

حجز العملات الافتراضية للضبطية القضائية و القضاة Seizing Virtual Currencies for Judicial Enforcement Officers and Judges



د. مناصرة يوسف¹

menasra@hotmail.com



تاريخ الإرسال: 2025/02/19 تاريخ القبول: 2025/11/04 تاريخ النشر: 2025/12/06

ملخص:

في ظل التحول الرقمي، انتقلت الأنشطة اليومية إلى العمل عبر الإنترنت مع زيادة اعتمادها على التكنولوجيا، مما دفع المجرمين إلى تكيف أساليبهم بنقل أنشطتهم الإجرامية إلى الفضاء الإلكتروني واستهداف عدد كبير من مستخدمي الإنترنت عالمياً، ويعتمد الجناة بشكل متزايد على العملات المشفرة التي تسهل في ارتكاب الجرائم السيبرانية لما توفره من سرية وعدم الكشف عن الهوية حيث يستهدفها المتسللون والمحتالون بانتظام. مما يستدعي تطوير آليات تطبيق القانون الحديثة و العصرية ونظام عدالة فعال وتعزيز تبادل الخبرات بشأن كيفية البحث عن هذه الأصول المشفرة.

فيما يعاني نظامنا التشريعي من نقص في المبادئ التوجيهية الخاصة بحجز ومصادرة هذه العملات، يهدف هذا المقال إلى تقديم أفضل الممارسات كخطوة أولى ضرورية لتعزيز فعالية التحقيقات السيبرانية واستخراج الأدلة الإلكترونية. كلمات مفتاحية: حجز، مصادرة، عملات افتراضية، بلوكشين، محفظة رقمية.

Abstract:

In light of digital transformation, daily activities have shifted to online operations with an increased reliance on technology. This evolution has prompted criminals to adapt their methods by transferring their illicit activities to the digital realm, thereby targeting a vast number of Internet users globally. Perpetrators increasingly depend on

cryptocurrencies—which facilitate the commission of cybercrimes due to the anonymity and non-disclosure of identity they provide—and are regularly exploited by hackers and fraudsters. Consequently, there is an imperative need to develop modern law enforcement mechanisms, an effective justice system, and to enhance the exchange of expertise on methods for investigating these cryptocurrency assets.

Given that our legislative framework suffers from a deficiency in guidelines pertaining to the seizure and confiscation of such currencies, this article aims to present best practices as an essential first step towards enhancing the effectiveness of cyber investigations and the extraction of electronic evidence.

Keywords: *Seizure, confiscation, virtual currencies, blockchain, digital wallet.*

1- المؤلف المرسل: د. مناصرة يوسف، الإيميل: menasra@hotmail.com

مقدمة :

تُشير التجارب العملية إلى تحول العديد من الشركات والمؤسسات من النشاط المادي إلى العمل عبر الإنترنت مع اعتماد متزايد على التكنولوجيا. وفي هذا السياق، قام المجرمون بتكييف أساليبهم بما يتلاءم مع التطورات الرقمية، حيث انتقلوا إلى استغلال الفضاء الإلكتروني لاستهداف العدد المتزايد من مستخدمي الإنترنت على مستوى العالم. ومن ضمن أنشطتهم الإجرامية، التي تتنوع بين التهرب الضريبي وغسيل الأموال والاتجار بالمخدرات¹، يعتمد الجناة بشكل متزايد على العملات المشفرة لما توفره من سرية وعدم الكشف عن الهوية.

وقد أفادت تقارير يوروبول، ومن بينها تقييم iOCTA لعام 2019 و 2021²، بأن "العملات المشفرة ما زالت تسهل الجرائم السيبرانية" وأن

"المتسللين والمحتالين يستهدفون بانتظام الأصول المشفرة والشركات"، مما يستدعي تطور آليات تطبيق القانون ونظام العدالة³. وفي هذا الإطار، تُعتبر عملية تبادل المعرفة حول أساليب البحث عن أصول العملات المشفرة وتتبعها وتعقبها واستيلاء السلطات عليها واستعادتها أمراً ضرورياً.

وعلى الرغم من قدم ظهور العملات المشفرة، فإن استخدام تقنيات إخفاء الهوية، وطبيعة المعاملات العابرة للحدود، واللوائح المالية غير المتسقة، وعدم انساق التشريعات الوطنية في مكافحة الأنشطة غير المشروعة، يجعلها العملة المفضلة لدى الكثير من المجرمين. ونظراً لافتقار منظومتنا التشريعية إلى مبادئ توجيهية محددة بشأن حجز ومصادرة العملات الافتراضية، فإنه من المفيد الاستعانة بالدليل الأوروبي الذي يعرض أفضل الممارسات والحلول للمشكلات المختلفة من منظور دولي، وذلك لتعزيز فعالية التحقيقات السيبرانية في تفتيش وضبط ومصادرة عائدات الجرائم الإلكترونية والحصول على الأدلة الإلكترونية.

و عليه ، تكمن أهمية الدراسة في مساهمة جزو/ أو مصادرة العملات الافتراضية في استرداد الأموال التي تم الحصول عليها بطرق غير قانونية، مما يمنع المجرمين من الاستفادة منها لاستمرار أنشطتهم الإجرامية. كما تُستخدم العملات الافتراضية في كثير من الأحيان كوسيلة لتبييض الأموال وتمويل الأنشطة الإرهابية، وبالتالي فإن حجزها يُعتبر خطوة هامة لقطع مسارات تمويل الجرائم المنظمة. زد على ذلك، يساهم حجز و/أو مصادرة العملات الافتراضية في تعزيز الثقة في نظام العدالة من خلال إظهار قدرة الجهات القضائية على مواكبة التحديات الرقمية وحماية النظام المالي من الاستغلال غير المشروع.

لذا فإن الأهداف المرجوة من البحث فهي:

- تسليط الضوء على التحديات التي تواجه الجهات القضائية والإنفاذية في حجز ومصادرة العملات الافتراضية، بما في ذلك عدم وجود كيان مركزي وتعقيدات الأدلة الرقمية.
- استعراض وتحليل القوانين والتوجيهات التي تنظم عمليات الحجز والمصادرة، مع التركيز على أفضل الممارسات المتبعة على المستوى الدولي لتطوير التشريعات الوطنية.
- وضع توصيات وإرشادات عملية تساعد في تعزيز قدرات الأجهزة القضائية والإنفاذية على التعامل مع الجرائم الرقمية المرتبطة بالعملات الافتراضية، مما يساهم في حماية النظام المالي والحد من الأنشطة غير المشروعة.

من الأهمية و الأهداف المسطرة، يتبين بأن مسألة حجز العملات المشفرة تكتسب أهمية قصوى في ظل التحول الرقمي المتسارع واعتماد أنماط جديدة في الجرائم المالية والرقمية، مما يفرض تحديات وإشكاليات قانونية وتقنية بالغة الدقة. تُعد هذه الأصول الرقمية، بطبيعتها اللامركزية وتنوع أساليب تخزينها واستخدامها، محور اهتمام أجهزة إنفاذ القانون، إذ تواجه السلطات تحديات كبيرة في تتبعها وحجزها بطريقة تحافظ على سلامة الأدلة دون المساس بحقوق المشتبه بهم، لذا سنجيب على إشكالية كيفية تبسيط إجراءات حجز أو مصادرة العملات الافتراضية في عمل الضبطية القضائية و القضاة؟ في ظل عدم إقرار التشريع الوطني بالعملات الافتراضية⁴ بخلاف العملة الرقمية .

يجدر بالذكر أن الصعوبات المترتبة على حجز العملات المشفرة تتمثل في عدم وجود كيان مركزي يسهل من خلاله إصدار أوامر تجميد أو مصادرة، فضلاً عن طبيعة الأدلة الرقمية التي يمكن إخفاؤها أو تدميرها بسرعة. هذه الإشكالية تدفع إلى ضرورة تطوير مهارات تقنية وقانونية متخصصة لضمان

التعامل الصحيح مع هذه الأدلة الحساسة، وهو ما استدعى اختيار هذا الموضوع لما له من أثر بالغ على كفاءة الجهود القضائية والإنفاذية في مكافحة الجرائم المالية الرقمية.

