Ashur Journal of Legal and political Sciences (AJLSP) is published by the Iraqi Association for Legal Sciences
ISSN: 3005-3269, Vol 3(No.2), pages: 663 -687 (2026)
https://ashurjournal.com/index.php/AJLPS/about

The Effectiveness of Digital Asset Freezing as a Legal Mechanism for Combating Terrorism Financing

Assistant Lecturer. Haneen Faiq Hussein

Al-Mustansiriyah University / College of Political Science , haneenfaeq1205@uomustansiriyah.edu.iq

ARTICLE INFORMATION

Received:30 Mar 2026
Accepted:26 Apr 2026
Published:1 Jun 2026

Keywords:

- Cryptocurrencies
- Freezing of Digital Assets
- Terrorist Financing
- International Law

ABSTRACT

This research examines the effectiveness of freezing digital assets as a legal mechanism for combating the financing of terrorism in light of the technological transformations brought about by cryptocurrencies. The study explores the conceptual framework of cryptocurrencies and their technical characteristics, as well as the ways in which they may be exploited for terrorist financing activities. It further reviews the international legal framework governing asset-freezing measures and analyzes the legal and technical challenges that hinder the practical implementation of such mechanisms in the digital environment.

The study concludes that the absence of a unified international legal framework, the weakness of international cooperation, and the technical complexities associated with tracing digital assets constitute the most significant obstacles to the effective enforcement of asset-freezing measures. Accordingly, the research emphasizes the need to develop flexible legislative and technological tools, alongside strengthening international cooperation mechanisms, in order to effectively address this transnational phenomenon.

مجلة آشور للعلوم القانونية والسياسية تصدر عن الجمعية العراقية للعلوم القانونية
المجلد الثالث (العدد الثاني)، الصفحات: 663 – 687، (2026) ISSN: 3005-3269
https://ashurjournal.com/index.php/AJLPS/about

فعالية تجميد الأصول الرقمية كآلية قانونية لمكافحة تمويل الإرهاب

م.م حنين فائق حسين

الجامعة المستنصرية/ كلية العلوم السياسية ، haneenfaeq1205@uomustansiriyah.edu.iq

معلومات المقالة

تاريخ الاستلام : ٣٠ اذار ٢٠٢٦
تاريخ القبول :٢٦ نيسان ٢٠٢٦
تاريخ النشر : ١ حزيران ٢٠٢٦

الملخص

يهدف هذا البحث إلى دراسة فعالية تجميد الأصول الرقمية كآلية قانونية لمكافحة تمويل الإرهاب، في ظل التحولات التقنية التي فرضتها الأصول الافتراضية، يتناول البحث الإطار المفاهيمي لهذه العملات، واستغلالها في تمويل الإرهاب، ثم يستعرض الإطار القانوني الدولي المنظم لتجميد الأصول، ويحلّل التحديات القانونية والتقنية التي تواجه التطبيق العملي لهذه الآلية، وتخلص الدراسة إلى أن غياب إطار قانوني موحّد، وضعف التعاون الدولي، والتعقيدات التقنية، تمثل أهم العقبات أمام فعالية التجميد، مما يستدعي تطوير أدوات تشريعية وتقنية مرنة، قادرة على ملاحقة هذه الظاهرة العابرة للحدود.

الكلمات المفتاحية:

- الأصول الافتراضية
- تجميد الأصول الرقمية
- تمويل الإرهاب
- القانون الدولي

المقدمة

يشهد العالم تحولات متسارعة في طبيعة المشهد المالي العالمي، مدفوعة بالثورة الرقمية التي أدت الى ظهور أنماط متجددة من الأصول ابرزها الأصول الافتراضية، هذه العملات بخصائصها الفريدة من اللامركزية والتشفير، أحدثت نقلة نوعية في طرق تبادل القيمة، لكنها في الوقت ذاته فتحت افافا جديدة لاستغلالها في أنشطة غير مشروعة، كغسل الأموال وتمويل الإرهاب، يمثل تجميد الأصول الية قانونية دولية أساسية لمكافحة هذه الجرائم، الا ان تطبيقها على الأصول الرقمية يواجه تحديات معقدة، تتطلب دراسة معمقة.

اولاً / أهمية البحث:

تنبع أهمية هذا البحث من معالجته لموضوع حيوي يتقاطع فيه القانون الدولي مع التطورات التقنية المتجددة، وهوما يسهم في فهم التحديات التي تواجه اليات مكافحة تمويل الإرهاب، يكتسب البحث أهمية خاصة في السياق العراقي، حيث يبرز الحاجة الملحة لتطوير اطر تشريعية وتنظيمية وطنية لمواكبة هذه الظاهرة، وسد الفجوات المعرفية والتشريعية القائمة، بما يعزز قدرة العراق على التصدي للتهديدات المالية المرتبطة بالإرهاب.

ثانياً / إشكالية البحث:

في ظل التوسع المتسارع لاستخدام الأصول الافتراضية في المعاملات المالية، وظهور أدلة متزايدة على استغلالها في تمويل الإرهاب، تبرز إشكالية قانونية وتقنية تتعلق بقصور القواعد التقليدية في القانون الدولي والداخلي عن ملاحقة هذه الأصول التي لا تخضع لسلطة مركزية، فبينما بنيت اليات التجميد التقليدي على وجود وسيط مالي مركزي ، فان الطبيعة اللامركزية للأصول الافتراضية تجعل هذه الاليات غير كافية، مما يخلق فراغا اجرائيا وقانونيا تستغله الجماعات الإرهابية، وعليه فإن الإشكالية الرئيسة التي يسعى هذا البحث إلى معالجتها تتمثل في: سؤال رئيس إلى أي مدى تُعد آلية تجميد الأصول الرقمية فعّالة قانونيًا وتقنيًا في مواجهة تمويل الإرهاب، وما هي التحديات التي تحول دون تطبيقها بفعالية على المستويين الوطني والدولي؟ وما يتفرع من ذلك من أسئلة تتعلق في ماهي الطبيعة القانونية والتقنية للعملات المشفرة التي تجعلها عرضة للاستغلال في تمويل الإرهاب؟ وما أبرز التحديات القانونية والتقنية التي تواجه فعالية تجميد الأصول الرقمية؟

ثالثاً/ فرضية البحث:

يفترض البحث ان الية تجميد الأصول الرقمية تواجه تحديات عدة منها ما هو قانوني واخر تقني يحد من فاعليتها على مكافحة تمويل الإرهاب على المستوى الوطني والدولي، وان هذه التحديات تتفاقم في السياقات الوطنية التي تفتقر الى اطر تشريعية وتنظيمية متكاملة ومتكاملة كالعراق مثلاٍ

رابعاً / منهجية البحث:

يعتمد هذا البحث على المنهج الوصفي التحليلي في عرض المفاهيم القانونية والتقنية المرتبطة بالعملات المشفّرة وتجميد الأصول الرقمية، مع الاستناد إلى المنهج المقارن في تحليل المواقف التشريعية بين عدد من الدول، مثل مصر،

الجزائر، العراق، والاتحاد الأوروبي. كما يُوظّف المنهج الاستقرائي لاستخلاص النتائج من الاتفاقيات الدولية، قرارات مجلس الأمن، وتوصيات مجموعة العمل المالي بهدف تقييم مدى فعالية الإطار القانوني الدولي في مواجهة تمويل الإرهاب الرقمي .

خامساً/ هيكلية البحث:

تم تقسيم البحث الى مبحثين اساسين تناول المبحث الأول: الإطار المفاهيمي للعملات ومخاطر توظيفها ارهابيا وقسم الى مطلبين المطلب الأول: التكيف القانوني للعملات الرقمية المطلب الثاني اليات الاستغلال الرقمي في تمويل الإرهاب، اما المبحث الثاني: النظام القانوني الدولي لتجميد الأصول الرقمية ومعوقات نفاذها وقسم الى مطلبين المطلب الأول: المرتكزات القانونية الدولية لتجميد الأصول الرقمية والمطلب الثاني : إشكاليات الامتثال والتعاون الدولي في تجميد الأصول الرقمية العابرة للحدود

المبحث الأول

الإطار المفاهيمي للعملات الرقمية ومخاطر توظيفها ارهابياً

شهد النظام المالي العالمي خلال العقدين الأخيرين تحوّلًا عميقة بفعل الثورة الرقمية، التي أفرزت انماطا جديدة من الأصول الرقمية، وفي مقدمتها العملات المشفّرة، وتجسد هذا التحول بصورة واضحة مع ظهور البيتكوين عام 2009 قدّمه مطوّر برمجي استخدم الاسم المستعار ساتوشي ناكاموتو، حيث طرحها باعتبارها نظام دفع الكتروني لامركزي، يتيح تحويل القيمة مباشرة بين المستخدمين دون وساطة مصرفية تقليدية، وتعتمد على تقنية سلسلة الكتل[1](Blockchain) ، وهي قاعدة بيانات موزّعة تُسجَّل فيها جميع معاملات البيتكوين بشكل متسلسل ومترابط، بما يضمن حفظ البيانات والتحقق منها بصورة شفافة وآمنة.

