة إلى بيانات خارجية تكشف هوية المستخدم أو نشاط حسابه.

ويظهر هذا التمييز في التطبيق المقارن في قضية الولايات المتحدة ضد غراتكوفسكي (United States v. Gratkowski)

(Gratkowski)؛ إذ بدأ التحقيق بتحليل سجل البيتكوين العام وتحديد عناوين ذات صلة بالنشاط محل التحقيق، ثم انتقل إلى بيانات عملاء منصة "كوين بيس". ورفضت محكمة الاستئناف الأمريكية للدائرة الخامسة دفع المتهم بعدم مشروعية الوصول إلى تلك البيانات وفق معايير الخصوصية في القانون الأمريكي⁽⁴⁾. ولا ينقل هذا الحكم إلى التشريع الإماراتي من حيث معيار

¹ - حيدر المياحي وهبة عبد الأمير حميد، "دور تقنية البلوكتشين في حفظ أدلة الإثبات القانوني: دراسة تحليلية"، مجلة جامعة الأنبار للعلوم القانونية والسياسية، المجلد 16، العدد 2، 2026، ص 880-903، DOI: 10.37651/aujpls.2025.157839.1477؛ وانظر كذلك: محمد والشيخ، "الحجية القانونية والقضائية للدليل الإلكتروني المعتمد في الإثبات الجنائي"، مجلة الشؤون الجنائية والحكامة الأمنية، المجلد 2، العدد 2، 2024.

² - المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية، المادة (1)، تعريف "الدليل الرقمي"، والمادة (65) بشأن حجية الأدلة المستمدة أو المستخرجة من الوسائل والأنظمة والبرامج الإلكترونية.

³ - دستور دولة الإمارات العربية المتحدة، المادة (31)؛ والمرسوم بقانون اتحادي رقم (38) لسنة 2022 بإصدار قانون الإجراءات الجزائية، المادة (1/73).

⁴ - United States v. Gratkowski, 964 F.3d 307, 309-313 (5th Cir. 2020).

الخصوصية، وإنما تكمن أهميته في بيان اختلاف المركز القانوني للبيانات بحسب مصدرها وطبيعتها وإتاحتها؛ فكون نقطة البداية متاحة على سجل عام لا يجعل جميع البيانات اللاحقة المستخدمة في الإسناد متاحة بالطريقة ذاتها.

ويرتبط بذلك سلامة البيانات الأصلية وأصالتها وتوثيق مصدرها وإجراءات استخراجها. فقد أكد الفقه الحديث أن سلامة الدليل الرقمي تستلزم معرفة مصدره وموثوقيته والتأكد من عدم تعرضه للتغيير، كما أشار مصباح إلى ضرورة استخلاص البيانات وحفظها بصورتها الأصلية والتحقق من سلامة البرنامج التقني المستخدم ودقة مخرجاته⁽¹⁾. ويؤكد المشرع الإماراتي بدوره أهمية حماية سلامة الدليل الرقمي؛ إذ جرم، في نطاق الجرائم الخاضعة للمرسوم بقانون رقم (34) لسنة 2021، إخفاء الدليل الرقمي أو العبث به بقصد عرقلة البحث أو التحقيق أو الاستدلال⁽²⁾.

وتكتسب مطابقة النسخة المستخرجة لمصدرها أهمية خاصة في تحليل البلوك تشين؛ إذ قد تعتمد الأداة على بيانات مستخرجة من السلسلة أو أعيد تنظيمها لأغراض التحليل، لا على السجل الموزع في صورته الأصلية. ومن ثم، تتوقف سلامة هذه المرحلة على إمكان رد البيانات المستخدمة إلى مصدرها والتحقق من مطابقتها له. ولذلك ينبغي توثيق مصدر البيانات، وتاريخ استخراجها، والأداة أو الوسيلة المستخدمة، والتحقق من أن عملية الاستخراج لم تضيف إليها أو تحذف منها أو تعدلها بصورة تؤثر في النتيجة اللاحقة

وقد ظهر هذا الاتجاه في قضية شركة هانغتشو هواتاي ضد شركة شنتشن داوتونغ أمام محكمة هانغتشو للإنترنت سنة 2018؛ إذ لم تعتبر المحكمة مجرد تسجيل البيانات باستخدام البلوك تشين كافيًا لإثبات صحتها، بل فحصت مصدر البيانات، وطريقة جمعها وتوليدها ونقلها، والبيئة التقنية المستخدمة، وإمكان التحقق منها، قبل قبولها⁽³⁾. ورغم الطبيعة المدنية للقضية، فإنها تكشف عن مبدأ صالح للاستئناس في موضوع البحث، وهو أن ثبات البيانات بعد تسجيلها لا يحسم بذاته سلامة الطريقة التي دخلت بها إلى النظام أو صحة المخرجات التي تبني عليها.

ويكمل ذلك توثيق سلسلة حيازة الدليل، فقد عرّف الدليل الاسترشادي للتعامل مع الأدلة الجنائية الرقمية في الدول العربية سلسلة متابعة الأدلة باعتبارها عملية تتبع لحركتها خلال مراحل جمعها وحمايتها وتحليلها، من خلال توثيق الأشخاص الذين تعاملوا معها، وتاريخ ووقت جمعها أو نقلها، والغرض من النقل. وفي مجال تحليل البلوك تشين ينبغي أن يمتد هذا التوثيق إلى هوية كل من تعامل مع البيانات، وتاريخ ووقت استخراجها أو نقلها أو فحصها، والغرض من كل انتقال أو معالجة، والنسخة التي

¹ - المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية، المادة (18)؛

² - مصبح، "القيمة الإثباتية لسجلات البلوك تشين في نظام العدالة الجنائية"، ص 42-43.

³ - Hangzhou Huatai Media Culture Media Co., Ltd. v. Shenzhen Daotong Technology Development Co., Ltd., Hangzhou Internet Court, (2018) Zhe 0192 Min Chu No. 81 ؛ وانظر كذلك: المحكمة الشعبية العليا لجمهورية الصين الشعبية، "أحكام المحكمة الشعبية العليا بشأن عدد من المسائل المتعلقة بنظر القضايا أمام محاكم الإنترنت"، 2018، المادة (11).

أجري عليها التحليل. ولا تحل مقاومة سجل البلوك تشين للتعديل محل سلسلة الحياة؛ لأن الأولى تتعلق بسلامة البيانات المسجلة على الشبكة، بينما تتعلق الثانية بما يطرأ على البيانات بعد استخراجها وانتقالها إلى بيئة التحقيق والفحص والتحليل⁽¹⁾.

ولا تقف الضوابط عند سلامة البيانات؛ إذ ينبغي أن تمتد إلى منهج التحليل والأداة المستخدمة. ويتطلب ذلك توثيق الخطوات الجوهرية التي أدت إلى النتيجة، وتحديد البرنامج وإصداره، ونطاق البيانات المستخدمة، والأسس أو القواعد التي استند إليها في التجميع أو الإسناد أو التصنيف. ولا يكفي ذكر اسم الأداة التجارية، بل ينبغي التحقق من صلاحيتها للغرض المستخدم من أجله، وحدود منهجها، وما يعرف عن أخطائها أو مواطن عدم اليقين فيها متى أمكن تحديد ذلك. وهذه الضوابط أكثر أهمية في مخرجات مثل إسناد العناوين أو تجميعها أو درجات المخاطر؛ لأنها ليست بيانات مثبتة أصلاً على السلسلة، وإنما استنتاجات ناتجة عن المعالجة. ومن ثم، فإن الثقة التقنية في سجل البلوك تشين لا تنتقل تلقائياً إلى البرنامج الذي يحلل بياناته.

ويتصل بصلاحية الأداة تأهيل القائم بالتحليل وخبرته الفنية؛ إذ يظل العنصر البشري حاضراً في تحديد البيانات الداخلة في التحليل، واختيار نطاقه، وتفسير نتائجه. وقد أظهرت الدراسات المتعلقة بالتحقيق في الجرائم المرتبطة بالعملات الافتراضية أن محدودية المعرفة التقنية تمثل إحدى صعوبات التحقيق، وهو ما يقتضي إشراك مختصين في التحليل الرقمي وتكنولوجيا البلوك تشين. ويتفق ذلك مع قانون الإجراءات الجزائية الإماراتي الذي يميز الاستعانة بالخبرة في المسائل التي تتطلب معرفة فنية، وينظم التقرير الذي يقدمه الخبير عن المهمة المكلف بها⁽²⁾. وبذلك لا يقتصر تقييم المخرج على صلاحية البرنامج، وإنما يشمل كذلك كفاءة من استخدمه ومدى سلامة تطبيقه للمنهج.