ومن هنا، ينبع سبب اختيار الموضوع من الحاجة الملحة لتزويد مؤسسات الدولة والجهات القضائية بأسس منهجية مدروسة تساعد في التعرف على التقنيات المستخدمة في تخزين العملات المشفرة وكيفية حجزها بصورة فعالة. وتكمن الفائدة المرجوة في تعزيز قدرات الأجهزة القضائية والأمنية على تتبع الأدلة الرقمية، وضمان استرداد العائدات غير المشروعة دون التنازل عن معايير سلامة الإجراءات القانونية.

تستند المنهجية المتبعة في الإجابة على اشكالية الدراسة إلى التحليل القانوني الوصفي والتقييم الفني لبعض التقنيات الرقمية، مستفيدين في ذلك من التجارب الدولية والتوجيهات القانونية المتخصصة وتتناول محورين رئيسيين، حيث يتناول المحور الأول ماهية حجز و مصادرة العملات الافتراضية أما المحور الثاني يستعرض التخطيط للحجز في سياق العملات المشفرة و ينتهي بخاتمة تقترح أهم التوصيات المستخلصة من البحث.

1. ماهية حجز/ مصادرة العملات الافتراضية

الحجز أو المصادرة هو إجراء قانوني يتم بموجبه الاستيلاء على الممتلكات أو الأدلة المرتبطة بجريمة أو نشاط غير مشروع، سواء كان ذلك بناءً على قرار قضائي أو من خلال تدخل السلطات المختصة باستخدام القوة العامة عند الضرورة⁵. يهدف هذا الإجراء إلى منع الجاني من الاستفادة من العائدات الإجرامية أو استخدام الأدوات التي ساعدت في ارتكاب الجريمة. ومن الأمثلة على ذلك ضبط الأموال أو الأدوات المستخدمة في الجرائم الإلكترونية أو المخدرات أو الجرائم الاقتصادية.

1.1. ما هو الحجز/المصادرة؟

في سياق العملة الافتراضية⁶، يشير الحجز أو المصادرة إلى استيلاء السلطات على الأصول الرقمية التي تم الحصول عليها أو استخدامها في أنشطة غير قانونية، مثل تبييض الأموال أو تمويل الإرهاب. ويعد هذا الأمر أكثر تعقيداً من مصادرة الأصول التقليدية، نظراً لطبيعة العملات المشفرة التي تعتمد على تقنية البلوكتشين وعدم وجود كيان مركزي يتحكم فيها. و عليه، تتطلب عملية الحجز أو المصادرة تخطيطاً دقيقاً⁷ لضمان نجاح التنفيذ دون تعريض الأدلة للخطر أو منح المشتبه به فرصة لإخفاء الأصول الرقمية أو تحويلها و تمر بمراحل⁸ يُمكن حصرها في الآتي:

- التخطيط للدخول

يتضمن التخطيط تحليل المعلومات الأولية للضبطية القضائية مهما كان مصدرها (استعلامات، بلاغ، شكوى معلومة أو مجهولة..الخ)، وتحديد الأطراف المعنية، والحصول على الأدونات القانونية اللازمة (التفتيش، الانتقال، التسرب، التصنت، الخ)، والتنسيق مع الجهات المختصة، مثل وكالات إنفاذ القانون والهيئات القضائية المختصة.

في حالات العملات الافتراضية، قد يتطلب التخطيط تحليل البنية التحتية الرقمية المستخدمة، مثل المحافظ الإلكترونية والمنصات المشفرة، إلى جانب تحديد الوصول إلى الأجهزة أو الحسابات التي تحتوي على هذه الأصول. يمكن أيضاً إشراك خبراء في التكنولوجيا الجنائية لضمان جمع الأدلة بطريقة تتماشى مع المعايير القانونية.

- جمع المعلومات و/أو الكشف عن العملة الافتراضية

يتضمن هذا الإجراء تحديد وتتبع العملات الافتراضية المرتبطة بالجريمة. قد يتم ذلك من خلال تحليل معاملات البلوكتشين، واستخدام أدوات

التحليل الجنائي الرقمي، والتعاون مع منصات تداول العملات المشفرة للحصول على بيانات الحسابات المشبوهة.

نظراً لطبيعة العملات الافتراضية التي قد توفر مستوى معيناً من إخفاء الهوية، فإن تتبع المعاملات يتطلب تقنيات متقدمة، مثل استخدام الذكاء الاصطناعي أو تحليل الأنماط المالية المشبوهة. كما يمكن للسلطات إصدار أوامر قانونية تلزم الجهات الوسيطة، مثل منصات التداول، بالكشف عن بيانات المستخدمين والمعلومات ذات الصلة.

- وضع اليد على العملات الافتراضية

بمجرد تحديد الأصول الرقمية، تتخذ السلطات الإجراءات اللازمة لوضع يدها عليها، وهو ما قد يشمل مصادرة المفاتيح الخاصة (Private Keys) التي تسمح بالتحكم في العملات المشفرة، أو حجز الأجهزة التي تحتوي على المحافظ الإلكترونية، مثل الهواتف الذكية أو أجهزة الحواسيب.

يعد هذا الجانب من المصادرة حساساً للغاية، حيث إن فقدان المفاتيح الخاصة أو أي خطأ تقني قد يؤدي إلى ضياع الأصول إلى الأبد. لذلك، تتبع السلطات إجراءات مشددة لضمان تأمين المفاتيح الخاصة، مثل تخزينها في أماكن آمنة أو نقل الأصول إلى محافظ رسمية تسيطر عليها الدولة.

- إدارة وتحويل العملات الافتراضية المصادرة

بعد المصادرة، يجب على السلطات إدارة هذه الأصول بطريقة قانونية ومؤمنة. في بعض الدول، يتم تحويل العملات المشفرة إلى أصول تقليدية من خلال بيعها في مزادات رسمية أو عبر منصات تداول معتمدة، ثم إيداع العائدات في خزانة الدولة.

كما يجب على الجهات المختصة تطوير آليات لإدارة العملات المصادرة، بما في ذلك إنشاء محافظ رسمية آمنة، والتنسيق مع الجهات المختصة لتحديد مصير الأصول وفقاً للقوانين الوطنية والدولية. في بعض الحالات، قد يتم

الاحتفاظ بالعملات المصادرة لفترة معينة قبل اتخاذ قرار بشأن تصريفها أو إعادة توزيعها وفقاً للإجراءات القضائية.

- الإطار القانوني في الاتحاد الأوروبي

في الاتحاد الأوروبي، يحدد التوجيه 42/2014 EU الإطار القانوني لمصادرة وتجميد عائدات الجريمة⁹، مما يمنح سلطات إنفاذ القانون أدوات قانونية واسعة لتحديد وتجميد وإدارة الأصول الإجرامية. يؤكد التوجيه على ضرورة اتخاذ الدول الأعضاء تدابير فعالة لمصادرة الأدوات والعائدات الإجرامية، سواء كانت مادية أو ذات قيمة معادلة.

يمثل هذا التوجيه خطوة مهمة في مكافحة الجرائم المالية، لا سيما في ظل التطور الرقمي واللجوء المتزايد إلى العملات الافتراضية في العمليات غير المشروعة¹⁰. وهو يلزم الدول الأعضاء بتبني تشريعات تتيح مصادرة العائدات الإجرامية حتى في الحالات التي لا يمكن فيها إثبات العلاقة المباشرة بين الجريمة والأصول المصادرة، مما يعزز من فعالية تطبيق القانون¹¹.