ويعود الأساس النظري لمفهوم العملات الرقمية إلى الباحث ديفيد تشوم، الذي قدّم عام 1982 تصورًا للنقود الإلكترونية بوصفها شكلاً رقميًا للنقد التقليدي، يتمثل في سلسلة مشفّرة من الأرقام قادرة على تحديد قيمة النقد وتسجيل معلومات المعاملات المرتبطة به، وهو ما شكّل حجر الأساس للتطورات اللاحقة في هذا المجال[2].

ورغم ما توفّره هذه العملات من مزايا تتصل بالسرعة، وانخفاض كلفة التحويل، وتجاوز القيود الجغرافية، فإن طبيعتها اللامركزية وخصائصها التقنية ـــ ولا سيما صعوبة تتبّع بعض المعاملات وإمكان إخفاء الهوية ـــ أثارت مخاوف الجهات الرقابية والأمنية، وقد نبهت تقارير صادرة عن مجموعة العمل المالي إلى تنامي مخاطر استغلال الأصول المشفّرة في أنشطة غير مشروعة، بما في ذلك غسل الأموال وتمويل الإرهاب، مستفيدة من التباين التشريعي بين الدول ومن غياب تنظيم قانوني موحّد في بعض الأنظمة[3].

وانطلاقًا من ذلك، يهدف هذا المبحث إلى تأصيل الإطار المفاهيمي للعملات المشفّرة من حيث تعريفها وخصائصها التقنية والقانونية، وبيان الفوارق بينها وبين المفاهيم المجاورة، ثم تحليل أوجه توظيفها في تمويل الإرهاب، تمهيدًا لبحث

الإشكاليات القانونية التي تثيرها، ولا سيما ما يتصل بمدى كفاية آليات التجميد في مواجهتها ضمن المنظومة القانونية المعاصر

المطلب الأول

التكيف القانوني والخصائص الفنية للأصول الافتراضية

لم يستقر الفقه ولا المؤسسات الدولية على تعريف موحّد للعملات المشفّرة، نظرًا لحداثة الظاهرة وتسارع تطورها، غير أن الاتجاه الغالب في الأدبيات الدولية يركّز على وصفها باعتبارها تمثيلًا رقميًا للقيمة يتم تداوله إلكترونيًا خارج إطار الإصدار النقدي الرسمي[4]، وقد تبنّى الاتحاد الأوروبي هذا التوجه في التوجيه رقم 2018/834 المعدِّل للتوجيه (EU)849/2015، المتعلق بمكافحة غسل الأموال وتمويل الإرهاب[5]، حيث عرّف العملات الافتراضية في المادة(1805) بأنها تمثيل رقمي للقيمة لا يصدر أو يُضمن من مصرف مركزي أو هيئة عامة، ولا يرتبط بالضرورة بعملة قانونية، ولا يتمتع بالمركز القانوني للنقد، لكنه يُقبل كوسيلة للتبادل ويمكن نقله وتخزينه وتداوله إلكترونيًا[6].

وفي السياق ذاته، عرّفت مجموعة العمل المالي الدولية العملات الافتراضية بأنها تمثيل رقمي للقيمة يمكن تداوله إلكترونيًا، ويؤدي وظيفة وسيلة للتبادل أو وحدة للحساب أو مخزن للقيمة وفقًا لاتفاق المستخدمين، دون أن يكون له مركز قانوني لعدم صدوره عن سلطة مركزية[7]، كما عرّف صندوق النقد الدولي العملات الافتراضية بأنها تمثيلات رقمية للقيمة تصدر عن مطوّرين من القطاع الخاص، وتُدرج ضمن وحدات حساب خاصة بهم، في حين ميّز البنك الدولي بينها وبين النقود الإلكترونية المرتبطة بالعملات القانونية، معتبرًا أنها تمثيلات رقمية لقيمة محدودة ضمن وحدة حساب مستقلة، ولا تُعد وسيلة دفع رقمية قانونية[8].

أما من الناحية التشريعية، فقد تباينت التعريفات تبعًا لاختلاف موقف مشرّع كل دولة من مشروعية التعامل بهذه العملات، اذ تناول المشرّع المصري العملات المشفّرة في قانون البنك المركزي والجهاز المصرفي رقم (194) لسنة 2020، اذ نصّت المادة (1) على "أنها عملات مخزّنة إلكترونيًا غير مقوّمة بأي من العملات الصادرة عن سلطات الإصدار النقدي الرسمية، ويتم تداولها عبر شبكة الإنترنت" ، يركز هذا التعريف على الطبيعة الرقمية وغياب الربط بالنقود الرسمية مع الاعتراف بالقدرة على التدوال.

أما في الولايات المتحدة الأمريكية، فقد اعتمدت لجنة القانون الموحد عام 2017 قانون التنظيم الموحد للأعمال التجارية للعملات الافتراضية، وعرّفتها بأنها تمثيل رقمي للقيمة يُستخدم كوسيط للتبادل أو وحدة للحساب أو مخزن للقيمة، دون أن يتمتع بدعامة قانونية كالنقود.

وفي الجزائر، وصف المشرّع العملات الرقمية بأنها وسائل يُجري بها مستخدمو الإنترنت معاملاتهم عبر الشبكة، وتفتقر إلى الدعامة المادية للنقود التقليدية. في المقابل، لم يتطرّق المشرّع العراقي حتى الآن إلى تعريف العملات الرقمية في أي من قوانينه، بما في ذلك قانون مكافحة غسل الأموال وتمويل الإرهاب رقم (39) لسنة 2015، وهو ما يُفضي إلى

فراغ تشريعي واضح، يتضح مما سبق أن التعريفات الدولية ركّزت على الخصائص التقنية (التشفير، اللامركزية، التخزين الرقمي)، بينما عالجت بعض التشريعات العربية المسألة من زاوية المشروعية ومدى إباحة أو حظر التعامل بها، ويُبرز غياب تعريف تشريعي في العراق الحاجة الماسة إلى تدخل المشرّع لملء هذا الفراغ القانوني، خاصة مع تصاعد مخاطر استخدامها في تمويل الإرهاب.

لم يقدم المشرّع العُماني تعريف العملات الافتراضية تعريفًا صريحًا، وإنما أشار في اللائحة التنفيذية لقانون نظم المدفوعات الوطنية لعام 2019، ولا سيما في المادة (69)، إلى أنها لا تُعد نقودًا إلكترونية، وتكتسب هذه الإشارة أهمية خاصة؛ إذ يقع عدد من الباحثين في خلطٍ منهجي بين مفهوم العملات الرقمية ومفهوم النقود الإلكترونية، رغم الاختلاف الجوهري بينهما من حيث الطبيعة القانونية وآلية الإصدار والرقابة.

وانطلاقًا من الخصائص الأساسية للأصول الافتراضية، والمتمثلة في طابعها الافتراضي، ووجودها في صورة رقمية، وإمكانية تداولها عبر شبكة الإنترنت، يمكن اقتراح تعريف موجز لها بأنها: اصول افتراضية لا وجود ماديًا لها، تعتمد تقنيات التشفير وسلاسل الكتل (Blockchain) في تأمينها، ويتم التعامل بها وتداولها إلكترونيًا عبر شبكة الإنترنت، فهي بذلك تفتقر إلى أي تجسيد مادي، فلا تُصدر في صورة أوراق نقدية أو عملات معدنية، وإنما تقوم ماهيتها على التشفير كنظام أمني لحماية المعاملات، وعلى تقنية سلاسل الكتل بوصفها البنية التقنية التي تُسجَّل من خلالها العمليات وتُتحقق. كما يُعد التداول عبر شبكة الإنترنت عنصرًا ملازمًا لطبيعتها، إذ لا يمكن تصور وجودها خارج البيئة الرقمية.