كما يجب أن يكون المخرج قابلاً للتحقق والمراجعة وإعادة إجراء التحليل. ويقتضي ذلك إمكان الرجوع إلى البيانات التي بنيت عليها النتيجة وتتبع المراحل الجوهرية المؤدية إليها، وإمكان إعادة تطبيق الخطوات الجوهرية للتحليل على البيانات ذاتها، متى سمحت طبيعة الأداة والمنهج بذلك، أو مقارنتها بتحليل مستقل للتحقق من استقرار النتيجة. ولا يقصد بإعادة الإنتاج ضرورة التطابق الحرفي بين جميع الأدوات، وإنما ألا تكون النتيجة قائمة على عملية لا يمكن فحص منطقتها أو اختبارها أو تكرار خطواتها الأساسية.

وقد شكلت قضية الولايات المتحدة ضد ستيرلينغوف (United States v. Sterlingov) تطبيقاً مهماً لهذا الضابط؛ إذ طعن الدفاع في النتائج التي أنتجها برنامج "ريكتور" التابع لشركة "تشيناليسس" في تجميع عناوين البيتكوين وإسنادها وتتبع معاملات مرتبطة بخدمة "بيتكوين فوغ". ورفضت المحكمة الفيدرالية لمقاطعة كولومبيا طلب استبعاد التحليل بعد فحص موثوقية المنهج، وكان من العناصر المهمة في تقديرها إمكان اختبار نتائج التجميع ومقارنتها بالتتبع اليدوي وبأدوات تحليل

¹ - الحمدوني، "حجية الدليل الرقمي الموثقة بالبلوكشين في الإثبات الجنائي"، ص 408-411؛ وانظر كذلك: الدليل الاسترشادي للتعامل مع الأدلة الجنائية الرقمية في الدول العربية، جامعة نايف العربية للعلوم الأمنية، دار جامعة نايف للنشر، الرياض، 2024، ص 12.

² - المرسوم بقانون اتحادي رقم (38) لسنة 2022 بإصدار قانون الإجراءات الجزائية، المادتان (94)، (96)؛ زروال، البلوك تشين وجريمة غسل الأموال، ص 89.

أخرى، فضلاً عن إتاحة البيانات الأساسية للدفاع لإجراء تحليل مستقل⁽¹⁾. وتدلل القضية على أن صلاحية الأداة لا تستمد من شهرتها، بل من إمكان اختبار ما تنتجه ومراجعتها ومناقشة الأساس الذي قامت عليه النتيجة، أما أثر الاعتراضات المتعلقة بدقة هذه النتائج في وزنها وقوتها الإثباتية، فيتناوله البحث في المطلب التالي.

وأخيراً، يجب أن تكون المخرجات قابلة للعرض والفحص والمناقشة أمام القضاء. فلا يكفي تقديم رسم شبكي أو نتيجة إسناد أو درجة مخاطر مجردة من بيان أساسها؛ بل ينبغي أن يتاح للمحكمة والخصوم معرفة مصدر البيانات وطريقة استخراجها وخطوات التحليل ودلالة المخرج وحدود ما يمكن استنتاجه منه. ويجد ذلك أساساً في الضمانات الدستورية للمحاكمة القانونية العادلة وحق الدفاع، كما يحول قانون الإجراءات الجزائية المحكمة أن تأمر بتقديم ما تراه لازماً من الأدلة لكشف الحقيقة، ويجيز لها ندب الخبراء واستدعاءهم ومناقشتهم بشأن تقاريرهم⁽²⁾. ومن ثم، فإن قدرة الدفاع على فحص الأساس الفني للنتيجة ومناقشة الخبر تمثّل ضمانات ذات أهمية خاصة عندما يعتمد المخرج على منهج استنتاجي أو برنامج تجاري لا تظهر جميع تفاصيل تشغيله للمستخدم.

وعليه، يرى البحث أن قبول مخرجات تحليل البلوك تشين يقوم على منظومة مترابطة من الضمانات لا على خاصية تقنية منفردة؛ فتبدأ بمشروعية الحصول على البيانات وتحديد مصدرها، وتمتد إلى سلامة الأصل والنسخة المستخرجة وسلسلة الحياة وإجراءات الاستخراج، ثم إلى توثيق منهج التحليل وصلاحية الأداة وتأهيل القائم به، وتنتهي بإمكان التحقق من النتيجة وإعادة فحصها ومناقشتها أمام القضاء. ولا تكفي مقاومة سجل البلوك تشين للتعديل لإضفاء الموثوقية على كل مخرج مشتق منه؛ فقد تكون البيانات الأصلية سليمة بينما يقع الخلل في طريقة استخراجها أو في قواعد التجميع أو الإسناد أو تفسير النتيجة. ومن ثم، كلما ازدادت الطبيعة الاستنتاجية للمخرج، ازدادت الحاجة إلى هذه الضمانات قبل التعويل عليه في الإثبات الجنائي.

المطلب الثاني: نطاق حجية مخرجات تحليل البلوك تشين والرقابة القضائية عليها

لا يترتب على قبول مخرجات تحليل البلوك تشين أن تتمتع جميعها بالقوة الإثباتية ذاتها؛ إذ تختلف بحسب طبيعة المخرج ومقدار الاستنتاج الذي يتضمنه ومصادر البيانات التي يستند إليها. لذلك يبحث هذا المطلب العوامل المؤثرة في وزنها، ثم يبين سلطة القاضي وضمانات الدفاع في فحصها ومناقشتها وتقدير مدى التعويل عليها.

الفرع الأول: العوامل المؤثرة في القوة الإثباتية لمخرجات التحليل

لا تتمتع جميع مخرجات تحليل البلوك تشين بقوة إثباتية واحدة؛ لأن ما تنتجه أدوات التحليل يتفاوت من حيث قربه من البيانات الأصلية ومقدار الاستنتاج الذي يتوسط بين تلك البيانات والنتيجة النهائية. فإثبات أن معاملة محددة سُجلت على

¹ - *United States v. Sterlingov*, 719 F. Supp. 3d 65 (D.D.C. 2024), Memorandum Opinion and Order, Feb. 29, 2024.

² - دستور دولة الإمارات العربية المتحدة، المادة (28)؛ والمرسوم بقانون اتحادي رقم (38) لسنة 2022 بإصدار قانون الإجراءات الجزائية، المادتان (180)، (181).

السلسلة، وأن قيمة معينة انتقلت بين عنوانين في وقت محدد، يختلف عن استنتاج أن عدة عناوين تخضع لسيطرة كيان واحد، كما يختلف عن إسناد ذلك الكيان إلى شخص معلوم أو تصنيفه على أنه مرتفع المخاطر. ومن ثم، لا ينبغي أن تنتقل الوثائق المرتبطة بسلامة السجل ذاته تلقائيًا إلى كل نتيجة مشتقة منه؛ بل تتحدد قوة المخرج بحسب طبيعته، ومقدار الاستنتاج الذي يتضمنه، والمنهج الذي أنتجه، ومصادر البيانات التي استند إليها، ومدى إمكان التحقق منه وتدعيمه بأدلة مستقلة.

ويظهر هذا التفاوت بوضوح عند الانتقال من الحقيقة المسجلة إلى تجميع العناوين وإسنادها. فتجميع العناوين لا يثبت واقعة مدونة على السلسلة، وإنما يقوم على تطبيق قواعد استدلالية لتقدير احتمال خضوع عدة عناوين لسيطرة مشتركة. وقد بينت دراسة حديثة حول تحليل معاملات البيتكوين أن غياب بيانات مرجعية مؤكدة بشأن المالك الحقيقي للعناوين يخلق قدرًا من عدم اليقين في نتائج التجميع، وأن اختلاف القواعد الاستدلالية وتقنيات تعزيز الخصوصية قد يؤدي إلى نتائج غير دقيقة ويحد من موثوقية التجميع في السياق الجنائي⁽¹⁾. ومن ثم، فإن مجرد ظهور عنوانين ضمن مجموعة واحدة لا يساوي إثباتًا قطعيًا بأنهما يعودان إلى الشخص نفسه، كما أن احتمال النتيجة الإيجابية الكاذبة يظل قائمًا متى أدت قاعدة التجميع إلى ضم عناوين لا تخضع في الواقع لسيطرة واحدة.