و في الولايات المتحدة الأمريكية¹²، يُعد إنشاء فريق إنفاذ العملات المشفرة الوطني NCET¹³ إحدى أحدث الجهود لمعالجة تحديات العملات المشفرة والأصول الرقمية التي كانت داخل وزارة العدل الأمريكية (DOJ) في عام 2021. وتتمثل مهمة فريق NCET في التعامل مع التحقيقات والملاحقات القضائية المعقدة المتعلقة بإساءة استخدام العملات المشفرة في الجرائم الجنائية، ولا سيما الجرائم التي ترتكبها بورصات العملات الافتراضية، وخدمات الخلط والتعتيم، والجهات الفاعلة في بنية تبييض الأموال. كما يساعد فريق NCET في تتبع واسترداد الأصول التي فقدت بسبب الاحتيال والابتزاز، بما في ذلك مدفوعات العملات المشفرة إلى مجموعات برامج الفدية (رانسوم وير)¹⁴.

2.1. مقارنة بين الأصول المشفرة والأصول العادية

تختلف الأصول المشفرة عن الأصول العادية من حيث البنية والآليات التنظيمية، مما يؤثر بشكل مباشر على طرق التتبع والمصادرة القانونية لهذه الأصول¹⁵. وفيما يلي تحليل مفصل لهذه الفروقات:

أ- السلطة المركزية والتحكم

الأصول العادية : تخضع الأصول التقليدية، مثل الأموال النقدية، والعقارات، والأسهم، لإشراف جهات مركزية مثل البنوك المركزية، والمؤسسات المالية، وسجلات الملكية العقارية. وهذا يجعل عمليات الحجز أو التجميد أو المصادرة أكثر وضوحاً وسهولة، حيث يمكن للسلطات إصدار أوامر قانونية للبنوك أو الجهات المختصة لتنفيذ الإجراءات المطلوبة.

الأصول المشفرة : لا يوجد عادةً كيان مركزي يتحكم في الأصول المشفرة، خصوصاً مع العملات الرقمية اللامركزية مثل البيتكوين والإثيريوم، التي تعمل عبر تقنية البلوكشين. وبالتالي، فإن الحجز أو المصادرة يتطلب وسائل متخصصة، مثل تحديد المفاتيح الخاصة (Private Keys) أو السيطرة على محافظ العملات المشفرة، نظراً لعدم وجود طرف ثالث يمكنه فرض تجميد الأصول.

ب- تتبع المعاملات المالية

الأصول العادية : يمكن تتبع المعاملات المالية التقليدية بسهولة من خلال السجلات المصرفية وتقارير الحوالات المالية، حيث تلتزم البنوك والمؤسسات المالية بإجراءات الامتثال للقوانين المالية، مثل مكافحة تبييض الأموال (AML) ومتطلبات اعرف عميلك (KYC).

الأصول المشفرة : رغم عدم وجود طرف مركزي، إلا أن المعاملات التي تتم عبر البلوكشين تكون مسجلة ومتاحة للعامة، مما يسمح بتحليل الأنماط المالية وتتبع التدفقات النقدية، ولكن دون ربط مباشر بالهويات الشخصية للمستخدمين. وفي بعض الحالات، قد يتم اللجوء إلى البيانات المالية للمشتبه به،

حيث تحتفظ بعض البنوك والمؤسسات المالية بسجلات للمعاملات المرتبطة بالعملات الافتراضية، مما قد يساعد في تحديد هوية المشتبه به أو وسائله المفضلة في تداول الأصول المشفرة.

ت- المصادرة والتجميد

الأصول العادية : عندما تتخذ السلطات قرارًا بمصادرة أو تجميد الأصول العادية، يمكن تنفيذ ذلك بسهولة من خلال إصدار أوامر قضائية تلزم المؤسسات المالية أو الهيئات الحكومية المختصة باتخاذ الإجراءات اللازمة، مثل تجميد الحسابات البنكية أو الحجز على الممتلكات.

الأصول المشفرة : يختلف الأمر بشكل جذري مع الأصول المشفرة، حيث لا يمكن تجميد الحسابات بالطرق التقليدية، لأن الوصول إلى العملات المشفرة يتطلب السيطرة على المفاتيح الخاصة. لذا، فإن مصادرة العملات المشفرة تعتمد على الاستحواذ على هذه المفاتيح أو السيطرة على المحافظ الرقمية الخاصة بالمشتبه بهم. وقد تطورت أساليب إنفاذ القانون لتشمل التعاون مع منصات تداول العملات المشفرة، واستخدام أدوات تحليل البلوكشين لتعقب الأموال المشبوهة¹⁶.

ث- استخدام الأصول في الجرائم المالية

الأصول العادية : رغم إمكانية استخدامها في الجرائم المالية، إلا أن الأنظمة المصرفية المطبقة حاليًا تضع قيودًا على المعاملات غير المشروعة، مما يجعل من الصعب استخدامها بحرية في أنشطة مثل تبييض الأموال وتمويل الإرهاب.

الأصول المشفرة : توفر درجة من إخفاء الهوية وإمكانية التحويل عبر الحدود دون تدخل البنوك، مما يجعلها جذابة للأنشطة غير المشروعة. ومع ذلك، فإن التطورات في تحليل بيانات البلوكشين أدت إلى تحسين قدرة السلطات على تعقب هذه الأصول وكشف الجرائم المرتبطة بها¹⁷.

و عليه، بينما توفر الأصول العادية إطاراً قانونياً وتنظيمياً واضحاً يسمح بالسيطرة عليها بسهولة، فإن الأصول المشفرة تفرض تحديات جديدة بسبب طبيعتها اللامركزية وصعوبة تتبعها بالطرق التقليدية. ومع ذلك، يمكن للجهات المختصة الاستفادة من أدوات التحليل الرقمي والبيانات المالية للمشتبه بهم لتحديد طرق الوصول إلى هذه الأصول، وإن كان ذلك يتطلب نهجاً أكثر تعقيداً من الحجز أو المصادرة التقليدية.

2. التخطيط للحجز في سياق العملات المشفرة

يعد التخطيط المسبق لعملية الضبط أمراً جوهرياً لضمان نجاح أي إجراء قانوني يتعلق بحجز أو مصادرة العملات المشفرة. نظراً للطبيعة الفريدة لهذه الأصول الرقمية، يتطلب ضبطها نهجاً قانونياً وتقنياً دقيقاً يأخذ في الاعتبار الأطر التنظيمية المختلفة، بالإضافة إلى التحديات المرتبطة بطرق تخزينها والوصول إليها¹⁸. وفيما يلي شرح تفصيلي لأهم الجوانب التي ينبغي مراعاتها عند التخطيط لحجز العملات المشفرة.

أ- مدى وجود الإطار القانوني

- التباين في التشريعات الوطنية

على الرغم من أن العملات المشفرة تعمل ضمن نظام بيئي عالمي بلا حدود واضحة، فإن الأطر القانونية التي تنظم حجزها أو مصادرتها تختلف من بلد إلى آخر. في بعض الدول، توجد قوانين واضحة تنظم مصادرة الأصول الرقمية وتحدد آليات تنفيذها¹⁹، بينما تفتقر دول أخرى إلى تشريعات صريحة تتناول العملات المشفرة، ما يفرض تحديات قانونية في تنفيذ عمليات الحجز.

حتى في الاتحاد الأوروبي، حيث يوجد التوجيه EU/42/2014 بشأن تجميد ومصادرة عائدات الجرائم، لا تزال هناك اختلافات في كيفية تعامل الدول الأعضاء مع العملات المشفرة. ففي بعض البلدان، يتم تطبيق القوانين التقليدية المتعلقة بحجز الأصول المالية على العملات المشفرة، بينما لا تزال دول أخرى تفتقر إلى تشريعات صريحة تتعامل مع هذه الفئة من الأصول من بينها الجزائر.

- ضرورة الامتثال للقوانين الوطنية والدولية

- لضمان قانونية عملية الحجز وتجنب أي طعون قضائية مستقبلية، يتعين على الجهات المختصة التحقق مما إذا كان الإطار القانوني في الدولة المستهدفة يسمح بحجز العملات المشفرة. ومن المهم فهم القوانين المحلية المتعلقة بما يلي:
- إجراءات حجز الأصول المالية والتطبيقات الممكنة على العملات المشفرة
- صلاحيات السلطات القضائية وإنفاذ القانون في التعامل مع الأصول الرقمية
- القيود القانونية على الأدلة الرقمية وطرق الحصول عليها.
- التعاون الدولي في ضبط ومصادرة الأصول المشفرة

يجب أيضًا الانتباه إلى المخاطر القانونية التي قد تنشأ من الحصول على الأدلة بطريقة غير مشروعة، مثل اختراق المحافظ الرقمية دون إذن قضائي أو الاستيلاء غير القانوني على المفاتيح الخاصة. قد يؤدي ذلك إلى استبعاد الأدلة لاحقًا، مما يعرقل سير القضية القضائية.