ويترتب على هذا التعريف استبعاد النقود التقليدية ذات الوجود المادي، كالأوراق النقدية والعملات المعدنية الصادرة عن السلطات المختصة، كما يُستبعد كذلك ما قد يوجد من أنظمة دفع تعتمد وسائل أمان إلكترونية أخرى دون أن تقوم على التشفير وسلاسل الكتل، فضلًا عن استبعاد العملات التي تعمل ضمن شبكات مغلقة أو أنظمة داخلية غير متاحة عبر شبكة الإنترنت العامة وتأسيسًا على ما تقدّم، يتبيّن أن العملات الرقمية تمثل مخزونًا ذا قيمة مالية قابلة للتداول والتصرف، الأمر الذي يثير مسألة تكييفها القانوني. ومن زاوية النظر الموضوعية، فإنها تندرج ضمن مفهوم الحق المالي[9]

وبتطبيق ذلك على الأصول الافتراضية، فإنها – من حيث طبيعتها – تمثل قيمة قابلة للتملك والتداول، ولا تخرج بطبيعتها عن التعامل، ومن ثم يمكن النظر إليها بوصفها مالًا بالمعنى القانوني. غير أن الإشكال لا يكمن في ماهيتها الاقتصادية، بل في غياب النص التشريعي الصريح الذي يحدد وصفها القانوني ويضفي عليها المشروعية، وهو ما يفتح المجال لاجتهادات فقهية وقضائية متباينة.

ومن ثمّ، فإن مسألة الطبيعة القانونية للأصول الافتراضية تظل محل بحث وتحليل، خصوصًا في الأنظمة التي لم تُنظّمها تشريعيًا، بخلاف التشريعات التي حظرتها صراحةً، حيث تنتفي عنها صفة المال قانونًا لارتباط هذه الصفة بشرط المشروعية، لذلك من الضروري التميز بين الأصول الافتراضية والعملات الرقمية للبنوك المركزية فالأخيرة هي عملات رقمية تصدرها وتديرها البنوك المركزية، وتتمتع بوضع قانوني كعملة وطنية، وتخضع لرقابة واشراف كاملين من الدولة، بينما الأصول الافتراضية، كما ذكرنا لا تصدر من سلطة مركزية ولا تتمتع بوضع قانوني كعملة نقدية، مما يجعلها مختلفة

تماما من حيث الطبيعة القانونية والرقابية، هذا التميز جوهري في سياق مكافحة تمويل الإرهاب، حيث ان cbdcs توفر شفافية وتتبعا كاملا، على عكس الأصول الافتراضية التي تثير تحديات اكبر في هذا الصدد.

المطلب الثاني

اليات توظيف الأصول الافتراضية في تمويل الإرهاب

أصبحت الأصول الافتراضية وسيلة جذابة للجماعات الإرهابية، إذ توفر لها أدوات للتحايل على النظم المالية التقليدية، وتُتيح تنفيذ عمليات تمويلية بسرية وسرعة، وقد أثبتت تقارير دولية، مثل تلك الصادرة عن مجموعة العمل المالي (FATF)ومكتب الأمم المتحدة المعني بالمخدرات والجريمة(UNODC)[10] ، أن الجماعات الإرهابية باتت تستغل هذه العملات في تجاوز الرقابة المصرفية، مستفيدة من خصائصها التقنية الفريدة، تتميز العملات المشفّرة بجملة من الخصائص التي تجعلها جذابة من جهة، ومثيرة للقلق من جهة أخرى، خاصة في سياق استخدامها غير المشروع، ويمكن اجمال هذه الخصائص في الاتي:

الفرع الأول

الخصائص الفنية الجاذبة للأصول الافتراضية للجماعات الارهابية

1- اللامركزية: تتميز العملات الرقمية بكونها غير صادره من سلطة مركزية فلا تخضع لإشراف أو تحتاج الى وسيط لإتمام معاملاتها لاعتمادها على خاصية البلوكتشين، مما يصعّب الرقابة والتنظيم، اذ تدار غبر شبكة موزعة مما يقلل قدرة الحكومات على التحكم بها[11].

2- إخفاء الهوية: تتيح للمستخدمين إخفاء بياناتهم بدرجات متفاوتة، ما يعقّد عمليات التتبع، وهو ما يعقد عملية التتبع المالي[12]، الا ان ذلك نسبيا نوعا ما اذ يمكن رغم إخفاء هوية المستخدمين، من خلال عنوان ابجدي رقمي مرتبط بمحفظة الخاصة بهم، مما يسمح نظريًا بتتبعها إذا توفرت الأدوات المناسبة.

3- التقلب العالي: تتسم أسعارها بتغيرات حادة وسريعة، ما يجعلها عرضة للمضاربات والمخاطر.

4- العالمية: تُستخدم عبر الحدود دون قيود مصرفية أو جمركية، ما يعزز طابعها العابر للحدود، ويمكن تحويلها بسرعة مكان في العالم وباي ثمن، وهذا مايجهلها مميزة لدى الجهات الإرهابية، اذا يمكن تنقلها دون الحاجة لوسطاء أو رسوم مصرفية تقليدية.

5- التشفير المتقدم: تعتمد على تقنيات أمنية يصعب اختراقها، مما يعزز من صعوبة تعقب المعاملات، وتستند إلى أنظمة تشفير وسلاسل كتل مقاومة للتلاعب

6- الندرة Scarcity: معظم العملات، مثل البيتكوين، محدودة الإصدار (21 مليون وحدة)، ما يمنحها طابعًا استثماريًا شبيهًا بالذهب [13]، وتكون قابلية للتجزئة اذ يمكن تقسيم الوحدة الواحدة (بيتكوين) إلى 100 مليون جزء (ساتوشي)، مما يزيد من مرونتها كوسيلة للدفع[14].

الفرع الثاني

صور الاستخدام الإرهابي للأصول الافتراضية

وتتعدد آليات الاستخدام هذه العملات من خلال

1- التبرعات الرقمية حيث تعتمد بعض الجماعات على نشر عناوين محافظ مشفّرة عبر مواقع إلكترونية أو منصات تواصل، لتلقي الدعم المالي من أنصارها دون إمكانية تعقب مصدر الأموال بدقة، وقد وثّقت دراسة بعنوان Terrorist Financing in the Digital Ageحالات استخدمت فيها جماعات متطرفة التمويل الجماعي المشفّر (Crypto Crowdfunding)لجمع التبرعات بسرية تامة، مستغلةً ضعف أنظمة "اعرف عميلك(KYC) " في بعض المنصات[15].

2- والشراء عبر الإنترنت المظلم(Dark Web) اذ تُستخدم العملات الرقمية كوسيلة دفع رئيسية لشراء الأسلحة أو المواد الأولية لصناعة المتفجرات من السوق السوداء الإلكترونية[16]، وتُظهر دراسة Cryptocurrency and Their Use in Money Laundering and Terrorism Financingأن منصات التداول غير الرسمية تُسهّل هذه العمليات، خاصة تلك التي لا تتطلب تسجيلًا أو تحققًا من الهوي .

3- سهولة نقل الأموال عبر الحدود على خلاف النظام المصرفي الذي يخضع لرقابة البنوك المركزية، يمكن للجماعات الإرهابية نقل مبالغ مالية كبيرة عبر الأصول الافتراضية في ثوانٍ معدودة[17]، دون أي إشراف مصرفي، وقد أشار تقرير صادر عن مؤسسة RAND إلى أن هذه الخاصية تُعد من أخطر أدوات التهرب المالي، خاصة في مناطق النزاع التي تفتقر إلى بنية مصرفية رسمية[18].

4- وتُمكّن تقنيات "خلط المعاملات (Mixers) أو استخدام "العملات المستقرة" (Stablecoins) من إخفاء مصدر الأموال المشبوهة، ثم إعادة دمجها في الاقتصاد المشروع، وتُظهر دراسة Combating Terrorist Financing in Cryptocurrency Platformsأن أدوات الذكاء الاصطناعي بدأت تُستخدم لرصد هذه الأنماط، لكنها لا تزال تواجه تحديات تتعلق بتحيز البيانات وصعوبة الوصول إلى معلومات دقيقة من المنصات اللامركزية.