ويزداد مقدار الاستنتاج عند إسناد العنوان أو المجموعة إلى كيان معلوم؛ إذ لا تتضمن السلسلة بذاتها اسم الشخص الذي يسيطر على المفتاح أو يستفيد من المعاملة. ويقوم الإسناد عادة على الجمع بين التحليل على السلسلة وبيانات خارجها، مثل بيانات "اعرف عميلك"، أو بيانات الضبط والتحقيق، أو المعلومات المقدمة من المنصات، أو المصادر المفتوحة. وحتى المصادر المتخصصة في صناعة تحليل البلوك تشين تميز بين التجميع والإسناد، وتقرر أن الهوية لا توجد على السلسلة، وأن صحة الادعاء بالإسناد تتفاوت بحسب مصدره ودرجة الثقة فيه، فضلًا عن ضرورة التمييز بين الجهة التي تتحكم في المحفظة والمستفيد الذي تستخدم المحفظة لحسابه⁽²⁾. ولهذا فإن عنوان المحفظة لا يتلائم قانونًا أو فنيًا مع هوية المتهم؛ فقد يعود العنوان إلى منصة تحفظ أصول عدد كبير من العملاء، أو إلى محفظة مجمعة، أو إلى مقدم خدمة يتصرف نيابة عن مستخدم آخر.

ويجد هذا التحفظ سندًا مهمًا في البيئة الإماراتية؛ إذ تشير الورقة الرقابية الصادرة عن اللجنة الوطنية لمواجهة غسل الأموال ومكافحة تمويل الإرهاب وتمويل انتشار التسليح إلى أن المحافظ المجمع وأصول المستخدمين قد يصعبان تحديد مصدر الأصول وملكيتهما، كما تقر بوجود فجوات في تغطية أدوات تحليل البلوك تشين وفي القدرة على تحديد المعاملات والمحافظ وتتبعها، ولا سيما المحافظ غير المستضافة ومعاملات الند للند⁽³⁾. وهذه الفجوات ذات أثر مباشر في القوة الإثباتية؛ لأن ضعف إمكانية الانتقال من العنوان إلى هوية موثقة يجعل المخرج صالحًا لإظهار مسار مالي محتمل أكثر من صلاحيته، منفردًا، لإثبات نسبة هذا المسار إلى شخص بعينه.

¹-Gong, Chow & Yiu, "Improved Bitcoin Simulation Model and Address Heuristic Method," p. 3.

²-Chainalysis, "What Is Wallet Attribution?", section "Assigning a Confidence Level."

³- اللجنة الوطنية لمواجهة غسل الأموال ومكافحة تمويل الإرهاب وتمويل انتشار التسليح، مزودو الخدمات الأصول الافتراضية، مرجع سابق، ص 13-16.

وينطبق التدرج ذاته على درجات المخاطر والتصنيفات التحليلية. فدرجة المخاطر لا تسجلها السلسلة، وإنما تنتج عن قواعد تحدد مدى تعرض معاملة أو محفظة لكيان أو نشاط مصنف على أنه عالي المخاطر. وتكشف الورقة الإماراتية الرسمية نفسها عن الطبيعة الاحتمالية لهذا النوع من المخرجات؛ إذ تدعو المؤسسات المرخصة إلى استخدام أدوات تمنح المعاملات التي مرت عبر جسور أو خدمات مزج "درجة مسار" تعكس احتمال استخدامها لأغراض الإخفاء، على أن تخضع المعاملات ذات الدرجة المرتفعة لمزيد من التدقيق⁽¹⁾. ويستفاد من ذلك أن ارتفاع درجة المخاطر يمثل إشارة تستدعي التحقيق والتحقق، ولا يثبت بذاته أن الأموال متحصلة من جريمة أو أن صاحب المحفظة كان عالمًا بمصدرها غير المشروع. ومن ثم، تكون القوة الإثباتية لدرجة المخاطر أقل من القوة التي قد تحملها واقعة مسجلة يمكن التحقق منها مباشرة، ما لم تتساند الدرجة مع بيانات أخرى تفسر سبب التصنيف وترتبط المعاملة بالواقعة الإجرامية.

كما تتأثر قوة المخرج بطبيعة المسار الذي مرت به الأصول الافتراضية. فخدمات المزج مصممة لإضعاف العلاقة الظاهرة بين المدخلات والمخرجات؛ وقد أظهرت دراسة حديثة لتحريات البيتكوين أن هذه الخدمات تعقد تتبع التدفقات بدرجة كبيرة، وأن التعرف على المشغلين أو المستخدمين في القضايا التي درستها لم يعتمد على بيانات السلسلة وحدها، بل كان للمعلومات خارج السلسلة وأساليب التحقيق التقليدية دور حاسم⁽²⁾. ويتفق ذلك مع التقييم الإماراتي الذي يقرر أن المزج يجعل تتبع تدفق الأموال بالغ الصعوبة، وأن العبور المتكرر بين الجسور وخدمات المزج يعد مؤشرًا للإخفاء يستوجب تدقيقًا إضافيًا. وتبرز الصعوبة بصورة أشد مع العملات المعززة للخصوصية؛ فبعضها، مثل مونيرو، يستخدم آليات تشفير تهدف إلى إخفاء المشاركين في المعاملة ومبالغها، بما يحيد من البيانات التي يستطيع التحليل المباشر للسلسلة استخلاصها. وقد بينت دراسة جنائية رقمية حديثة أن تجاوز هذه القيود استلزم الانتقال إلى آثار خارج السلسلة، مثل بيانات الذاكرة وملفات المحفظة والمفاتيح المخزنة على الجهاز⁽³⁾. كما يضع الإطار التنظيمي لسلطة تنظيم الأصول الافتراضية في دبي العملات المعززة لإخفاء الهوية والوسائل التي تسمح بإجراء معاملات معززة لإخفاء الهوية ضمن المخاطر التي يجب على مزودي الخدمات تقييمها تحديدًا⁽⁴⁾.

¹ - المرجع السابق، ص 8-9، بشأن درجات مسارات الجسور وخدمات المزج والتدقيق المعزز في المعاملات ذات الدرجة المرتفعة.

² - Pascal Tuppe & Christoph Deckers, "Unmixing the Mix: Patterns and Challenges in Bitcoin Mixer Investigations," *Forensic Science International: Digital Investigation*, Vol. 52, Supplement, March 2025, Article 301876, DOI: 10.1016/j.fsidi.2025.301876.

³ - Jeongin Lee, Geunyeong Choi, Jihyo Han & Jungheum Park, "Advanced Monero Wallet Forensics: Demystifying Off-Chain Artifacts to Trace Privacy-Preserving Cryptocurrency Transactions," *Forensic Science International: Digital Investigation*, Vol. 54, Supplement, October 2025, Article 301988, DOI: 10.1016/j.fsidi.2025.301988.

⁴ - سلطة تنظيم الأصول الافتراضية بدبي، قواعد مكافحة غسل الأموال وتمويل الإرهاب وتحويل الأموال - تقييم مخاطر الأعمال، بند تقييم المخاطر المتعلقة بالأصول الافتراضية المعززة لإخفاء الهوية والمعاملات المعززة لإخفاء الهوية، 2026.

وتؤكد هذه الصورة أن نقصان البيانات المرئية على السلسلة لا يؤدي بالضرورة إلى استحالة الإثبات، لكنه يزيد اعتماد النتيجة على مصادر خارجية، ومن ثم يغير طبيعتها ودرجة قوتها.