ب- أهمية التخطيط الجيد لعملية الضبط

- الغايات القانونية لحجز العملات المشفرة

- لا يتم تنفيذ عمليات الحجز لمجرد الاستيلاء على الأصول، بل لتحقيق أهداف قانونية محددة، من بينها:
- استرداد الأموال المسروقة أو الاحتيالية : في حالات الاحتيال الإلكتروني، يمكن أن تكون العملات المشفرة التي تم الاستيلاء عليها جزءًا من أموال الضحايا.
- مصادرة العائدات غير المشروعة : قد يكون الحجز وسيلة لاستعادة الأرباح التي حصل عليها المجرمون من أنشطة غير قانونية، مثل تجارة المخدرات أو تبويض الأموال.
- تنفيذ العقوبات المالية : في بعض القضايا، يمكن أن يشكل الحجز أو المصادرة وسيلة بديلة أو مكملية للعقوبات الجنائية التقليدية، مثل الحبس.

إن حجز العائدات الإجرامية يمكن أن يكون أكثر تأثيراً على بعض المجرمين من عقوبة السجن نفسها، ما يستلزم تكثيف الجهود الأمنية والقانونية لضمان نجاح عملية المصادرة. لذلك، ينبغي لأجهزة إنفاذ القانون والجهات القضائية المعنية إبلاء أهمية قصوى لهذه الإجراءات، باعتبارها عنصراً أساسياً في مكافحة الجرائم المالية والرقمية.

- التخطيط كجزء من التحقيق الجنائي

يعد التخطيط الدقيق أمراً ضرورياً لضمان نجاح التحقيقات الأولية في الجرائم المتعلقة بالعملات المشفرة، حيث ينبغي:

- تحديد أماكن تخزين العملات المشفرة : هل يتم الاحتفاظ بها في محافظ رقمية على أجهزة محلية أم في محافظ عبر الإنترنت؟
- تحديد الأطراف الفاعلة : هل يتحكم المشتبه به شخصياً في الأصول، أم أن هناك وسطاء أو منصات تداول تدبر هذه الأموال؟
- الحصول على الأدلة الرقمية بطرق قانونية : يجب التأكد من أن جميع الأدلة، بما في ذلك المفاتيح الخاصة، تم الحصول عليها وفقاً للإجراءات القانونية المعتمدة.

ج- أماكن تخزين العملات المشفرة والتحديات القانونية المرتبطة بها

- طرق تخزين العملات المشفرة

يمكن أن تُخزن العملات المشفرة في أماكن متعددة، ولكل منها تحديات قانونية وتقنية مختلفة:

- محافظ الحفظ (Custodial Wallets) : حيث يتم الاحتفاظ بالأصول بواسطة طرف ثالث مثل منصات التداول. وهنا يمكن للسلطات إصدار أوامر قانونية لهذه المنصات لحجز الأصول أو تجميدها.
- محافظ غير الحفظ (Non-Custodial Wallets) : تكون المفاتيح الخاصة بحوزة المستخدم نفسه، مما يجعل الوصول إلى الأموال أكثر تعقيداً.

- التخزين البارد (Cold Storage) : يمكن تخزين العملات المشفرة في أجهزة غير متصلة بالإنترنت، مثل محافظ الأجهزة (Hardware Wallets) أو حتى على ورقة مكتوبة (Paper Wallet).

- التحديات في مصادرة المحافظ غير الحفظية

عندما تكون الأموال مخزنة في محافظ غير احتجازية، فإن السيطرة عليها تصبح أكثر تعقيداً، نظراً لأن المشتبه به وحده (أو شركاؤه) يتحكم في المفاتيح الخاصة²⁰. وهذا يتطلب استراتيجيات مختلفة، مثل:

- محاولة الوصول إلى الجهاز الذي يحتوي على المحفظة
- إقناع المشتبه به بالكشف عن المفاتيح الخاصة (في بعض الدول، قد يكون إجبار المشتبه عليه على الكشف عن مفاتيحه الخاصة غير قانوني)
- التعاون مع منصات التداول (VASPs) للحصول على بيانات المستخدم ومعاملاته

وبالتالي، فإن ضبط العملات المشفرة المخزنة ذاتياً يتطلب استخدام أساليب قانونية وتقنية متطورة لضمان نجاح العملية دون المساس بحقوق المشتبه به أو الطعن في الإجراءات القانونية لاحقاً.

ومنه فإن مصادرة العملات المشفرة عملية معقدة تتطلب استعداداً دقيقاً واستراتيجية مدروسة تشمل:

1. التحقق من الإطار القانوني لضمان الامتثال للقوانين المحلية والدولية.
2. تحديد الهدف من الحجز، سواء كان لاسترداد أموال الضحايا، أو مصادرة العائدات الإجرامية، أو تنفيذ العقوبات المالية.
3. فهم تقنيات التخزين المختلفة للعملات المشفرة وكيفية الوصول إليها بطرق قانونية.
4. التعاون مع الجهات المختصة، مثل منصات تداول العملات المشفرة، لتسهيل عملية المصادرة.

من خلال التخطيط الفعال والتنفيذ القانوني السليم، يمكن إنفاذ القانون التعامل مع الجرائم المالية المرتبطة بالعملات المشفرة بطريقة أكثر كفاءة وفعالية، مما يعزز من قدرة الدولة على مكافحة الأنشطة غير المشروعة في المجال الرقمي.

1.2. التحديات و الرهانات في حجز العملات المشفرة

يُعد حجز العملات المشفرة من أكثر العمليات تعقيداً في المجال القانوني والتقني، نظراً للطبيعة الفريدة لهذه الأصول الرقمية. فهي لا تخضع لسلطة مركزية، ويمكن تخزينها بطرق متعددة تجعل الوصول إليها أمراً صعباً، مما يستدعي مهارات وكفاءات متخصصة لضبطها بشكل قانوني ناجح. وفي هذا السياق، يعد تدريب ضباط الشرطة القضائية، ووحدات الدرك الوطني، والجمارك على التقنيات المرتبطة بالعملات المشفرة ضرورة لا غنى عنها، لا سيما في ظل تنامي استخدامها في القضايا الجزائية والمدنية.

أ- ضرورة التخصص في حجز العملات المشفرة

- تعقيد طبيعة الأصول الرقمية

تتميز العملات المشفرة بخصائص تجعل من الصعب الاستيلاء عليها مقارنة بالأصول المالية التقليدية. فبدلاً من أن تكون الأموال محتجزة في حساب مصرفي يمكن تجميده بأمر قضائي، قد تكون العملات المشفرة مخزنة في محافظ رقمية لا يمكن الوصول إليها إلا من خلال المفاتيح الخاصة التي يحتفظ بها المستخدم نفسه.

ونظراً لهذه التحديات، فمن الضروري أن يتم إسناد مهمة حجز هذه الأصول إلى أفراد ذوي خبرة متخصصة، مثل وحدات إنفاذ القانون أو الجمارك التي تمتلك معرفة تقنية متقدمة في هذا المجال. ويجب أن يتم تعزيز هذه المعرفة من خلال التدريب المستمر والممارسة العملية لضمان التعامل الفعال مع القضايا ذات الصلة.

- دور أجهزة إنفاذ القانون في مكافحة الجرائم المرتبطة بالعملات المشفرة مع تزايد استخدام العملات المشفرة في الجرائم المالية، مثل تبلييض الأموال وتمويل الإرهاب، يصبح من الضروري أن يكون ضباط الشرطة القضائية وقضاة التحقيق على دراية بكيفية تحديد الأصول المشفرة المشبوهة. ويشمل ذلك معرفة أبرز العملات المشفرة المستخدمة في الأنشطة الإجرامية، مثل بيتكوين (BTC) و مونيرو (XMR) و زد كاش (ZEC) ، وفهم تأثيراتها القانونية والتقنية في التحقيقات²¹.