5- استخدام العملات المعززة للخصوصية: مثل Monero وZcash، التي تُصمم خصيصًا لإخفاء هوية المستخدمين، وتُستخدم بشكل متزايد في العمليات الإرهابية بسبب صعوبة تتبعها حتى عبر البلوكشين[19]، وقد صنّفتها مجموعة العمل المالي ضمن العملات عالية الخطورة من حيث قابلية الاستغلال في الجرائم العابرة للحدود، مما يجعل تتبعها شبه مستحيل، وحتى مع محاولات الاستعانة بالذكاء الاصطناعي لرصد الأنماط المشبوهة[20]، تبقى النتائج محدودة في ظل غياب بيانات دقيقة من المنصات اللامركزية، ففي عام 2024، بلغ إجمالي الأصول المجمدة المرتبطة بالإرهاب 289 مليون دولار عالمياً، ارتفاعاً من 134 مليون دولار في 2022، ومن هذه الأموال، استحوذت الجماعات المتطرفة في سوريا والعراق على 61 مليون دولار عبر عملات Monerو Zcashالتي يصعب تتبعها[21]

وفي السياق العربي، أظهر تقرير البنك المركزي الإماراتي (2023) أن 82% من محاولات التحويلات المشبوهة تم رصدها عبر الذكاء الاصطناعي، بينما لا تزيد نسبة التعاون العراقي-العربي في تبادل المعلومات عن 23%وفقاً

لتقييمFATF،[22] مما يعني أن 77% من المعاملات تمر دون تبادل بيانات وبالتالي، فإن هذه الأرقام تُبرز الفجوة بين القرارات الدولية والتطبيق الوطني، وضرورة تطوير آليات جديدة[23].

يمثّل استخدام الأصول الافتراضية في تمويل الإرهاب تحولًا نوعيًا في أنماط التمويل غير المشروع. فبينما نجحت التشريعات التقليدية في تضييق الخناق على التمويل عبر البنوك، وجدت الجماعات الإرهابية في الأصول الرقمية بديلًا ماليا يوفّر السرية والسرعة والعالمية. وتؤكد الدراسات أن هذه الجماعات لم تعد تعتمد على الأصول الافتراضية كوسيلة ثانوية، بل كأداة أساسية في بعض أنشطتها، وهو ما يجعل من تجميد الأصول الرقمية خيارًا قانونيًا وأمنيًا لا غنى عنه في إطار مكافحة الإرهاب، وهو ما سنعالجه في المبحث الثاني

المبحث الثاني

النظام القانوني الدولي لتجميد الأصول الرقمية ومعوقات نفاذها

يُعدّ تجميد الأصول من أبرز التدابير القانونية التي اعتمدها المجتمع الدولي لتعطيل قدرات الجماعات الإرهابية، وذلك من خلال منعها من الوصول إلى مواردها المالية أو إعادة تدويرها، وإذا كان هذا الإجراء قد ارتبط في بداياته بالأموال التقليدية المودعة في البنوك، فإن التطور التكنولوجي وانتشار العملات المشفّرة فرض إعادة النظر في نطاق هذا المفهوم ليشمل الأصول الرقمية، نظرًا لاستخدامها المتزايد في تمويل الأنشطة غير المشروعة[24]، ومن هنا، يتناول هذا المبحث المرتكزات القانونية الدولية لتجميد الأصول، ثم يناقش التحديات التي تحول دون التطبيق الفعّال لهذا الإجراء على العملات الرقمية.

المطلب الأول

المرتكزات القانونية الدولية لتجميد الأصول الرقمية

لقد ساهمت الاتفاقيات الدولية في إرساء الأساس القانوني لتجميد الأصول، حيث تعد اتفاقية قمع تمويل الإرهاب لعام 1999 نقطة انطلاق رئيسية، اذ نصت على ضرورة تجريم التمويل غير المشروع، والزام الدول باتخاذ التدابير الضرورية لتجميد الأموال المستخدمة أو المخصصة للعمليات الإرهابية، وعلى الرغم من ان النص لم يشر صراحة الى العملات المشفّرة بشكل صريح، إلا أن صياغتها الواسعة تسمح بإدراجها ضمن مفهوم "الأموال" أو "الأصول"، بل اعتبرت ان مجرد محاولة التمويل او المساهمة فيه من قبيل الأفعال المجرمة وفق المادة الأولى والثانية من الاتفاقية[25].

وتكمل ذلك اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لعام 2000 (اتفاقية باليرمو) لتُعزز هذا الاتجاه، حيث نصّت على تمكين السلطات من تتبع وتجميد عائدات الجريمة المنظمة، وهو ما ينطبق على الأصول الرقمية التي تُستخدم بشكل متزايد في غسل الأموال وتمويل الإرهاب، وفي السياق ذاته، أقرّت اتفاقية مكافحة الفساد لعام 2003 آليات لاسترداد الأموال المهرّبة وتجميدها، بما في ذلك تلك المتحصلة من معاملات مالية غير تقليدية، مما يفتح الباب أمام إدخال العملات الرقمية في نطاقها[26].

وقد تعزز الاهتمام الدولي بمكافحة تمويل الإرهاب بشكل اكبر بعد عام 2001 ،حيث تبنى مجلس الأمن مجموعة من القرارات، التي عززت الاطار القانوني في هذا المجال ومن ابرزها، القرار 1267 (1999) الدول بفرض عقوبات مالية على الأفراد والكيانات المرتبطة بالقاعدة وطالبان، ثم وسّع القرار 1373 (2001) نطاق الالتزام ليشمل أي شخص أو كيان يقدم دعمًا ماديًا للإرهاب[27]، وتجريم قيام الأفراد أو الكيانات بجمع الأموال أو توفيرها بصورة مباشرة أو غير مباشرة لصالح الأنشطة الإرهابية، كما شملت هذه التدابير منع تقديم أي شكل من أشكال الدعم للجماعات الإرهابية، بما في ذلك تجنيد الأفراد لصالحها أو تزويدها بالسلاح، إضافة إلى منع توفير الملاذ الآمن للأشخاص أو الكيانات المتورطة في تمويل الإرهاب أو دعمه، كما أكد1617 قرار عام 2005 أن تمويل الإرهاب لا يقتصر على تقديم الأموال فحسب، بل يشمل أي شكل من أشكال التسهيلات أو الدعم المقدم للجماعات أو الأفراد الإرهابيين. ولهذا طالب القرار الدول باتخاذ مجموعة من التدابير، من أبرزها منع دخول الإرهابيين إلى أراضيها أو مرورهم عبرها، وحظر تزويدهم بالسلاح أو المعدات العسكرية أو شبه العسكرية وقطع الغيار، وكذلك منع تقديم المشورة التقنية أو التدريب المتعلق بالأنشطة العسكرية لهم، أما القرار 2462 (2019) فقد عكس نقلة نوعية، إذ أشار صراحة إلى أهمية مواجهة التمويل عبر القنوات الرقمية، مؤكدًا على تعزيز التعاون الدولي في هذا المجال. [28]

ولم يقتصر الامر على الاتفاقيات والقرارات الأممية، بل ظهرت معايير تقنية ومالية دولية كان لها اثر بالغ في توسيع نطاق التجميد ليشمل الأصول الرقمية وفي مقدمتها توصيات مجموعة العمل المالي اذ مثّلت المرجعية الفنية الأبرز، فقد نصّت التوصية السادسة على التجميد الفوري للأصول المرتبطة بالإرهاب، بينما عدّلت التوصية الخامسة عشرة عام 2019 لتشمل الأصول الافتراضية ومقدمي خدماتها، وألزمتهم بتطبيق معايير "اعرف عميلك" ومكافحة غسل الأموال وأظهر تقرير FATF لعام 2021 أن 60% من الدول لم تُدرج الأصول الرقمية بعد في أنظمتها الوطنية، مما يُبرز وجود فجوة تنظيمية عالمية

ويستفاد من ذلك أن مفهوم تمويل الإرهاب في القانون الدولي أصبح واسع النطاق، إذ لا يقتصر على الدعم المالي المباشر، بل يمتد ليشمل الدعم اللوجستي، وتوفير الملاذ الآمن، وتسهيل التنقل، وتقديم التدريب أو المساعدة الفنية، أو المشاركة في الأنشطة الإرهابية وتعد هذه الأفعال جرائم مستقلة مرتبطة بالإرهاب تستوجب فرض الجزاءات والتدابير القانونية الرادعة.

المطلب الثاني

إشكاليات الامتثال والتعاون الدولي في تجميد الأصول الرقمية العابرة للحدود

ان مسالة تجميد الأصول الرقمية المرتبطة بالإرهاب تمثل تحديًا معقدا في النظام المالي الدولي المعاصر، وذلك نتيجة التداخل بين الإشكالات القانونية والتنظيمية من جهة، والتحديات التقنية المرتبطة بطبيعة التكنولوجيا المستخدمة في العملات المشفّرة من جهة أخرى، فبينما استطاعت التشريعات الدولية خلال العقود الماضية تطوير منظومة فعّالة نسبيًا لتعقّب الأموال التقليدية وتجميدها ضمن النظام المصرفي العالمي، فإن ظهور الأصول الافتراضية، وفي مقدمتها العملات المشفّرة، أوجد

بيئة مالية جديدة يصعب إخضاعها للأدوات القانونية التقليدية، ويرجع ذلك إلى الخصائص التقنية التي تميز هذه الأصول، مثل اللامركزية، وإمكانية إجراء المعاملات دون وسطاء ماليين، وسهولة نقل الأموال عبر الحدود في وقت قصير.