وتطرح **الجسور بين الشبكات** مشكلة مشابهة؛ لأن انتقال الأصل من شبكة إلى أخرى قد يستلزم الربط بين معاملتين مسجلتين في سجلين مستقلين. وقد أظهرت دراسة تطبيقية على جسور إيثيريوم وبوليغون أن هذا الربط يمكن أن يعتمد على خوارزمية مطابقة استدلالية تجمع بين توقيت المعاملات وقيمتها ونوع الأصل، وقد حققت الدراسة معدلات مطابقة مرتفعة لكنها غير كاملة، ولا سيما في عمليات السحب⁽¹⁾. وهذا مهم إثباتيًا؛ فوجود المعاملتين على السلسلتين قد يكون ثابتًا، بينما **كونهما** **تمثلان انتقالًا واحدًا للأصل نفسه** هو نتيجة تحليلية تتوقف قوتها على دقة قاعدة المطابقة. وقد صنفت الجهات الرقابية الإماراتية الجسور وخدمات المزج وموجهات التداول اللامركزي ضمن أبرز وسائل الإخفاء عبر السلاسل، وأقرت بالحاجة إلى تحليلات مخصصة لكل سلسلة ومراقبة النشاط العابر لها.

ولا يقتصر عدم اليقين على بنية المعاملة، بل قد يرجع إلى **مصدر البيانات التي تعتمد عليها أداة التحليل في التصنيف والإسناد**. فقد أشارت الورقة الإماراتية إلى اعتماد شركات تحليل البلوك تشين على قواعد بيانات للعناوين المرتبطة باختراقات وأنشطة غير مشروعة لاستخدامها في فحص المعاملات.⁽²⁾ وهنا تتأثر قوة النتيجة بدرجة موثوقية الإدخال الأصلي في قاعدة البيانات، وحدائته، ووضوح أساس التصنيف. فإذا تغيرت السيطرة على عنوان، أو استند التصنيف إلى معلومة غير مؤكدة، أو كانت بيانات الطرف المقابل أو المستفيد الحقيقي ناقصة، فإن هذا القصور ينعكس على المخرج المشتق منه. ولذلك يمكن القول إن **الإسناد لا يكون أقوى من مصدر المعرفة الخارجية التي بُني عليها**. ويؤكد ذلك أيضًا أن بيانات الإسناد ليست ثابتة بطبيعتها؛ فقد تتغير بمرور الزمن وتتفاوت درجة الثقة فيها، وهو ما يستوجب عدم التعامل مع كل تصنيف محفوظ في قاعدة بيانات تجارية باعتباره حقيقة نهائية.

ويضاف إلى ذلك **اختلاف منهجيات أدوات تحليل البلوك تشين وقابليتها للمراجعة والتكرار**. فاختيار قاعدة التجميع أو طريقة حساب المخاطر أو معيار الإسناد قد يؤدي إلى اختلاف النتائج بين الأدوات، وهو ما يجعل إمكان مراجعة الخطوات الجوهرية للتحليل ومقارنتها بتحليل مستقل عاملاً مؤثرًا في قوة المخرج. وقد ظهر ذلك عملًا في قضية **الولايات المتحدة ضد ستيرلينغوف**؛ إذ عزز من قابلية نتائج التحليل للتقييم إمكان اختبار بعض عمليات التجميع بالتتبع اليدوي ومقارنتها

¹-Tao Yan, Chuanshan Huang & Claudio J. Tessone, "Tracing Cross-Chain Transactions Between EVM-Based Blockchains: An Analysis of Ethereum-Polygon Bridges," *Ledger*, Vol. 10, 2025, pp. 113-134, DOI: 10.5195/ledger.2025.433.

²- اللجنة الوطنية لمواجهة غسل الأموال ومكافحة تمويل الإرهاب وتمويل انتشار التسلح، مرجع سابق، ص 9؛ وانظر كذلك : Chainalysis, "What Is Wallet Attribution?",

بمخرجات أدوات تحليل أخرى، بدل الاكتفاء بالنتيجة التي أنتجها برنامج واحد⁽¹⁾. ومن ثم، فكلما أمكن الرجوع إلى البيانات المستخدمة وإعادة تطبيق المنهج أو التحقق من النتيجة بأداة أو وسيلة مستقلة، ارتفعت درجة الثقة فيها؛ وعلى العكس، تضعف القوة الإثباتية عندما لا يكون من الممكن تحديد كيفية الانتقال من البيانات الأولية إلى المخرج أو اختبار الأساس الذي قامت عليه النتيجة.

وعليه، يخلص البحث إلى أن القوة الإثباتية لمخرجات تحليل البلوك تشين قوة متدرجة وليست موحدة. فكلما اقترب المخرج من واقعة مسجلة يمكن التحقق منها مباشرة من السلسلة، قل مقدار الاستنتاج الذي يتوسط بينها وبين النتيجة. أما مخرجات التجميع والإسناد ودرجات المخاطر والربط عبر السلاسل، فتزداد فيها أهمية منهج التحليل ومصادر البيانات الخارجية واحتمالات الخطأ. كما تؤدي خدمات المزج والعملات المعززة للخصوصية والمحافظة غير المستضافة ونقص بيانات الأطراف المقابلة إلى زيادة عدم اليقين في التتبع. ولذلك لا تقاس قوة المخرج بمجرد صدوره عن أداة متخصصة، وإنما بقربه من البيانات الأصلية، ومقدار الاستنتاج الذي يتضمنه، وموثوقية منهج إنتاجه ومصادر الإسناد التي يستند إليها، ومدى قابليته للاختبار المستقل، وتسانده مع أدلة أخرى. ويتفق هذا الاتجاه مع ما رصدته دراسة حديثة في البيئة الإماراتية من تعامل حذر مع الاعتماد المنفرد على بعض صور الدليل الرقمي، والاستعانة بأدلة أخرى كالشهادة والإقرار والخبرة في بناء الاقتناع القضائي⁽²⁾.

الفرع الثاني: سلطة القاضي وضمانات الدفاع في تقدير مخرجات التحليل

لا يترتب على قبول مخرجات تحليل البلوك تشين ضمن عناصر الإثبات أن تكتسب قوة ملزمة للمحكمة؛ إذ يجب التمييز بين الاعتراف التشريعي بالدليل الرقمي وبين تقدير وزنه في الدعوى. فقد أقر المشرع الإماراتي، في نطاق المرسوم بقانون اتحادي رقم (34) لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية، للأدلة المستمدة أو المستخرجة من الأجهزة والوسائط والنظم المعلوماتية وبرامج الحاسب حجية الأدلة الجنائية المادية في الإثبات الجنائي وفق المادة (65). غير أن تقرير الحجية من حيث الأصل لا يعني أن كل نتيجة رقمية تكون قاطعة أو متساوية مع غيرها في القوة؛ إذ يظل تقديرها خاضعاً للقواعد العامة التي تحكم اقتناع القاضي الجنائي.

وفي هذا الإطار، تقرر المادة (209) من قانون الإجراءات الجزائية الإماراتي أن المحكمة لا تنقيد بما هو مدون في التحقيق الابتدائي أو محاضر الاستدلالات إلا إذا نص القانون على خلاف ذلك، بينما تنص المادة (210) على أن القاضي يحكم في الدعوى وفق القناعة التي تكونت لديه، مع عدم جواز بناء الحكم على دليل لم يطرح على الخصوم أمامه في الجلسة.

¹ - *United States v. Sterlingov*, 719 F. Supp. 3d 65 (D.D.C. 2024), Memorandum Opinion and Order, Feb. 29, 2024.