ب- رفع مستوى الوعي والفهم التقني داخل الأجهزة القضائية والأمنية

- التعرف على المفاهيم الأساسية المرتبطة بالعملات المشفرة

حتى يكون حجز العملات المشفرة فعالاً، ينبغي للجهات المكلفة بالتحقيق أن تمتلك معرفة أساسية حول بعض المفاهيم الجوهرية، مثل:

- رموز QR المستخدمة لنقل العناوين بين المحافظ الرقمية.
- العبارات التذكيرية (Seed Phrase) التي تسمح باستعادة المحافظ الرقمية.
- المفاتيح العامة والخاصة التي تتحكم في الأصول المشفرة.
- تحديد أنواع المحافظ الرقمية ، سواء كانت محافظ سطح المكتب، الهواتف الذكية، أو محافظ الأجهزة (Hardware Wallets).

إن اكتساب هذه المعرفة يمكن أن يساعد وكلاء النيابة العامة، وضباط الشرطة القضائية، وقضاة التحقيق في التعامل مع الأدلة الرقمية المرتبطة بالعملات المشفرة بطريقة أكثر كفاءة.

- أهمية معرفة تنسيقات عناوين العملات المشفرة

من الجوانب الحاسمة في عملية الحجز هو القدرة على التمييز بين مختلف تنسيقات عناوين العملات المشفرة. فقد يؤدي الخطأ في التعرف على نوع العنوان إلى الفشل في نقل الأموال المضبوطة أو حتى فقدانها نهائياً. على سبيل المثال:

- عناوين البيتكوين (BTC) تبدأ عادةً بـ 1 أو 3 أو bc1 .

- عناوين الإيثريوم (ETH) تبدأ دائماً ب x0 .
- إذا واجه المحققون عنواناً غير معروف، فمن الممكن استخدام أدوات تحليل عناوين العملات المشفرة المتاحة على الإنترنت لتحديد نوع العملة المشفرة المرتبطة به. كما أن بعض العملات المشفرة نادرة الاستخدام، مما قد يجعل تحديدها أكثر صعوبة، وبالتالي يستلزم أدوات وخبرات إضافية.
- ج- أهمية معرفة أنواع المحافظ الرقمية
- فهم الاختلافات بين المحافظ الرقمية
- تختلف طرق حجز العملات المشفرة تبعاً لنوع المحفظة المستخدمة، حيث يمكن تصنيفها إلى عدة فئات²²:
- محافظ الأجهزة (Hardware Wallets) مثل Ledger و Trezor ، والتي توفر أماناً عالياً ولكنها تتطلب الوصول المادي إلى الجهاز.
- محافظ سطح المكتب (Desktop Wallets) مثل Electrum ، والتي يتم تشغيلها على الحواسيب الشخصية.
- محافظ الهاتف المحمول (Mobile Wallets) مثل Trust Wallet و Mycelium ، والتي تكون أكثر سهولة في النقل ولكنها أقل أماناً إذا لم تكن مشفرة بشكل جيد.
- محافظ الويب (Web Wallets) التي يتم تشغيلها من خلال منصات الإنترنت، مثل المحافظ الموجودة على منصات التداول (Kraken، Binance).
- تأثير نوع المحفظة على آلية الحجز
- لكل نوع من المحافظ طريقة مختلفة في الحجز، مما يتطلب اتباع إجراءات قانونية وتقنية خاصة بها²³. على سبيل المثال:
- إذا كانت العملات المشفرة مخزنة في محفظة حفظ (Custodial Wallet) لدى منصة تداول، فيمكن إصدار أمر قانوني لتجميدها أو مصادرتها.
- أما إذا كانت مخزنة في محفظة غير احتجازية (Non-Custodial Wallet)، فسيكون الوصول إلى المفاتيح الخاصة أمراً بالغ الصعوبة، مما يستدعي

استراتيجيات أخرى مثل إقناع المشتبه به بالكشف عنها أو تحليل أجهزته الرقمية.

بعض المحافظ تدعم عملة مشفرة واحدة فقط، مثل Bitcoin Core ، في حين أن محافظ أخرى مثل Exodus تدعم العديد من العملات المشفرة. لذا، ينبغي على جهات التحقيق التأكد من نوع المحفظة المستخدمة، وطريقة استرداد الأموال منها، وفقاً للإجراءات القانونية الصحيحة.

2.2. مرحلة البحث عند حجز العملات المشفرة

تعد مرحلة البحث والتحري خطوة حاسمة في إجراءات حجز العملات المشفرة، حيث يجب تحديد الأدلة الرقمية المتعلقة بالمحفظة المشفرة والمفاتيح الخاصة والعناصر الأخرى التي تتيح الوصول إلى الأصول الافتراضية. ونظراً للطبيعة غير الملموسة لهذه الأصول، يواجه ضباط الشرطة القضائية تحديات كبيرة في العثور عليها وتحديد هويتها وحجزها بطريقة قانونية وفعالة²⁴.

أ- العناصر المستهدفة في عملية البحث

عند تنفيذ أمر تفتيش أو حجز يتعلق بالعملات المشفرة، هناك مجموعة من العناصر الأساسية التي ينبغي البحث عنها، وتشمل ما يلي:

1. العناوين العامة/مفاتيح العملات المشفرة

- تمثل هذه العناوين الوجهة التي يتم إرسال العملات المشفرة إليها أو استقبالها منها.

- يمكن العثور عليها في السجلات الرقمية، أو برامج المحفظة المشفرة، أو حتى في مذكرات مكتوبة يدوياً.

2. المفاتيح الخاصة وقوائم العبارات التذكيرية (Seed Phrases)

- المفاتيح الخاصة هي المعلومات الأكثر حساسية، حيث تسمح بالوصول الكامل إلى الأموال المشفرة.

- غالباً ما تُحزن العبارات التذكيرية على الورق أو الأجهزة الرقمية، وتتكون عادةً من 12 إلى 24 كلمة.

- يمكن العثور عليها مكتوبة على ورق، محفورة على معدن، أو حتى مخبأة في صورة أو ملف رقمي مشفر.
- 3. رموز الاستجابة السريعة (QR Codes)**
 - تُستخدم في المحافظ الرقمية لسهولة تبادل العناوين وإتمام المعاملات.
 - قد تكون مطبوعة أو مخزنة في صور على الهاتف المحمول أو الكمبيوتر.
- 4. أرقام التعريف الشخصية (PIN Codes) وكلمات المرور**
 - تُستخدم لحماية الوصول إلى المحافظ الرقمية أو تطبيقات المحفظة المثبتة على الأجهزة.
 - قد تكون مكتوبة في ملاحظات شخصية أو مخزنة في تطبيقات إدارة كلمات المرور.
- 5. أجهزة المحافظ الرقمية (Hardware Wallets)**
 - تشمل أجهزة مثل Ledger Nano و Trezor ، والتي تحتفظ بالمفاتيح الخاصة في وضع غير متصل بالإنترنت.
 - عادةً ما تكون بحجم مفتاح USB ويمكن إخفاؤها بسهولة.
- 6. برامج المحافظ المشفرة على الحواسيب أو الهواتف الذكية**
 - يمكن العثور على برامج المحافظ مثل Exodus أو Electrum على الحواسيب الشخصية أو الهواتف المحمولة.
 - يتطلب فحص هذه الأجهزة بحثاً شاملاً عن تطبيقات المحافظ أو ملفات التكوين الخاصة بها.
- 7. معدات التعدين (Mining Equipment)**
 - قد تحتوي الأجهزة المخصصة لتعدين العملات المشفرة على محافظ رقمية أو بيانات متعلقة بمعاملات التشفير.
 - تتضمن هذه المعدات بطاقات الرسومات القوية (GPUs) أو أجهزة التعدين المتخصصة (ASICs).
- 8. الأدلة الرقمية الأخرى**

- يمكن أن تشمل هذه الأدلة رسائل البريد الإلكتروني، المحادثات المشفرة، أو سجلات المعاملات المالية التي تربط المتهم باستخدام العملات المشفرة.
- قد تكون محفوظة على وحدات تخزين USB، أو محركات أقراص خارجية، أو حتى في السحابة الإلكترونية.
- ب- أماكن البحث عن الأدلة الرقمية المتعلقة بالعملات المشفرة
تتطلب طبيعة العملات المشفرة غير الملموسة توسيع نطاق البحث عن الأدلة الرقمية في أماكن مختلفة، بما في ذلك:

1. أثناء تفتيش المباني والممتلكات

- قد يتم العثور على عبارات التذكير أو المفاتيح الخاصة مكتوبة على الورق في الأدراج، أو مخابأة بين الأوراق الشخصية.
- من الممكن أيضاً أن تكون أجهزة المحافظ الرقمية (مثل USB Wallets) مخابأة في أماكن يصعب الوصول إليها.