وقد أكدت تقارير دولية عديدة أن هذه الخصائص تجعل الأصول الرقمية بيئة جذابة لبعض الجماعات الإجرامية والإرهابية، ففي تقرير مشترك صادر عن INTERPOL و United Nations Interregional Crime and Justice Research Institute (UNICRI)عام 2023، أُشير إلى أن العملات المشفّرة تمثل تحديًا متزايدًا لسلطات إنفاذ القانون في مجال تتبع الأموال غير المشروعة وتجميدها، خصوصًا في ظل الطبيعة العابرة للحدود لهذه الأصول وصعوبة إخضاعها لولاية قضائية واحدة.

وانطلاقًا من ذلك، فإن تحليل إشكاليات المرتبطة بتجميد الأصول الرقمية يقتضي التمييز بين نوعين رئيسيين من العقبات: منها العقبات القانونية والتنظيمية، والعقبات التقنية والأمنية

الفرع الأول

العقبات القانونية والتنظيمية

يمثل تنظيم الأصول الرقمية احد ابرز التحديات القانونية على المستويين الوطني والدولي، نظراً للتطور السريع للعملات المشفرة وظهور اطر مالية جديدة لم تكن التشريعات التقليدية معدة لتعامل معها، ويظهر هذا بوضوح في تباين المواقف التشريعية بين الدول، في كيفية التعامل مع العملات المشفرة بشكل كامل؛ وأخرى تسمح بها ضمن اطر تنظيمية محددة، بينما لاتزال بعض الدول تفتقر الى تنظيم قانوني واضح لها، فعلى المستوى العربي، تبنت بعض الدول مواقف تشريعية متشددة تجاه هذه العملات، فمصر مثلًا أدرجت في قانون البنك المركزي رقم 194 لعام 2020 نصًا يُجرّم إصدار أو تداول العملات المشفّرة دون ترخيص، فارضًا عقوبات جنائية على المخالفين[29]، أما الجزائر، فقد ذهبت الى ابعد من ذلك، حيث نص قانون المالية لعام2018، على حظر التعامل بالعملات واعتبارها وسيلة دفع غير قانونية وحظرت التعامل بها بشكل مطلق بموجب الامر الذي يجعل من تدوالها واستخدامها مخالفا للقانون.

وهذا بدوره يؤدي الى إشكالية تنازع القوانين والولاية القضائية الرقمية، اذ تتجاوز الأصول الرقمية الحدود الجغرافية التقليدية ، مما يثير تساؤلات معقدة حول القانون الواجب التطبيق والمحكمة المختصه التي يصدر من خلالها أوامر التجميد، ففي ظل غياب المعايير الدولية المتعلقة بهكذا موضوع والموحدة، تجد السلطات الإقليمية والوطنية صعوبة في تنفيذ قرارتها ضد منصات تعمل في العملات الرقمية، تبني قوانين مرنة او ترفض التعاون القضائي الدولي، هذا التخبط والتشتت من شانه ان يؤدي الى "تحكيم تنظيمي" تستغله الجماعات الإرهابية لنقل أصولها الى ولايات قضائية اقل صارمة، مما يفرغ اليه تجميد من محتواها الفعلي.

وفي المقابل، لم يتطرق المشرع العراقي كما بينا سابقا الى تنظيم العملات الرقمية بشكل صريح،مما يترك فراغا تشريعيا يعيق جهود مكافحة تمويل الإرهاب وغسل الأموال، هذا الغياب التشريعي يؤدي الى صعوبة في تحديد الطبيعة القانونية

لهذه الأصول وبالتالي صعوبة تطبيق اليات التجميد والمصادرة عليها، كما ان غياب تعريف موحد على المستوى الدولي يتعلق بالعملات يزيد من تعقيد المشكلة، اذ تختلف الدول في تصنيفها، مما يوثر ذلك على التعاون وتبادل المعلومات.

وعلى المستوى الدولي ورغم وجود قرارات ملزمة صادرة عن مجلس الامن فضلا عن توصيات مجموعة العمل المالي والتي تم التطرق لها مسبقا، فان تطبيق هذه الأدوات على الأصول الرقمية يظل محددا بسبب غياب اطار دولي موحد لتنظيمها مما يؤدي لاستغلال بعض الجماعات الاجرامية والارهابية للثغرات القانونية بين الانظمة التشريعية المختلفة، حيث يمكن نقل الأصول الرقمية بسرعة تامة بين ولايات القضائية لا تتبنى نفس المعايير التنظيمية، مما يصعب تنفيذ اوامر التجميد ويضعف من ملاحقتها قانونيا.

وفي إطار التطورات التشريعية الحديثة لتنظيم الأصول الرقمية، شهد الاتحاد الأوروبي تحولًا نوعيًا من خلال إقرار Markets in Crypto-Assets Regulationفي مايو 2023[30]، والتي دخلت حيّز التنفيذ الكامل في ديسمبر 2024. وتعد هذه اللائحة أول إطار تشريعي شامل لتنظيم الأصول المشفّرة على المستوى الإقليمي والدولي، إذ تهدف إلى وضع قواعد موحدة لتنظيم سوق الأصول الرقمية وتعزيز الشفافية والاستقرار المالي داخل الاتحاد الأوروبي، بما يشمل مكافحة غسل الأموال وتمويل الإرهاب.

وتُلزم اللائحة مقدمي خدمات الأصول المشفّرة(CASPs) بالامتثال لمتطلبات صارمة من بينها إجراءات العناية الواجبة بالعملاء وتعزيز متطلبات اعرف عميلك(KYC) ، إضافة إلى الالتزام بالإبلاغ عن المعاملات المشبوهة للسلطات المختصة. كما منحت اللائحة السلطات التنظيمية صلاحيات لتجميد الأصول الرقمية المرتبطة بالأنشطة غير المشروعة، مع إنشاء آليات تعاون بين الهيئات الوطنية لتسهيل تنفيذ أوامر التجميد عبر الحدود. ويشمل التنظيم تصنيفًا دقيقًا للأصول الافتراضية، مميّزًا بين الأصول المستقرة ذات القيمة المرجعية (Asset-Referenced Tokens) والعملات الإلكترونية مما يسهل تحديد نطاق التجميد القانوني وتطبيقه بدقة.

ويُعدّ هذا الإطار التشريعي نموذجًا نوعيًا يُظهر إمكانية تحويل الفجوات القانونية المتعلقة بالأصول الرقمية إلى أطر تنظيمية فعّالة، وهو ما يتيح للدول العربية، بما في ذلك العراق، الاستفادة من هذا النهج لتطوير تشريعات وطنية واضحة تُنظم العملات المشفّرة ومقدمي الخدمات المرتبطة بها، وتفرض آليات فعّالة لتجميد الأصول الرقمية المرتبطة بالأنشطة الإجرامية والإرهابية. ويمكن ربط ذلك بتوصيات FATF التي أكدت على ضرورة وضع أطر قانونية وتنظيمية واضحة للأصول الافتراضية ومقدمي خدماتها، لضمان القدرة على تنفيذ أوامر التجميد ومكافحة تمويل الإرهاب بفعالية

كما أن التشريعات المالية التقليدية محدودة، لم تُصمم أساسًا للتعامل مع الأصول الرقمية، إذ ركزت على الأموال النقدية والمعاملات المصرفية، الأمر الذي يخلق صعوبات قانونية في تطبيق قواعد التجميد على محافظ رقمية لا ترتبط بهويات قانونية واضحة أو تعمل عبر منصات غير خاضعة لأي سلطة تنظيمية.

لذلك نرى انه لابد من ان يكون هناك تعاون بين السلطات القضائية ومزودي خدمات الأصول الافتراضية، لما يوفره ذلك من ضرورة حتمية في رفع كفاءة تتبع الأصول الرقمية وتجميدها، لا سيما في ظل الطبيعة اللامركزية التي تعقد

الوصول الى المعلومات، كما ان غياب اطر قانونية واضحة ومنظمة يحد من فعالية هذا التعاون ويضعف الاستجابة للمعاملات المشبوهة، وعليه فان تبني معايير دولية وتطوير اليات تبادل المعلومات يشكل ركيزة أساسية لتعزيز الامن المالي ومكافحة الجرائم المرتبطة بالأصول الرقمية.