² - Alhawawsheh et al., "Digital Evidence as a Means of Proof in Criminal Proceedings in the UAE," pp. 521-540,

ويترتب على ذلك أن ورود نتيجة تحليل البلوك تشين في محضر استدلال أو تقرير فني أو تقرير خبرة لا يحولها إلى نتيجة مفروضة على المحكمة، وإنما تبقى عنصرًا تخضع قوته لتقديرها في ضوء طبيعته وأساسه الفني ومدى اتساقه مع سائر الأدلة. وقد استقر القضاء الاتحادي على ما يؤكد هذا الاتجاه؛ إذ قررت المحكمة الاتحادية العليا في الطعن رقم (257) لسنة 31 القضائية، الصادر في 12 يناير 2004، أن لمحكمة الموضوع "كامل الحرية في تقدير القوة التدللية لتقرير الخبير"، فلها أن تأخذ بما تطمئن إليه وتطرح ما عدها⁽¹⁾. ورغم صدور الحكم في ظل قانون الإجراءات الجزائية السابق، فإن مبدئه ينسجم مع المادتين (209) و(210) من القانون الحالي. وتزداد أهمية هذا المبدأ في مخرجات تحليل البلوك تشين؛ لأن الخبير قد يعتمد في تقريره على نتيجة تجميع عناوين أو إسناد عنوان إلى كيان أو درجة للمخاطر، إلا أن إدراج هذه المخرجات في تقريره لا يزيل طبيعتها الاستنتاجية ولا يجعل تفسيره لها ملزمًا للقاضي.

ويتأكد ذلك بالنظر إلى الطبيعة الفنية للبلوك تشين ذاتها؛ إذ ينبغي الفصل بين سلامة السجل وبين صحة مضمون البيانات أو الاستنتاج المستخلص منها. فمقاومة البيانات المسجلة للتعديل قد تدعم الثقة في أن سجلًا معينًا لم يتغير بعد تسجيله، لكنها لا تكفل بذاتها صحة المعلومات المدخلة إليه، كما لا تثبت صحة ما تستخلصه أداة التحليل من علاقات أو إسنادات. وقد أشار مصبح إلى أن القيمة الإثباتية لأدلة البلوك تشين تختلف بحسب بنية السلسلة، ومحتوى المعاملات، وسياق القضية، وطريقة جمع الدليل وتقديمه، وأن تعقيد التقنية قد يستلزم الاستعانة بالخبراء لتفسير أنظمتها وحدودها⁽²⁾. ومن ثم، لا يصح أن تتحول الثقة في البنية التقنية للسجل إلى افتراض قضائي بصحة كل استنتاج تحليلي مشتق منه.

ولا ينتقص ذلك من أهمية الخبرة الفنية في هذا المجال. فقد أجازت المادة (94) من قانون الإجراءات الجزائية للنيابة العامة ندب خبير عندما يتطلب التحقيق معرفة فنية، وأوجبت المادة (96) تقديم تقرير مكتوب عن المهمة المكلف بها، كما خولت المادة (181) المحكمة تعيين خبير أو أكثر، واستدعاء الخبراء لمناقشتهم فيما قدموه من تقارير، وأوجبت عليها إجراء المناقشة إذا طلبها الخصوم⁽³⁾. وتزداد أهمية الخبرة في تحليل البلوك تشين لتمكين المحكمة من فهم منهج التجميع أو الإسناد ومصادر البيانات وحدود النتيجة. غير أن الحاجة إلى المعرفة المتخصصة لا تعني أن رأي الخبير "قاطع" أو أنه يخرج عن سلطة المحكمة؛ فالأدق أن القاضي لا يستبدل المسألة الفنية برأي شخصي مجرد، لكنه يظل محتصًا بتقدير التقرير ومدى سلامة أساسه وكفايته واتساقه مع بقية عناصر الدعوى.

وتثير هذه السلطة مسألة أخرى تتعلق بمدى كفاية مخرج التحليل وحده للإدانة. ولا يظهر في التشريع الإماراتي ما يسمح بصياغة قاعدة عامة مؤداها أن الدليل الرقمي لا يمكن أن يكفي منفردًا؛ بل تتحدد المسألة بحسب قوة الدليل في ظروف

¹ - المحكمة الاتحادية العليا، الطعن رقم (257) لسنة 31 القضائية، أمن دولة، جلسة 12 يناير 2004.

² - عمر عبد المجيد مصبح، "القيمة الإثباتية لسجلات البلوك تشين في نظام العدالة الجنائية: دراسة تحليلية مقارنة"، *المجلة الدولية للقانون*، المجلد 15، العدد 1، 2026، ص 55-56، DOI: 10.29117/irl.2026.0361.

³ - المرسوم بقانون اتحادي رقم (38) لسنة 2022، المواد (94)، (96)، (181).

كل قضية. غير أن التفرقة التي انتهى إليها الفرع السابق بين الحقيقة المسجلة والاستنتاج التحليلي تصبح حاسمة هنا؛ فقد يكون سجل المعاملة كافيًا لإثبات انتقال قيمة إلى عنوان معين، بينما لا يلزم من ذلك أن يكون مخرج إسناد هذا العنوان إلى المتهم كافيًا وحده لإثبات السيطرة عليه. وكلما ارتفع مقدار الاستنتاج وعدم اليقين في المخرج، ازدادت أهمية وجود أدلة مستقلة تعضده. ويؤيد هذا التحفظ ما رصدته دراسة حديثة عن الدليل الرقمي في البيئة الإماراتية من أن المحاكم، في التطبيقات التي تناولتها الدراسة، دعمت الأدلة الرقمية بعناصر أخرى مثل الاعتراف والشهادة والخبرة، بدل عزلها عن بقية البناء الإثباتي⁽¹⁾. ولا يعني ذلك اشتراط التعدد في كل دعوى، وإنما يكشف عن أهمية النظر إلى تساند الأدلة عند تقييم المخرجات الاستنتاجية. ويمكن الاستئناس في هذا السياق بقضية الولاية ضد لوميس (State v. Loomis)، وإن كانت تتعلق بأداة لتقييم مخاطر العودة إلى الجريمة في مرحلة الحكم بالعقوبة وليست بأداة لتحليل البلوك تشين. فقد أجازت المحكمة العليا لولاية ويسكونسن النظر إلى مخرج أداة "كومباس"، لكنها قيدت استخدامه بحيث لا يكون العامل الحاسم، ولاحظت أن الأداة تقوم على بيانات جماعية ولا تقدم تنبؤًا فرديًا يقينًا، كما أكدت ضرورة وجود عوامل مستقلة أخرى تسند القرار⁽²⁾. وتفيد هذه المقارنة في تقرير قاعدة أضيق: النتيجة الاحتمالية أو الاستنتاجية لا ينبغي أن تتحول، لمجرد صدورهما عن نظام تقني، إلى حقيقة فردية قاطعة بشأن المتهم.

ويقابل سلطة المحكمة في تقدير المخرج ضمان حق الدفاع في فحص أساسه ومناقشته. فقد كفلت المادة(28) من دستور دولة الإمارات قرينة البراءة والمحكمة القانونية العادلة وحق المتهم في الاستعانة بمن يدافع عنه، كما تقرر المادة(98) من قانون الإجراءات الجزائية تمكين محامي المتهم من حضور التحقيق والاطلاع على أوراق الدعوى، مع جواز تقييد ذلك لمصلحة التحقيق. ويضاف إلى ذلك حكم المادة(210) التي تمنع بناء الحكم على دليل لم يطرح على الخصوم في الجلسة، والمادة(181) التي تكفل مناقشة الخبر بناءً على طلبهم⁽³⁾.

ولا تكون المناقشة فعالة في مخرجات تحليل البلوك تشين إذا اقتصر على عرض النتيجة النهائية دون الأساس الذي أدى إليها. فإذا قرر التقرير، مثلاً، أن مجموعة من العناوين ترتبط بالمتهم أو أن عنوانًا معينًا ينتمي إلى كيان مصنف عالي المخاطر، فقد يكون محل النزاع الحقيقي هو قاعدة التجميع، أو المصدر الخارجي الذي قام عليه الإسناد، أو البيانات التي أدخلت إلى الأداة، أو درجة الثقة في النتيجة. ومن ثم، ينبغي أن تتاح للمحكمة والدفاع، بالقدر الذي تسمح به طبيعة القضية والقواعد الإجرائية، المعلومات اللازمة لإجراء مناقشة حقيقية للمخرج لا مجرد الاطلاع على خلاصته.

¹-Alhawawsheh et al., "Digital Evidence as a Means of Proof in Criminal Proceedings in the UAE," pp.12.

²-State v. Loomis, 2016 WI 68, 371 Wis. 2d 235, 881 N.W.2d 749.

³- دستور دولة الإمارات العربية المتحدة، المادة (28)؛ والمرسوم بقانون اتحادي رقم(38) لسنة 2022، المواد(98)،(181)،(210).