2. عند تفتيش المشتبه به شخصياً

- قد يحمل المشتبه به أوراقاً مكتوب عليها العبارات التذكيرية أو أكواد المحافظ في جيبه أو محفظته الشخصية.
- يمكن أيضاً أن تكون كلمات المرور أو المعلومات المهمة مخزنة على هاتفه المحمول أو جهازه اللوحي.

3. عند تحليل الأجهزة الإلكترونية

- تحتوي أجهزة الحاسوب والهواتف الذكية على تطبيقات محفظة أو ملفات نصية تخزن معلومات تتعلق بالعملات المشفرة.
- يمكن لمختبرات التحليل الرقمي استخراج البيانات المخزنة في الذاكرة وتحليلها لتحديد أي أدلة متعلقة بالعملات المشفرة.

4. في منصات التخزين السحابي والخوادم عن بُعد

- بعض المشتبه بهم يستخدمون التخزين السحابي لحفظ مفاتيحهم الخاصة أو عبارات التذكير، مما يتطلب الحصول على أوامر قانونية للوصول إلى هذه البيانات.
- يمكن أن تكون هذه المعلومات مشفرة، مما يستدعي استخدام أدوات متخصصة لفك التشفير وتحليل المحتوى.

ج- التحديات المرتبطة بالبحث عن العملات المشفرة

1. سهولة إخفاء العملات المشفرة

- على عكس الأموال النقدية، التي تحتاج إلى مكان مادي لتخزينها، يمكن حفظ العملات المشفرة في أي مكان رقمي، مثل ذاكرة فلاش صغيرة، أو حتى في صورة مشفرة على السحابة.
- يمكن أن يؤدي ذلك إلى تعقيد عمليات التفتيش، حيث قد لا يكون هناك أي دليل مادي واضح يدل على وجود أصول مشفرة.

2. إمكانية تدمير الأدلة بسرعة

- يمكن لمشتبه به مسح محفظته الرقمية أو إعادة ضبط أجهزته الإلكترونية خلال ثوانٍ قليلة.
- من الممكن أيضًا أن يستخدم المشتبه به تطبيقات تحذف المعلومات تلقائيًا بعد فترة زمنية معينة.

3. اختلاف إجراءات الحجز تبعًا لنوع المحفظة

- تختلف آليات الحجز إذا كانت العملة المشفرة مخزنة في محفظة حفظ (Custodial Wallet) لدى منصة تداول مركزية، حيث يمكن إصدار أوامر قضائية لتجميد الحسابات.
- أما في المحافظ غير الحفظية (Non-Custodial Wallets)، فقد يكون الوصول إليها أصعب بكثير، حيث يحتاج التحقيق إلى العثور على المفتاح الخاص أو العبارة التذكيرية.
- د- التخطيط المسبق لعمليات البحث والتفتيش

نظرًا لهذه التحديات، يجب اتخاذ بعض التدابير التحضيرية قبل تنفيذ أوامر التفتيش، مثل:

1. تحليل المعلومات المتوفرة مسبقًا عن المشتبه به
- إذا كان المشتبه به معروفًا بتعامله بالعملات المشفرة، يجب فحص سجلات معاملاته المالية وعلاقاته المحتملة بالمنصات الرقمية.
2. استخدام التكنولوجيا المتقدمة في البحث عن الأدلة
- يمكن الاستعانة بخبراء الجرائم السيبرانية للتحليل الرقمي للأجهزة المضبوطة.
- استخدام أدوات البحث المتخصصة لتحديد المحافظ الرقمية والعناوين المرتبطة بها.
3. اتخاذ الاحتياطات لتجنب فقدان الأدلة
- عند العثور على مفتاح خاص أو عبارة تذكيرية، يجب التعامل معها بحذر شديد، حيث أن أي خطأ قد يؤدي إلى فقدان إمكانية الوصول إلى الأموال المصادرة.
- في بعض الحالات، قد يكون من الضروري تسجيل الجلسة بالفيديو عند العثور على أدلة رقمية حساسة لحمايتها من التلاعب أو الضياع.

الخاتمة:

من خلال اللحة الوجيزة في هذا المقال لعملية الحجز و المصادرة للعملات الافتراضية، توصلنا إلى أن عمليات البحث عن العملات المشفرة تتطلب مستوى عالٍ من الدقة والخبرة، نظرًا للطبيعة الفريدة لهذه الأصول وإمكانية إخفائها بسهولة. ولذلك، فإن نجاح عمليات الحجز يعتمد على التخطيط الجيد، والاستعانة بالخبراء الرقميين، واتخاذ الإجراءات اللازمة لحماية الأدلة من التلف أو الضياع.

ومن خلال الجمع بين المعرفة التقنية والإجراءات القانونية الصارمة، يمكن تعزيز فعالية جهود إنفاذ القانون في مكافحة الجرائم المالية الرقمية وضبط العائدات غير المشروعة المتأتية من المعاملات المشفرة.

إن حجز العملات المشفرة يتطلب مزيجًا من المعرفة القانونية والتقنية لضمان تحقيق نتائج فعالة دون المساس بالإجراءات القانونية السليمة. و لا يمكن أن يكون الفراغ التشريعي في الوقت الحالي حاجزا و حائلا دون تعقب العملات المشفرة، بل يكمن التحدي الحقيقي في تزويد المحققين بالأدوات والمهارات الضرورية لتتبع وتعقب العملات المشفرة.

أبرز النتائج المتوصل إليها

(1) أدت عملية التحول الرقمي إلى انتقال الأنشطة اليومية إلى البيئات الإلكترونية، مما دفع المجرمين إلى تكييف أنشطتهم الإجرامية عبر الفضاء الرقمي.

(2) اعتمد الجناة على العملات المشفرة لاستغلال سرية هويتها وطبيعة المعاملات العابرة للحدود.

(3) أشارت تقارير يوروبول إلى أن هذه العملات تسهل الجرائم السيبرانية باستهدافها بانتظام.

(4) واجهت السلطات تحديات كبيرة في حجز هذه الأصول نظرًا لعدم وجود كيان مركزي ونقص المبادئ التوجيهية التشريعية.

(5) لذا، يتطلب الأمر تطوير مهارات قانونية وتقنية وتعزيز تبادل المعرفة بالاستعانة بأفضل الممارسات الدولية لتحسين فعالية التحقيقات والإجراءات القانونية.

الاقتراحات و التوصيات²⁵:

ويجب على ضبطية قضائية و قضاة وكلاء الجمهورية و قضاة التحقيق وأجهزة إنفاذ القانون:

- (1) تعزيز قدراتها عبر التدريب المستمر لفهم تعقيدات الأصول الرقمية.
- (2) رفع مستوى الوعي بالمفاهيم الأساسية المتعلقة بالعملات المشفرة داخل الأجهزة القضائية.
- (3) تطوير قوانين و أنظمة مخصصة لحجز الأصول الرقمية -وفقاً لنوع المحفظة المستخدمة- إحتراماً لمبدأ الشرعية.
- (4) التعاون مع الجهات المتخصصة مثل وحدات الجرائم السيبرانية والمنصات الرقمية للحصول على المعلومات اللازمة.
- ختاماً، من خلال الجمع بين الفهم العميق للتكنولوجيا والالتزام بالمعايير القانونية، يمكن إنجاح عمليات الحجز والمصادرة، وتحقيق العدالة في القضايا التي تتضمن العملات المشفرة.