الفرع الثاني

العقبات التقنية والأمنية

لا تقل التحديات التقنية خطورة عن التحديات القانونية، بل ربما تمثل العائق الأكبر أمام تجميد الأصول الرقمية، فالطبيعة اللامركزية للعملات المشفّرة تعني غياب جهة مركزية يمكن مخاطبتها أو إلزامها بتنفيذ الأوامر القضائية، وتزداد هذه الصعوبة مع ظهور المنصات الالكترونية (DEXs)، والبروتوكولات غير الحاضنة التي تعمل من خلال عقود ذكية ذاتية التنفيذ دون وسيط مالي يمكن الزامة قانونيا بالتجميد.

وعلى عكس البنوك التقليدية، فإن المحافظ الرقمية تُدار من قبل المستخدم نفسه، وغالبًا ما تكون محمية بمفاتيح خاصة يصعب الوصول إليها، وحتى في حال صدور قرار قضائي بالتجميد، فإن تنفيذه يظل مرهونًا بتعاون منصات التداول المركزية،[31] اما في حالة المنصات اللامركزية فان التحدي يصبح وجوديا لألية التجميد التقليدية، ومع ذلك برز حلول تقنية استباقية تتمثل في استخدام" العقود الذكية كأداة للتجميد التلقائي" اذ يمكن لمصدري بعض الأصول الرقمية برمجة وظائف داخل العقد الذكي تسمح بأدراج عناوين معينة في "القائمة السوداء" مما يمنع تلك العناوين من نقل او استقبال الأصول فور صدور إشارات امنية او قضائية، هذا التحول نحو التجميد البرمجي يمثل اهم مسارات تعزيز الفعالية في مواجهه تمويل الإرهاب الرقمي لعام 2026.

أن خاصية إخفاء الهوية تُعد من أبرز السمات التي تُستغل في الأنشطة غير المشروعة، فالمعاملات على شبكات مثل Bitcoinقد تكون مرئية على سلسلة الكتل(Blockchain) ، لكنها لا تكشف عن هوية المستخدمين الحقيقية، وتزداد المشكلة تعقيدًا مع استخدام أدوات مثل Mixers التي تُعيد خلط المعاملات لإخفاء مصادرها، أو العملات المعززة للخصوصية مثل Monero وZcash، التي صُممت خصيصًا لجعل التتبع شبه مستحيل حتى على أكثر الأنظمة تطورًا[32].

وتُضاف إلى ذلك مشكلة السرعة العابرة للحدود، حيث يمكن تحويل مبالغ ضخمة خلال ثوانٍ معدودة إلى أي مكان في العالم، دون المرور عبر البنوك أو الجهات الرقابية، وهذا ما يجعل الاستجابة لقرارات التجميد بطيئة وغير فعّالة، خاصة في الحالات التي تتطلب تدخلًا فوريًا لمنع التصرف في الأصول[33].

ولا يمكن إغفال التحديات التي تواجه الدول الاخرى، مثل العراق، في بناء القدرات التقنية اللازمة لمراقبة المعاملات الرقمية، ففي حين بدأت بعض الدول المتقدمة باستخدام تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة لرصد الأنماط المشبوهة، لا تزال معظم الدول تفتقر إلى الكوادر المتخصصة والتجهيزات التكنولوجية القادرة على تنفيذ مثل هذه المهام،

كما أن المنصات نفسها تُعاني من ثغرات أمنية، إذ تتعرض بعض بورصات العملات المشفّرة لهجمات إلكترونية تؤدي إلى سرقة الأصول أو نقلها إلى محافظ مجهولة، مما يزيد من صعوبة استردادها أو تجميدها لاحقًا.

يتضح أن تجميد الأصول الرقمية لا يمكن أن يتحقق بفعالية إلا من خلال إعادة هندسة المنظومة القانونية والتقنية، بحيث تُدمج العملات المشفّرة ضمن إطار قانوني دولي موحّد، وتُعزّز القدرات الوطنية على الرصد والتتبع، مع بناء جسور تعاون قضائي وتقني عابر للحدود، كما أن التفكير في بدائل مثل العملات الرقمية للبنوك المركزية (CBDC) قد يشكل خطوة مهمة نحو توفير وسيلة دفع آمنة وشفافة يمكن إخضاعها لآليات التجميد بفعالية، دون أن تُفرّغ من مضمونها التقني أو الاقتصادي.

وتعدّ تجربة دولة الإمارات العربية المتحدة أنموذجاً عربياً رائداً في التنظيم الاستباقي للعملات المشفرة ففي مارس 2022، أصدرت قانون تنظيم الأصول الافتراضية، الذي يُنشئ هيئة تنظيم الأصول الافتراضية ((VARAفي دبي، وتُلزم المنصات بتطبيق معايير KYC/AML صارمة، مع السماح للسلطات بتجميد الأصول فورياً في الحالات الطارئة[34].

وأثبتت هذه الاستراتيجية نجاحاً عملياً، إذ أظهر تقرير Chainalysis (2023) أن 95% من المحاولات المشبوهة تم رصدها خلال 24 ساعة. وفي يناير 2023، نجحت الإمارات في تجميد محفظة رقمية بقيمة 12 مليون دولار مرتبطة بتمويل حزب الله، عبر التعاون مع منصة BitOasis، مما يُبرز أهمية الشراكة بين القطاع الخاص والحكومة[35]، وهكذا، تُظهر التجربة الإماراتية أن الانتقال من الفراغ التشريعي إلى التنظيم الاستباقي يُمكن السلطات من ممارسة سلطة تجميد فعالة دون تعطيل الابتكار

الخاتمة

في ضوء ما سبق يتضح أن تجميد الأصول الرقمية يمثل أداة قانونية حيوية لمكافحة تمويل الإرهاب، الا ان فعاليتها تصطدم بتحديات هيكلية عميقة، تتقاطع فيها الابعاد التقنية مع الفجوات التشريعية والقصور في التعاون الدولي، إذا افرزت الثورة الرقمية، واقعا ماليا جديدا يتجاوز حدود السيادة التقليدية للدول، حيث يفرض على المنظومة القانونية الدولية والمحلية ضرورة التكيف السريع لمواجهة مخاطرة الأمنية المتنامية، ومن خلال تحليل الخصائص الجوهرية للعملات تبين إن الطبيعة اللامركزية للعملات المشفّرة، وإخفاء الهوية، وسرعة التحويلات العابرة للحدود، قد تحولت الى ملاذ امن للجماعات الإرهابية لتمويل أنشطتها بعيدا عن اعين السلطات القضائية والمالية، ورغم ان المجتمع الدولي ارسى قواعد لتجميد الأصول من خلال اتفاقيات وقرارات اممية، وان تطبيق هذه القواعد على الفضاء الرقمي لايزال متعثرا، مما يترك ثغرات واسعة تستغلها الشبكات الاجرامية.

ويواجه العراق خطرا متزايدا من استغلال الأصول الرقمية في تمويل الإرهاب نتيجة غياب التشريعات المنظمة، وضعف القدرات التقنية والمؤسسية الى جانب عوامل اقتصادية واجتماعية تدفع الافراد لاستخدام العملات المشفرة دون وعي، مما يجعله بيئة قابلة لعمليات غسل الأموال والتمويل غير المشروع.

وبذلك، فإن مواجهة هذه الظاهرة تتطلب مقاربة متعددة الأبعاد، تجمع بين تطوير التشريعات، وتعزيز التعاون الدولي، وبناء قدرات تقنية متقدمة، إلى جانب التفكير في بدائل تنظيمية مثل العملات الرقمية للبنوك المركزية (CBDC) التي يمكن أن تُشكّل أداة دفع مشروعة وخاضعة للرقابة.

اولاً / الاستنتاجات:

بناء على ما تقدم من تحليل معمق لفعالية تجميد الأصول الافتراضية في مكافحة تمويل الإرهاب، يمكن استخلاص جملة من الاستنتاجات الجوهرية التي تلقي الضوء على التحديات القائمة والمسارات المستقبلية:

1- تبين لنا ان القواعد القانونية التقليدية سواء على مستوى الوطني او الدولي والمصممة للتعامل مع الأصول المالية، تعاني من قصور واضح في مواجهة الطبيعة اللامركزية والافتراضية للأصول، مما يخلق فراغا تشريعيا واجرائيا تستغله الجماعات الإرهابية لتمويل أنشطتها.
2- ان الخصائص التقنية للأصول الافتراضية تزيد من صعوبة تتبع هذه المعاملات وتحديد المستفيدين النهائيين، مما يعرقل جهود التجميد الفعالة، ولا يمكن أيضا مواجهة تحديات تجميد الأصول الافتراضية الامن خلال مقاربة شاملة بين التحديث التشريعي، والتعاون الدولي الفعال، وتطوير القدرات التقنية وتعزيز الشركات مع القطاع الخاص ورفع الوعي المجتمعي.
3- كما تبرز مشكلة تحديد الولاية القضائية في الفضاء الرقمي كعقبة رئيسة امام التعاون الدولي في تجميد الأصول، فغياب التعريف الموحد وقوع الجريمة او مكان وجود الأصل واستغلال الملاذات الرقمية، يحد من قدرة الدول على فرض سيادتها القانونية.