وقد ظهرت هذه المسألة بصورة مباشرة في قضية الولايات المتحدة ضد ستيرلينغوف (**United States v. Sterlingov**)، حيث طعن الدفاع في نتائج برنامج "ريكتور" التابع لشركة "تشيناليسس"، ونازع في قواعد تجميع عناوين البيوتكوين وإسنادها، وفي غياب معدل مركزي للأخطاء وعدم خضوع بعض القواعد لمراجعة علمية. ورغم رفض المحكمة استبعاد التحليل، فإنها لم تعتبر البرنامج بمنأى عن الاعتراض؛ بل كان من عناصر قبولها للخبرة أن بعض عمليات التجميع يمكن اختبارها ومقارنتها ببيانات البلوك تشين العامة، مع بقاء حق الدفاع في الطعن في دقة النتائج وموثوقيتها أمام هيئة المحلفين⁽¹⁾. ولذلك لا يصلح الحكم سنداً للقول بموثوقية جميع منتجات "تشيناليسس"، وإنما يبين أهمية قابلية المنهج للاختبار والمناقشة في القضية المحددة.

وتزداد الإشكالية عندما تكون أداة التحليل تجارية مغلقة ولا يظهر للمستخدم إلا المخرج النهائي، وهو ما يثير مشكلة "الصندوق الأسود". ولا يعني مجرد عدم الكشف عن الشفرة المصدرية بطلان الدليل؛ إذ قد توجد وسائل أخرى كافية لفحص الطريقة والتحقق من النتيجة. إلا أن عدم الشفافية يصبح أكثر خطورة عندما تكون العملية البرمجية محل النزاع هي ذاتها التي أنتجت الدليل المؤثر في الإسناد الجنائي. ويشير الدليل المرجعي للأدلة العلمية، في طبعته الرابعة لعام 2025، إلى أهمية فهم البرامج والأنظمة الحاسوبية التي تنتج أو تعالج الأدلة، ويوفر للقضاة إطاراً لتقييم مسائل علوم الحاسب والأدلة التقنية⁽²⁾.

وتقدم قضية الولاية ضد بيكيت (**State v. Pickett**) مثالاً مقارناً مهماً في الموازنة بين سرية البرنامج وحقوق الدفاع. فقد تعلق النزاع ببرنامج تجاري للتحليل الاحتمالي للحمض النووي، وطالب الدفاع بالشفرة المصدرية والوثائق الفنية اللازمة لاختبار موثوقيته. وقررت محكمة الاستئناف في نيوجيرسي أن الحماية المقررة للأسرار التجارية لا تمنع الكشف متى أثبت المتهم حاجة محددة للمعلومات اللازمة لضمان محاكمة عادلة، مع إمكانية حماية مصالح المنتج عن طريق أمر قضائي يحد من تداول المواد والإفصاح عنها⁽³⁾. وقد أكدت الكتابات القانونية كذلك أن تحويل السر التجاري إلى حجاب دائم أمام فحص الأدوات المستخدمة في الإثبات الجنائي قد يخل بالتوازن بين حماية الملكية الفكرية وحق المتهم في اختبار الدليل المقدم ضده⁽⁴⁾.

¹ - *United States v. Sterlingov*, 719 F. Supp. 3d 65 (D.D.C. 2024), Memorandum Opinion and Order, Feb. 29, 2024.

² - Brian N. Levine, Joanne Pasquarelli & Clay Shields, "Reference Guide on Computer Science," in National Academies of Sciences, Engineering, and Medicine & Federal Judicial Center, *Reference Manual on Scientific Evidence*, 4th ed., National Academies Press, 2025, pp. 1411–1482, DOI: 10.17226/26919.

³ - *State v. Pickett*, 466 N.J. Super. 270, 246 A.3d 279 (App. Div. 2021).

⁴ - Rebecca Wexler, "Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System," *Stanford Law Review*, Vol. 70, 2018, pp. 1343–1429.

وعليه، يخلص البحث إلى أن التطور التقني لا يقلل من سلطة القاضي في تقدير الدليل الرقمي، وإنما يغير طبيعة الرقابة التي يمارسها عليه. فالقاضي لا يتولى بنفسه حل المسائل الفنية التي تستلزم خبرة متخصصة، لكنه لا يفقد في المقابل سلطته في تقدير سلامة الأساس الذي بني عليه التقرير، ومدى صلة المخرج بالواقعة، وكفايته، واتساقه مع سائر الأدلة، وقابليته للمناقشة. ويقابل هذه السلطة حق الدفاع في الوصول إلى القدر اللازم من البيانات والمنهج الذي يسمح باختبار النتيجة اختباراً فعلياً. ومن ثم، لا يجوز أن تتحول مقاومة البلوك تشين للتعديل أو خبرة المحلل أو حماية السر التجاري للأداة إلى قرينة مستقلة على صحة المخرج؛ بل كلما ازداد أثر المخرج في نسبة الجريمة إلى المتهم، ازدادت الحاجة إلى شفافية تسمح للمحكمة والخصوم بفحص الأساس الذي أنتجه، مع إمكان حماية المصالح التجارية بوسائل إجرائية أقل مساساً بحق الدفاع.

الخاتمة:

خلصت الدراسة إلى أن تتبع المعاملات المرتبطة بالعملات المشفرة يمثل مساراً تحليلياً متدرجاً يبدأ من البيانات المسجلة على البلوك تشين، ويمتد إلى ربط المعاملات والعناوين وتحليل حركة القيمة وصولاً إلى محاولة إسنادها إلى شخص أو كيان محدد. وقد تبين أن خصائص المعاملات المشفرة، كاللامركزية والهوية المستعارة، قد تعقد تحديد الفاعل الحقيقي، لكنها لا تحول دون إمكان التتبع في ظل علانية بعض السجلات وإمكان التحقق اللاحق منها. كما أظهرت الدراسة أن مخرجات التحليل تختلف في طبيعتها ودرجة اليقين التي تعكسها، إذ يجب التمييز بين البيانات المسجلة والاستنتاجات التحليلية. وتظل الفجوة بين العنوان الرقمي والهوية القانونية التحدي الأبرز، مما يستلزم دعم نتائج التحليل ببيانات "اعرف عميلك" وبيانات المنصات والأجهزة وغيرها من مصادر الإثبات المستقلة.

نتائج الدراسة

- 1- كشفت الدراسة أن خصائص المعاملات المشفرة تحمل أثراً مزدوجاً في التتبع الجنائي؛ فاللامركزية والهوية المستعارة والمخاطر غير المستضافة وخدمات المزج تعقد الوصول إلى الفاعل الحقيقي، في حين تتيح علانية بعض سجلات البلوك تشين وتربط معاملات وإمكان التحقق اللاحق منها إعادة بناء حركة الأصول وتتبع مساراتها الرقمية.
- 2- توصلت الدراسة إلى أن مخرجات تحليل البلوك تشين ليست متجانسة من حيث طبيعتها أو درجة اليقين التي تعكسها؛ إذ يتدرج التحليل من بيانات أصلية قابلة للتحقق مباشرة من السجل إلى نتائج استنتاجية، كتجميع العناوين وإسنادها ودرجات المخاطر، بما يوجب الفصل بين ما أثبتته السجلات وما استنتجته أداة التحليل.
- 3- انتهت الدراسة إلى أن إسناد المعاملة المشفرة إلى شخص محدد لا يتحقق بمجرد ظهور عنوان رقمي مرتبط به في مسار التحويل؛ لأن العنوان الرقمي لا يساوي الهوية القانونية أو السيطرة الفعلية على المحفظة. ومن ثم، يقوم الإسناد السليم على تضافر بيانات السلسلة مع بيانات المنصات و"اعرف عميلك" والأجهزة والحسابات وغيرها من الأدلة المستقلة.