قائمة المراجع:

1. المؤلفات:

1. Alice Barbet-massin, William O'rorke, Faustine Fleuret, Claire Pion, , Alexandre Lourimidroit des crypto-actifs et de la blockchain, paris, lexisnexis, 2020.
2. Enée Bussac, Blockchain et monnaies numériques L'avènement de l'économie en temps réel, Collection : Finance, : Dunod, 224 pages, juin 2022
3. Claire Balva (Auteur), Alexandre Stachtchenko, Gwendal Fossois, Bitcoin & cryptomonnaies faciles - Comprendre les monnaies numériques et leurs enjeux économiques et politiques: Comprendre les monnaies numériques et leurs enjeux économiques et politiques Broché – Grand livre, First, 2022
2. المقالات و المذكرات:

1. Clément, S. et Lelieur, J. (2021) . La conformité anti-blanchiment face aux crypto-actifs. Revue de science criminelle

- et de droit pénal comparé, N° 1(1), 15-27.
<https://doi.org/10.3917/rsc.2101.0015>.
2. Charlotte Andrée Saumagne. La confiscation et le recouvrement des produits du crime dans l'Union européenne. Droit. Université de Pau et des Pays de l'Adour, 2021. Français.
 3. Dougherty, Thomas, and Nevenka Lastrić Đurić. "The United States approach to the investigation and prosecution of cybercrime and cryptocurrency crime." *Hrvatski ljetopis za kaznene znanosti i praksu* 29.2 (2022): 409-431.
 4. "Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team", October 6, 2021, <https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team>, accessed August 1, 2022.
 5. Goldbarsht, Doron. "Adapting confiscation and anti-money laundering laws to the digital economy: exploring the Australian interplay between proceeds and technology." *Journal of Money Laundering Control* 27.3 (2023): 472-488.
 6. Marty, Marie. « Actualités législatives de l'Union européenne ». *Revue pénale luxembourgeoise*, 2019/2 N° 2, 2019. p.35-40. CAIRN.INFO, droit.cairn.info/revue-revue-penale-luxembourgeoise-2019-2-page-35?lang=fr).
 7. Galienni, Stéphane. et al. « Chapitre 13. Le cryptowallet ou le portefeuille Web3 ». *La vague Web3 Maîtriser les nouveaux codes du marketing digital 3.0 Blockchain, NFT, DAO, métavers...* Dunod, 2023. p.109-112. CAIRN.INFO, shs.cairn.info/la-vague-web3--9782100845835-page-109?lang=fr.

8. Guide sur la saisie des cryptomonnaies, Version 1.0, Bureau de programme du conseil de l'europe sur la cybercriminalite, 10 fevrier 2021.
9. Jérémy Bourgaïs, La saisie pénale des actifs numériques : une saisie virtuelle ? Issu de Gazette du Palais - n°05 - page 10, Date de parution : 14/02/2023
10. Julien Cabrespines, Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES , Frédéric Ruiz Genève , Les cryptoactifs sont-ils une classe d'actifs à part entière , 08.07.2023 Haute École de Gestion de Genève (HEG-GE).
11. Patrick Gielen, [Le point sur...] Saisies des biens digitaux en droit international, Lexbase Contentieux et Recouvrement, septembre 2024.
12. Thibaud Guillebon. Les monnaies virtuelles : essai sur l'intégration d'une nouvelle classe d'actifs dans les concepts fondamentaux du droit privé. Droit. Université de Bordeaux, 2022. Français. NNT : 2022BORD0283. tel-04633022v2
13. مكتب الأمم المتحدة المعني بالمخدرات و الجريمة، دليل مسرح الجريمة والأدلة المادية، الأمم المتحدة ، نيويورك 2009،
3. المؤتمرات:
1. المؤتمر العالمي الخامس بشأن التمويل الجنائي والعملات المشفرة ، منشورة بتاريخ 01-2022، الناشر: معهد بازل للحوكمة؛ الإنترنت؛ اليوربول Combating virtual assets based money laundering and crypto-enabled crime
4. مواقع الانترنت:
1. <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>.
2. https://www.unodc.org/documents/scientific/ST_NAR_39_A.pdf
3. :<https://www.arabictrader.com/ar/learn/forex-school/559>.

الهوامش و الإحالات:

¹ Goldbarsht, Doron. "Adapting confiscation and anti-money laundering laws to the digital economy: exploring the Australian interplay between proceeds and technology." Journal of Money Laundering Control 27.3 (2023): 472-488.

² Les rapports IOCTA - Internet Organized Crime Threat Assessment - sont des publications annuelles au travers desquelles Europol met en lumière les menaces qu'elle a identifiées comme étant les plus préoccupantes.

³ المرجع السابق، على وجه التحديد، يُشير التقرير إلى أنه رغم أن البيبتكوين لا يزال العملة الافتراضية الأكثر استخدامًا – بما في ذلك على الشبكة المظلمة (Darkweb) – إلا أنه غالبًا ما يتم تحويله إلى عملة مونيرو (Monero) من خلال ما يُعرف بتقنية "التبديل بين السلاسل" (chain swapping). تُساهم هذه الظاهرة في اتجاه عام نحو تعقيد أساليب تبييض الأموال، والتي أصبحت تعتمد بشكل متزايد على خدمات الخلط (mixers)، والقفز بين السلاسل (chain hopping)، ومنصات التحويل وغيرها من الأدوات.

⁴ حظر قانون المالية لعام 2018 التعامل بالعملات الرقمية بشكل صريح، إذ نصت المادة 117 على ما يلي: "يُمنع شراء أو بيع أو استخدام أو حيازة العملات الافتراضية". ويعكس هذا الحظر مخاوف السلطات الجزائرية من المخاطر المحتملة لهذه العملات على استقرار الاقتصاد المحلي وأمن المنظومة المالية.

⁵ المادة 15 مكرر من قانون (قانون رقم 06-24 المؤرخ في 28 أبريل 2024) في حالة الإدانة لارتكاب جناية، تأمر المحكمة بمصادرة الأشياء التي استعملت أو كانت ستستعمل في تنفيذ الجريمة أو التي تحصلت منها، وكذلك الهبات أو المنافع الأخرى التي استعملت كمكافأة مرتكب الجريمة، مع مراعاة حقوق الغير حسن النية.

و يمكن في حالة الإدانة لارتكاب جنحة، الأمر بمصادرة الأشياء المذكورة في الفقرة السابقة، مالم ينص القانون على وجوبيتها.

وفي حالة الإدانة لارتكاب مخالفة يؤمر بمصادرة الأشياء المذكورة في الفقرة السابقة وجوبا إذا كان القانون ينص صراحة على هذه العقوبة،

ويجب أن تراعي في جميع الحالات حقوق الغير حسن النية.

⁶ تعريف مجموعة العمل المالي GAFI، 2014، أين يفرق التقرير بين العملة الافتراضية والعملة الورقية حيث تمثل هاتاه الأخيرة المجموع النقدي أو المال الأكثر استخدامًا على نطاق واسع في دول العالم و تتمثل في العملة المعدنية والورقية لبلد ما مثل الدينار ، الدولار، اليورو.. الخ، وهي العملة القانونية و المقبولة كوسيلة للتبادل في كل بلد.

<http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>.

⁷ مكتب الأمم المتحدة المعني بالمخدرات والجريمة، دليل مسرح الجريمة والأدلة المادية، الأمم المتحدة، نيويورك 2009، متاح على الموقع:

https://www.unodc.org/documents/scientific/ST_NAR_39_A.pdf

⁸ Guide sur la saisie des cryptomonnaies, Version 1.0, Bureau de programme du conseil de l'europe sur la cybercriminalite, 10 fevrier 2021.