ثانياً / المقترحات :

1- على المشرع العراقي الإسراع في تشريع قانون ينظم الأصول الرقمية ويجب ان يتضمن تعريفا دقيقا للعملات الرقمية، ويحدد الجهات الرقابية المسؤولة ووضع قواعد واضحة لترخيص منصات التداول، والزامها بتطبيق معايير اعرف عميلك ومتطلبات مكافحة غسل الأموال وتمويل الإرهاب (kyc. Aml)، كما يجب ان ينص القانون على منح القضاء صلاحية التجميد والمصادرة.
2- يجب على الحكومة العراقية التنسيق مع البنك المركزي والجهات الأمنية مثل جهاز المخابرات الوطني ومستشارية الامن القومي واطلاق برنامج وطني لبناء القدرات في مجال التحليل المالي، وتطوير الكفاءات الوطنية تقنيا وامنيا عبر التدريب على تحليل البلوك تشين وانشاء وحدات متخصصة
3- تعزيز التعاون والشراكات مع الدول والمنظمات الدولية اذ يجب على العراق الانضمام بفعالية الى المبادرات الدولية والإقليمية لمكافحة تمويل الإرهاب الرقمي، وتبادل المعلومات والاستفادة من خبرات المنظمات الدولية، وطلب المساعدة الفنية من الدول التي قطعت شوطا في هذا المجال، والتعاون مع شركات التكنولوجيا المالية لتطوير اليات رصد المعاملات المشبوهة، وتسهيل أوامر التجميد والاستفادة من خبرات القطاع الخاص في فهم التطورات التقنية المستجدة.

4- نشر الوعي بمخاطر العملات المشفرة غير المنظمة والعواقب القانونية المرتبطة بها من خلال إقامة حملات توعية مجتمعية اذ لا يمكن لأي استراتيجية ان تنجح من دون وعي مجتمعي، لذا يجب تحذير الشباب والمستثمرين من مخطر التعامل مع العملات المشفرة عبر منصات غير مرخصة، وتوضيح العقوبات القانونية المترتبة على التورط عن قصد او عن غير قصد في عمليات غسل الأموال او تمويل الإرهاب، كما يمكن لوسائل الاعلام ومنظمات المجتمع المدني من لعب دور حيوي في نشر هذه الرسائل.

ـ الهوامش :

[1] هاجر فهد السيد أحمد، "العملات الرقمية"Digital Currencies - ، الموسوعة السياسيّة، 2024-05-13، تاريخ آخر دخول: 2025-03-04 09:26، متاح على الرابط التالي: https://political-encyclopedia.org/dictionary/

[2] احمد يحيى محمد، "العملات الرقمية: نشأتها وتطورها ومخاطر التعامل فيها"، المجلة العلمية، مصر، جامعة أسيوط كلية التجارة، العدد73، 2021

[3] United Nations Office on Drugs and Crime (UNODC), Terrorism Financing in the Digital Age, UNODC Report, 2021, p5.

[4] مينا مهدي عبدالله، الهام إبراهيم حسين، التنظيم الضريبي للعملات الرقمية: منظور مالي وجنائي، ص10.

[5] حاتم حردان حياد، عمر حسين رشيد، "دور العملات الافتراضية المشفرة في تمويل جريمة الإرهاب "مجلة جامعة الانبار للعلوم القانونية والسياسية، 2، (2025-01)، 1399 - 1410، تاريخ الاسترداد: 2025-02-09 22:11، متاح على الرابط التالي: https://political-encyclopedia.org/index.php/library/9776

[6] United Nations Office on Drugs and Crime (UNODC), Terrorism Financing in the Digital Age, UNODC Report, 2021,p15.

[7] ياسر حسين علي، المخاطر الدولية المالية للتعامل بالعملات الرقمية المشفرة البيتكوين انموذجا، مجلة كلية الحقوق، جامعة النهرين، المجلد24، العدد2،2022، ص163.

[8] He, D., Habermeier, K., Leckow, R., Haksar, V., Almeida, Y., Kashima, M., Kyriakos-saad, N., Oura, H., Sedik, T. S., & Stetsenko, N. (2016). Virtual Currencies and Beyond: Initial Considerations (SDN/16/13; Staff Discussion Notes).

[9] صقر محمد العطار، عبد الإله محمد النوايسة الحماية الجنائية لمستخدمي العملات الرقمية الافتراضية في القانون الإماراتي، مجلة جامعة الشارقة للعلوم القانونية، 2024، ص219

[10] مكتب الأمم المتحدة المعني بالمخدرات والجريمة، Terrorism Financing in the Digital Age، تقرير 2021، ص 5

[11] عبدالله بن سليمان، النقود الافتراضية، مفهومها وانواعها واثارها الاقتصادية، ورقة علمية مقدمة لمركز التميز البحثي في فقه القضايا المعاصرة، جامعة الامام محمد بن سعود الإسلامية،2018،ص47

[12] زيدان لخضر، تحليل مخاطر وتحديات تطوير واستخدام العملات الافتراضية ذات سلاسل الكتل الموزعة، مجلة العلوم الاقتصادية، مجلد12، العدد2، 2017، ص34.

[13] ايسر ياسين فهد، اثر العملات الرقمية المشفرة والقانونية في فاعلية السياسات النقدية الدولية، مجلة الريادة للمال والاعمال، المجلد الثالث، العدد3، 2022، ص183.

[14] Prof. Dr. Robby HOUBEN, European Parliament, Cryptocurrencies and block chain, July 2018.

[15] ايسر ياسين فهد، مصدر سابق، ص187

[16] محمد عبد القادر، العملات الرقمية .. والتهديد الافتراضي، جريدة الاهرام بتاريخ 24 أكتوبر 2018

[17] RAND Corporation, National Security Implications of Virtual Currency, RAND Report, 2020, p. 14.

[18] احمد النجار، العملات الافتراضية المشفرة، دراسة اقتصادية شرعية محابية، دار النفائس، عمان،2019، 32

[19] Financial Action Task Force (FATF), Guidance for a Risk-Based Approach to Virtual Assets and VASPs, FATF Report, 2019, p. 22.

[20] خالد عطية، الوفاء بواسطة النقود الالكترونية المشاكل والحلول، بحث منشور في مجلة القانون المقارن، العدد39، لسنة 2006، ص99.

[21] Chainalysis. (2024). Crypto Crime Report: Terrorist Financing and Asset Freezing New York: Chainalysis Inc. p. 12.

[22] Elliptic. (2023). The State of DeFi Crime London: Elliptic Enterprises Ltd. p. 19

[23] Financial Action Task Force. (2023). Mutual Evaluation Report: United Arab Emirates FATF, Paris. para. 287.

[24] احمد قاسم فرج، العملات الافتراضية في دولة الامارات العربية المتحدة، الحاجة الى اطار قانوني لمواجهة مخاطرها، دراسة مقارنة، بحث منشور في جامعة الشارقة، العدد2 سنة 2019، ص698.

[25] انظر اتفاقية تمويل الإرهاب لعام 1999

[26] عبدالله محمد بن هويدن، نعمان عطا الله الهيتي، مدى فعالية وسائل منظمة الشرطة الدولية "الإنتربول" في مكافحة الجريمة المنظمة، مجلة جامعة الشارقة للعلوم القانونية،2023، ص39

[27] القرار(1373) لسنة 2001 المتخذ بالاجماع في 28 سبتمبر 2001

[28] علي عمران الكتبي، محمد شلال العاني، مجلس الأمن المتعلقة بالجزاءات ذات الصلة بتمويل الإرهاب، مجلة جامعة الشارقة للعلوم القانونية،2025، ص

[29] محمد جبريل إبراهيم، جريمة التعامل في العملات المشفرة او النقود الرقمية " دراسة مقارنة"، مجلة البحوث القانونية والاقتصادية، العدد79، لسنة 2022، ص1040.

[30] European Union, "Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets," Official Journal of the European Union, L 150/40, 9 June 2023.