- 4- كشفت الدراسة أن التكييف القانوني لمخرجات تحليل البلوك تشين في التشريع الإماراتي تكيف متدرج لا موحد؛ فسجل المعاملة قد يمثل دليلاً رقمياً مصدره السلسلة، بينما تمثل المخرجات التحليلية معلومات رقمية مشتقة متفاوتة في طابعها الاستنتاجي، ويظل تقرير الخبير وسيلة لتفسيرها، في حين تشكل الأدلة الخارجية مصادر إثبات مستقلة.
- 5- توصلت الدراسة إلى أن قبول مخرجات التحليل لا يستمد من مقاومة البلوك تشين للتعديل وحدها، وإنما من منظومة متكاملة من الضمانات؛ تشمل مشروعية الحصول على البيانات، وسلامة استخراجها وحفظها وسلسلة حيازتها، وموثوقية منهج التحليل وصلاحية الأداة المستخدمة، وكفاءة القائم به، وإمكان التحقق من النتيجة وإعادة فحصها ومناقشتها قضائياً.
- 6- انتهت الدراسة إلى أن القوة الإثباتية لمخرجات تحليل البلوك تشين متدرجة وليست مطلقة؛ فتأثر بمقدار الاستنتاج، واحتمالات الخطأ، ومصادر الإسناد، وقابلية النتيجة للاختبار المستقل وتساندها مع أدلة أخرى. كما تظل تقديرات قوتها خاضعة لسلطة القاضي الجنائي، مع ضرورة تمكين الدفاع من فحص أساسها الفني، ولا سيما عند استخدام أدوات تجارية مغلقة.

توصيات الدراسة:

1. توصي الدراسة بوضع إطار إجرائي وفني موحد للتعامل مع مخرجات تحليل البلوك تشين في التحقيق والإثبات الجنائي، يقوم على التمييز الصريح بين البيانات الأصلية المسجلة على السلسلة والمخرجات التحليلية المشتقة منها، مع إلزام الجهات المختصة بتوثيق مصدر البيانات، وأداة التحليل وإصدارها، والمنهج المستخدم، وخطوات المعالجة، ومواطن الخطأ ودرجات عدم اليقين؛ بما يمنع إضفاء قوة إثباتية واحدة على مخرجات تختلف في طبيعتها ودرجة الاستنتاج التي تتضمنها.
2. توصي الدراسة بتعزيز التكامل المؤسسي بين تحليل البلوك تشين ومصادر الإثبات المستقلة خارج السلسلة في دولة الإمارات، ولا سيما بيانات "اعرف عميلك"، ومزودي خدمات الأصول الافتراضية، والمؤسسات المالية، وبيانات الحسابات والأجهزة وسجلات الدخول؛ بما يحد من بناء إسناد المعاملة إلى شخص معين على مخرج تحليلي منفرد، خصوصاً في نتائج التجميع أو الإسناد التحليلي، على المخرج التقني منفرداً متى أمكن تدعيمه بأدلة مستقلة تثبت الصلة والسيطرة الفعلية.
3. توصي الدراسة بإقرار ضمانات إجرائية أكثر تحديداً لفحص مخرجات أدوات تحليل البلوك تشين أمام القضاء، ولا سيما الأدوات التجارية المغلقة، بما يكفل للمحكمة والدفاع الوصول إلى القدر اللازم من البيانات والأسس والمنهجيات التي تسمح باختبار النتيجة ومناقشة الخبير وإجراء تحليل مستقل عند الحاجة، مع حماية الأسرار التجارية بتدابير قضائية مناسبة دون تحويل السرية إلى عائق يحول دون الطعن الفعلي في الدليل.

ثالثاً: مقترحات لدراسات مستقبلية

1. دراسة مقارنة لمدى الحجية الإثباتية لمخرجات تحليل البلوك تشين في عدد من الأنظمة القانونية المختلفة، بهدف بيان أوجه الاتفاق والاختلاف في شروط القبول، ومعايير الموثوقية، وسلطة القاضي في تقدير النتائج التحليلية ومناقشتها.
2. بحث الأثر القانوني لاستخدام أدوات تحليل البلوك تشين التجارية المغلفة في الإثبات الجنائي، مع التركيز على متطلبات الشفافية، وإمكان مراجعة المنهج والخوارزمية، والموازنة بين حماية الأسرار التجارية وضمانات المحاكمة العادلة وحقوق الدفاع.
3. دراسة فاعلية التكامل بين بيانات البلوك تشين والبيانات الخارجية في تعزيز دقة الإسناد الجنائي وموثوقيته، ولا سيما بيانات "اعرف عميلك" والأجهزة والمنصات والمؤسسات المالية، وتقييم أثر هذا التكامل في الحد من أخطاء التجميع والإسناد.

لائحة المراجع:

الكتب بالعربية

- 1- المرجان، عبدالرزاق، ومُحَمَّد شوقي، ويوسف السباعي، ومُحَمَّد المنشاوي، إعداد، الدليل الاسترشادي للتعامل مع الأدلة الجنائية الرقمية في الدول العربية، مراجعة سيوكي لي وجلال الهاشل، الرياض: دار جامعة نايف للنشر، جامعة نايف العربية للعلوم الأمنية، 2024، DOI: 10.26735/978-603-8361-78-8.
- المقالات والدراسات المنشورة في المجلات العلمية المحكمة
- 1- الحمدوني، هاجر، «حجية الدليل الرقمي الموثقة بالبلوكشين في الإثبات الجنائي»، مجلة القانون والأعمال الدولية، المجلد 11، العدد 4، الإصدار رقم 65، أغسطس 2026، ص 406-424.
- 2- زروال، الحسين، «البلوك تشين وجريمة غسل الأموال: بين المخاطر التنظيمية وفرص المكافحة»، مجلة القانون والأعمال الدولية، الإصدار رقم 66، مارس 2026، DOI للإصدار: UWRW9962.10.63585.
- 3- الشيخ، مُحَمَّد، «الحجية القانونية والقضائية للدليل الإلكتروني المعتمد في الإثبات الجنائي»، مجلة الشؤون الجنائية والحكامة الأمنية، المجلد 2، العدد 2، 2024.
- 4- الصالبي، وجدان، «غسل الأموال باستخدام العملات المشفرة في ضوء التشريع الجنائي المغربي ومستجدات مشروع قانون الأصول المشفرة»، مجلة القانون والأعمال الدولية، المجلد 11، العدد 4، الإصدار رقم 65، أغسطس 2026، ص 772-791.
- 5- فضيل، عائشة، وعلي بناني الخير، «غسل الأموال والأصول المشفرة بين الخطر الواقعي وضرورة التقنين»، مجلة القانون والأعمال الدولية، الإصدار رقم 64، يونيو 2026، DOI للإصدار: RPD9639.10.63585.
- 6- لواتي، فوزي، وعبد القادر بوبكر، «حجية الدليل الإلكتروني في الإثبات الجنائي»، مجلة الفكر القانوني والسياسي، المجلد 10، العدد 1، 2026، ص 349-360.

7- مصبح، عمر عبد المجيد، «القيمة الإثباتية لسجلات البلوك تشين في نظام العدالة الجنائية: دراسة تحليلية

مقارنة»، *المجلة الدولية للقانون*، المجلد 15، العدد 1، 2026، DOI: 10.29117/irl.2026.0361.

8- المياحي، حيدر، وهبة عبد الأمير حميد، «دور تقنية البلوكتشين في حفظ أدلة الإثبات القانوني: دراسة

تحليلية»، *مجلة جامعة الأنبار للعلوم القانونية والسياسية*، المجلد 16، العدد 2، يونيو 2026، ص 880-903، DOI: 10.37651/aujpls.2025.157839.1477.

9- النعمة، محمد واجد، ومنى م. بالو، وسلوى م. علي، «سلسلة الكتل (Blockchain) والذكاء الاصطناعي

في الأدلة الرقمية: التحديات القضائية ومعايير القبول»، *Journal Port Science Research*، المجلد 9، عدد خاص، 2026، ص 20-33، DOI: 10.36371/port.2026.special.3.

الدوريات والتقارير والمصادر المؤسسية العربية

1- اللجنة الوطنية لمواجهة غسل الأموال ومكافحة تمويل الإرهاب وتمويل انتشار التسليح، اللجنة الفرعية للجهات

الرقابية، *مزود خدمات الأصول الافتراضية: المخاطر والتحديات ونقاط الضعف الناشئة المتعلقة بغسل الأموال وتمويل الإرهاب وتمويل انتشار التسليح في دولة الإمارات المرتبطة بالعملة المستقرة*، دولة الإمارات العربية المتحدة، ديسمبر 2025.