⁹ Directive 2014/42/UE du Parlement européen et du Conseil du 3 avril 2014 concernant le gel et la confiscation des instruments et des produits du crime dans l'Union européenne. Et le Règlement (UE) 2018/1805 du Parlement européen et du Conseil du 14 novembre 2018 concernant la reconnaissance mutuelle des décisions de gel et des décisions de confiscation (Marty, Marie. « Actualités législatives de l'Union européenne ». Revue pénale luxembourgeoise, 2019/2 N° 2, 2019. p.35-40. CAIRN.INFO, droit.cairn.info/revue-revue-penale-luxembourgeoise-2019-2-page-35?lang=fr).

¹⁰ اللائحة (الاتحاد الأوروبي) 1113/2023 الصادرة عن البرلمان الأوروبي والمجلس بتاريخ 31 مايو 2023 بشأن المعلومات المصاحبة لتحويلات الأموال وبعض الأصول المشفرة وتعديل التوجيه (الاتحاد الأوروبي) 849/2015، الجريدة الرسمية للاتحاد الأوروبي L 150، 9.6.2023.

¹¹ المادة 6 من التوجيه الأوروبي 42/2014:

تتخذ الدول الأعضاء التدابير اللازمة لتمكين مصادرة العائدات أو الممتلكات التي تعادل قيمتها قيمة العائدات التي تم تحويلها، بشكل مباشر أو غير مباشر، إلى أطراف ثالثة من قبل مشتبه به أو شخص ملحق قضائياً، أو التي حصل عليها الغير من مشتبه به أو شخص ملحق قضائياً، على الأقل في الحالات التي كان يعلم فيها هؤلاء الأطراف من الغير أو كان ينبغي لهم أن يعلموا، استناداً إلى وقائع أو ظروف موضوعية، بأن الغرض من التحويل أو الاستحواذ كان التهرب من المصادرة، بما في ذلك عندما يتم التحويل أو الاستحواذ دون مقابل أو مقابل مبلغ يقل بشكل كبير عن القيمة السوقية.

¹² “Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team”, October 6, 2021, <https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team>, accessed August 1, 2022.

¹³ يتألف فريق NCET من مدعين عامين فيدراليين من وحدات متخصصة مختلفة، بما في ذلك قسم مكافحة تبييض الأموال واسترداد الأصول (MLARS)، ووحدة جرائم الكمبيوتر والملكية الفكرية (CCIPS)، إضافة إلى أعضاء منتدبين من أقسام الجنايات بمكاتب المدعين

العامين في مختلف الولايات الأمريكية. في عام 2022، أسست وزارة العدل الأمريكية وحدة متخصصة تُعرف بوحدة استغلال الأصول الافتراضية (VAXU) ضمن مكتب التحقيقات الفيدرالي (FBI)، وتهدف إلى تحليل معاملات البلوكشين ومصادرة الأصول الرقمية. وتعمل هذه الوحدة بالتعاون الوثيق مع فريق قسم العملات المشفرة الوطني التابع لوزارة العدل (NCET) في قضايا المصادرة.
اقرأ المزيد عن مصادرة العملات الرقمية المشفرة: <https://www.arabictrader.com/ar/learn/forex-school/559>

¹⁴ Dougherty, Thomas, and Nevenka Lastrić Đurić. "The United States approach to the investigation and prosecution of cybercrime and cryptocurrency crime." Hrvatski ljetopis za kaznene znanosti i praksu 29.2 (2022): 409-431.

¹⁵ Julien Cabrespines? Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES ?Frédéric Ruiz Genève ? Les cryptoactifs sont-ils une classe d'actifs à part entière ?, 08.07.2023 Haute École de Gestion de Genève (HEG-GE).

¹⁶ Jérémy Bourgaïs, La saisie pénale des actifs numériques : une saisie virtuelle ? Issu de Gazette du Palais - n°05 - page 10, Date de parution : 14/02/2023

¹⁷ Clément, S. et Lelieur, J. (2021) . La conformité anti-blanchiment face aux crypto-actifs. Revue de science criminelle et de droit pénal comparé, N° 1(1), 15-27.
<https://doi.org/10.3917/rsc.2101.0015>.

¹⁸ المرجع السابق، GUIDE SUR LA SAISIE DES CRYPTOMONNAIES

¹⁹ مثلًا قانون العقوبات الفرنسي وسع بموجب قانون 24 يناير 2023 (LOI n° 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur) إجراءات الجوز استثناء على المادة 154-706 من قانون الإجراءات الجنائية لتشمل الأصول المشفرة.

²⁰ المرجع السابق، GUIDE SUR LA SAISIE DES CRYPTOMONNAIES

²¹ المرجع السابق،

²² Galienni, Stéphane. et al. « Chapitre 13. Le cryptowallet ou le portefeuille Web3 ». La vague Web3 Maîtriser les nouveaux codes du marketing digital 3.0 Blockchain, NFT, DAO, métavers... Dunod, 2023. p.109-112. CAIRN.INFO, shs.cairn.info/la-vague-web3--9782100845835-page-109?lang=fr.

²³ المرجع السابق، GUIDE SUR LA SAISIE DES CRYPTOMONNAIES

²⁴ نفس المرجع.

²⁵ للتفصيل أنظر التوصيات السبعة من المؤتمر العالمي الخامس بشأن التمويل الجنائي والعملات المشفرة، منشورة بتاريخ 01-2022، الناشر: معهد بازل للحوكمة؛ الإنترنت؛ اليوروبول
Combating virtual assets based money laundering and crypto-enabled crime
التعاون الدولي.

1. تعزيز قنوات التعاون الدولي بين وكالات إنفاذ القانون والسلطات القضائية.

- تسريع تبادل المعلومات لملاحقة الجرائم المتعلقة بالأصول الافتراضية.
- الاستفادة من آليات التعاون العالمية مثل قنوات الإنترنت واليوروبول.
- 2. استرداد الأصول الافتراضية
- معاملة الأصول الافتراضية بنفس آليات الأصول التقليدية.
- استخدام خطط ما قبل المصادرة والتعاون بين القطاعين العام والخاص.
- معالجة القوانين التي تعيق استرداد الأصول لمكافحة الجرائم المالية.
- 3. التعاون بين القطاعين العام والخاص
- بناء الثقة بين سلطات إنفاذ القانون ومزودي خدمات الأصول الافتراضية (VASPs).
- تبادل المعلومات الفنية والتكتيكية بين الطرفين لتحديد العمليات غير القانونية.
- دعم التحقيقات المشتركة والاعتماد على أدوات تحليل المعاملات المتقدمة.
- 4. التنظيم الموحد والتطبيق الفعال
- وضع معايير تنظيمية دولية موحدة لمنع "التحكيم التنظيمي".
- فرض لوائح مكافحة تبييض الأموال وتمويل الإرهاب (AML/CFT) على جميع خدمات تقنية السجلات الموزعة (DLT).
- متابعة التطورات في مجالات NFT والميتافيرس والصناعات المرتبطة.
- 5. تطوير تقنيات وأساليب التحقيق
- تحديث تقنيات التحقيق لمواكبة تطور عمليات تبييض الأموال القائمة على الأصول الافتراضية.
- توظيف أدوات التحليل المستندة إلى تقنية البلوكتشين.
- التعاون مع القطاع الخاص لتطوير تقنيات تتبع المعاملات المعقدة.
- 6. بناء القدرات
- تدريب وحدات إنفاذ القانون المتخصصة في الجرائم المرتبطة بالأصول الافتراضية.
- تسريع تدريب الموظفين في الخطوط الأمامية للكشف عن المعاملات المشبوهة.
- تعزيز فهم السلطات القضائية لآليات العمل الجديدة في سوق الأصول الافتراضية.
- 7. النهج المتعدد التخصصات
- تشكيل فرق متخصصة تضم خبراء في المالية وتكنولوجيا المعلومات والجرائم السيبرانية.
- تعزيز التنسيق بين الوحدات المختلفة داخل الوكالات الأمنية.
- إنشاء وحدات خاصة لدعم التحقيقات المحلية والدولية بكفاءة أعلى.