المراجع الأجنبية

1- Adewuyi, Oluleye M., "The Double-Edged Ledger: Cryptocurrency, Financial Crime, and the Potential of Blockchain Forensics," *International Journal of Research and Innovation in Social Science (IJRISS)*, Vol. 9, Issue 5, 2025, pp. 5739-5742, DOI: 10.47772/IJRISS.2025.905000442.

2- Alhawawsheh, Ayman Nawwaf, Qusay Salman Alfalahi, Khaled Ramadan Soltan, Abdulghani Qasem Taher & Luma Ali Al Dhaheri, "Digital Evidence as a Means of Proof in Criminal Proceedings in the UAE," *Access to Justice in Eastern Europe*, Vol. 8, No. 3, 2025, pp. 521-540, DOI: 10.33327/AJEE-18-8.3-a000111.

3- Bhattarai, Abhishek, Abdulhadi Sahin, Maryna Veksler, Ahmet Kurt, Devrim Aras, Carlos Imery & Kemal Akkaya, "Cryptocurrency Forensics Automation: A Deep Learning and NLP-Based Approach for Mobile Platforms," *Discover Computing*, Vol. 28, Article 123, 2025, DOI: 10.1007/s10791-025-09595-1.

4- Chainalysis, “What Is Blockchain Analytics?”, sections on “Clustering and Attribution,” “Graph Analysis,” and “Risk Scoring and Visualization,” accessed 10 September 2026.

5- Chainalysis, “What Is Wallet Attribution?”, sections “On-chain Analysis and Wallet Clustering,” “Off-chain Evidence and Entity Attribution,” “Assigning a Confidence Level,” and “Risks and Common Misconceptions about Wallet Attribution,” accessed 10 September 2026.

6- Financial Action Task Force (FATF), *Targeted Report on Stablecoins and Unhosted Wallets – Peer-to-Peer Transactions*, Paris, 3 March 2026.

7- Gjorgjev, Jelena, M. F. Fajar Ramadhan & Sonny Dhamayana, “Blockchain Forensics – Unmasking Anonymity in Dark Web Transactions,” *International Journal of Criminology and Sociology*, Vol. 14, 2025, pp. 68–75, DOI: 10.6000/1929-4409.2025.14.07.

8- Gong, Yanan, Kam Pui Chow & Siu Ming Yiu, “Improved Bitcoin Simulation Model and Address Heuristic Method,” *Forensic Science International: Digital Investigation*, Vol. 53, Supplement, July 2025, Article 301935, DOI: 10.1016/j.fsidi.2025.301935.

9- Hamzah, Noor Hazfalinda, Khairul Osman, Qi Wei Kong, Atikah Mohd Nasir & Nur Mahiza Md Isa, “Forensic Analysis of Cryptocurrencies: A Comprehensive Overview,” *Asia-Pacific Journal of Information Technology and Multimedia*, Vol. 14, No. 2, 2025, pp. 585–594, DOI: 10.17576/apjitm-2025-1402-15.

10- Lee, Jeongin, Geunyeong Choi, Jihyo Han & Jungheum Park, “Advanced Monero Wallet Forensics: Demystifying Off-Chain Artifacts to Trace Privacy-Preserving Cryptocurrency Transactions,” *Forensic Science*

International: Digital Investigation, Vol. 54, Supplement, October 2025, Article 301988, DOI: 10.1016/j.fsidi.2025.301988.

11- Levine, Brian N., Joanne Pasquarelli & Clay Shields, "Reference Guide on Computer Science," in National Academies of Sciences, Engineering, and Medicine & Federal Judicial Center, *Reference Manual on Scientific Evidence*, 4th ed., Washington, D.C.: The National Academies Press, 2025, pp. 1411–1482, DOI: 10.17226/26919.

12- Lin, Wei-Hsiang & Che-Yen Wen, "A Lawful Metadata-Driven Framework for Linking Encrypted Communication Behavior and Cryptocurrency Wallet Activity in Digital Investigations," *Applied System Innovation*, Vol. 9, No. 4, 2026, Article 73, DOI: 10.3390/asi9040073.

13- Schnoering, Hugo & Michalis Vazirgiannis, "Bitcoin Research with a Transaction Graph Dataset," *Scientific Data*, Vol. 12, Article 404, 2025, DOI: 10.1038/s41597-025-04684-8.

14- Tippe, Pascal & Christoph Deckers, "Unmixing the Mix: Patterns and Challenges in Bitcoin Mixer Investigations," *Forensic Science International: Digital Investigation*, Vol. 52, Supplement, March 2025, Article 301876, DOI: 10.1016/j.fsidi.2025.301876.

15- Wexler, Rebecca, "Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System," *Stanford Law Review*, Vol. 70, 2018, pp. 1343–1429.

16- Yan, Tao, Chuanshan Huang & Claudio J. Tessone, "Tracing Cross-Chain Transactions Between EVM-Based Blockchains: An Analysis of Ethereum-Polygon Bridges," *Ledger*, Vol. 10, 2025, pp. 113–134, DOI: 10.5195/ledger.2025.433.

التشريعات والقرارات واللوائح والقواعد التنظيمية

أ- التشريعات والقرارات الإماراتية

- 1- دستور دولة الإمارات العربية المتحدة.
- 2- قرار مجلس الوزراء رقم (111) لسنة 2022 بشأن تنظيم الأصول الافتراضية ومزودي خدماتها.
- 3- قرار مجلس الوزراء رقم (55) لسنة 2026 بإصدار اللائحة التنفيذية للمرسوم بقانون اتحادي رقم (30) لسنة 2024 بشأن المنصة الرقمية «اعرف عميلك».
- 4- المرسوم بقانون اتحادي رقم (10) لسنة 2025 في شأن مواجهة جرائم غسل الأموال ومكافحة تمويل الإرهاب وتمويل انتشار التسلح.
- 5- المرسوم بقانون اتحادي رقم (30) لسنة 2024 بشأن المنصة الرقمية «اعرف عميلك».
- 6- المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية.
- 7- المرسوم بقانون اتحادي رقم (38) لسنة 2022 بإصدار قانون الإجراءات الجزائية.

ب- اللوائح والقواعد التنظيمية الإماراتية

- 1- هيئة تنظيم الأصول الافتراضية بدبي (VARA)، كتاب قواعد الامتثال وإدارة المخاطر، الجزء الثالث: مكافحة غسل الأموال وتمويل الإرهاب، القسم (د): تقييم المخاطر، النسخة النافذة اعتباراً من 19 يونيو 2025.
- 2- هيئة تنظيم الأصول الافتراضية بدبي (VARA)، كتاب قواعد التكنولوجيا والمعلومات، القسم (د): «المفاتيح التشفيرية وإدارة محافظ الأصول الافتراضية»، النسخة النافذة اعتباراً من 19 يونيو 2025.

ج- القرارات والقواعد القضائية الأجنبية

- 1- المحكمة الشعبية العليا لجمهورية الصين الشعبية، «أحكام المحكمة الشعبية العليا بشأن عدد من المسائل المتعلقة بنظر القضايا أمام محاكم الإنترنت»، 2018.

الأحكام والقضايا القضائية

أ- الأحكام القضائية الإماراتية

- 1- المحكمة الاتحادية العليا، الطعن رقم (257) لسنة 31 القضائية، أمن دولة، جلسة 12 يناير 2004.

ب- الأحكام والقضايا القضائية الأجنبية

- 1- *Hangzhou Huatai Media Culture Media Co., Ltd. v. Shenzhen Daotong Technology Development Co., Ltd.*, Hangzhou Internet Court, (2018) Zhe 0192 Min Chu No. 81.

- 2- *State v. Loomis*, 2016 WI 68, 371 Wis. 2d 235, 881 N.W.2d 749.

- 3- *State v. Pickett*, 466 N.J. Super. 270, 246 A.3d 279 (App. Div. 2021).
- 4- *United States v. Gratkowski*, 964 F.3d 307 (5th Cir. 2020).
- 5- *United States v. Sterlingov*, 719 F. Supp. 3d 65 (D.D.C. 2024), Memorandum Opinion and Order, February 29, 2024.