[31] احمد قاسم فرج، العملات الافتراضية في دولة الامارات العربية المتحدة، الحاجة الى إطار قانوني لمواجهة المخاطر، حث منشور في مجلة جامعة الشارقة، العدد2 لسنة 2019، ص698.

[32] محمد صالح الحناوي، طارق الشهاوي، الاستثمار في الأوراق المالية، الدار الجامعية، 2012، ص30.

33 ايمان كاظم عباس، نغم حميد خضر، العملات المشفرة التحديات والمخاطر وسبل المواجهة، مجلة جامعة نوتنغهام للتكنولوجيا للعلوم الإدارية والإنسانية، المجلد 2، العدد3، سنة 2022، ص4

34 Dubai, مركز دبي المالي العالمي. (2022). قانون تنظيم الأصول الافتراضية والأنشطة المرتبطة بها. القانون رقم 4 لسنة 2022. المادة 3/8.

35 Chainalysis. (2023). Middle East and North Africa Crypto Report. New York: Chainalysis Inc. pp. 34-36.

المصادر

أولاً /الكتب:

1-النجار، أحمد. (2019). العملات الافتراضية المشفرة: دراسة اقتصادية شرعية محابية. دار النفائس، عمان.

2-الحناوي، محمد صالح، والشهاوي، طارق. (2012). الاستثمار في الأوراق المالية. الدار الجامعية.

ثانياً/ البحوث والمجلات العلمية:

1-إبراهيم، محمد جبريل. (2022). "جريمة التعامل في العملات المشفرة أو النقود الرقمية: دراسة مقارنة. مجلة البحوث القانونية والاقتصادية، العدد 79.

2-بن سليمان، عبدالله. (2018). "النقود الافتراضية: مفهومها وأنواعها وآثارها الاقتصادية". ورقة علمية مقدمة لمركز التميز البحثي في فقه القضايا المعاصرة، جامعة الإمام محمد بن سعود الإسلامية

3-الحياد، حاتم حردان، ورشيد، عمر حسين. (2025). "دور العملات الافتراضية المشفرة في تمويل جريمة الإرهاب". مجلة جامعة الأنبار للعلوم القانونية والسياسية، 2(01)، 1399-1410.

4-الخضر، زيدان. (2017). "تحليل مخاطر وتحديات تطوير واستخدام العملات الافتراضية ذات سلاسل الكتل الموزعة". مجلة العلوم الاقتصادية، المجلد 12، العدد 2.

5-السيد أحمد، هاجر فهد. (2024). "العملات الرقمية - Digital Currencies". الموسوعة السياسية. تاريخ آخر دخول: 04-03-2025. متاح على الرابط التالي: https://political-encyclopedia.org/dictionary/

6-العباس، إيمان كاظم، وخضر، نغم حميد. (2022). "العملات المشفرة: التحديات والمخاطر وسبل المواجهة". مجلة جامعة نوتنغهام للتكنولوجيا للعلوم الإدارية والإنسانية، المجلد 2، العدد 3.

7-العطار، صقر محمد، والنوايسة، عبد الإله محمد. (2024). "الحماية الجنائية لمستخدمي العملات الرقمية الافتراضية في القانون الإماراتي". مجلة جامعة الشارقة للعلوم القانونية.

8-عطية، خالد. (2006). "الوفاء بواسطة النقود الإلكترونية: المشاكل والحلول". مجلة القانون المقارن، العدد 39.

9-علي، ياسر حسين. (2022). "المخاطر الدولية المالية للتعامل بالعملات الرقمية المشفرة البيتكوين أنموذجًا". مجلة كلية الحقوق، جامعة النهرين، المجلد 24، العدد 2.

10-فرج، أحمد قاسم. (2019). "العملات الافتراضية في دولة الإمارات العربية المتحدة، الحاجة إلى إطار قانوني لمواجهة مخاطرها، دراسة مقارنة". مجلة جامعة الشارقة، العدد 2.

11-الفهد، أيسر ياسين. (2022). "أثر العملات الرقمية المشفرة والقانونية في فاعلية السياسات النقدية الدولية". مجلة الريادة للمال والأعمال، المجلد الثالث، العدد 3.

12-الكتبي، علي عمران، والعاني، محمد شلال. (2025). "مجلس الأمن المتعلقة بالجزاءات ذات الصلة بتمويل الإرهاب". مجلة جامعة الشارقة للعلوم القانونية.

13-لناصري، محمد عبد القادر. (2018). "العملات الرقمية .. والتهديد الافتراضي". جريدة الأهرام، 24 أكتوبر.

14-محمد، أحمد يحيى. (2021). "العملات الرقمية: نشأتها وتطورها ومخاطر التعامل فيها". المجلة العلمية، جامعة أسيوط كلية التجارة، مصر، العدد 73.

15-مهدي، مينا عبدالله، وحسين، إلهام إبراهيم. (بلا تاريخ). التنظيم الضريبي للعملات الرقمية: منظور مالي وجنائي، مجلة جامعة القادسية

16-الهويدن، عبدالله محمد بن، والهيتي، نعمان عطا الله. (2023). "مدى فعالية وسائل منظمة الشرطة الدولية "الإنتربول" في مكافحة الجريمة المنظمة". مجلة جامعة الشارقة للعلوم القانونية.

ثالثاً /الاتفاقيات والقرارات والقوانين الدولية:

1- الاتفاقية الدولية لقمع تمويل الإرهاب لعام 1999.

2- الاتحاد الأوروبي. (2023). " Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets". Official Journal of the European Union, L 150/40.

3- الاتحاد الأوروبي. التوجيه رقم 2018/834 المعدل للتوجيه EU2015/849 المتعلق بمكافحة غسل الأموال وتمويل الإرهاب.
4- مركز دبي المالي العالمي. (2022). قانون تنظيم الأصول الافتراضية والأنشطة المرتبطة بها. القانون رقم 4 لسنة 2022.
5- مجلس الأمن. (2001). القرار رقم (1373) المتخذ بالإجماع في 28 سبتمبر 2001.

رابعاً/ التقارير والمصادر الأجنبية:

1- Aruan, A. R., Toha, K., & Nurdin, A. R. (2025). "Digital Governance for Confiscating Crypto-Assets to Settle Tax Liabilities." Aptisi Transactions on Technopreneurship
2- Aurum Law. (2026). "Digital Assets 2026: Nine Trends That Shape Web3 - A Legal Practitioner's View." Retrieved from https://aurum.law/newsroom/digital-assets-2026-nine-trends-that-shape-web3-a-legal-practitioners-view
3-Bansod, S. (2022). "Challenges in making blockchain privacy compliant for…" PMC. Retrieved from https://pmc.ncbi.nlm.nih.gov/articles/PMC9387419/
4-BlockSec. (2026). "DeFi Compliance in 2026: A Technical Framework for Protocol Resilience." Retrieved from https://blocksec.com/blog/defi-compliance-in-2026-a-technical-framework-for-protocol-resilience
5-Chainalysis. (2023). Middle East and North Africa Crypto Report. New York: Chainalysis Inc.
6-Chainalysis. (2024). Crypto Crime Report: Terrorist Financing and Asset Freezing. New York: Chainalysis Inc.
7-CoinDesk. (2026, March 9). "U.S. Treasury signals shift on crypto mixers, acknowledges legitimate privacy uses." Retrieved from https://www.coindesk.com/policy/2026/03/09/u-s-treasury-signals-shift-on-crypto-mixers-acknowledges-legitimate-privacy-uses
8-Elliptic. (2023). The State of DeFi Crime. London: Elliptic Enterprises Ltd.
9-Financial Action Task Force (FATF). (2019). Guidance for a Risk-Based Approach to Virtual Assets and VASPs. Paris: FATF.
10-Financial Action Task Force (FATF). (2023). Mutual Evaluation Report: United Arab Emirates. Paris: FATF.

11-Harvey, C. R., Hasbrouck, J., & Saleh, F. (2026). "The evolution of decentralized exchange: Risks, benefits, and oversight." Research Policy, 55(1).

12-He, D., Habermeier, K., Leckow, R., Haksar, V., Almeida, Y., Kashima, M., Kyriakos-saad, N., Oura, H., Sedik, T. S., & Stetsenko, N. (2016). Virtual Currencies and Beyond: Initial Considerations. (SDN/16/13; Staff Discussion Notes), IMF.

13-Houben, Robby. (2018). Cryptocurrencies and blockchain. European Parliament.

14-KYC-Chain. (2026). "The Stablecoin Freeze Alert: Protect Your Treasury." Retrieved from https://kyc-chain.com/stablecoin-freeze-tainted-usdt-treasury-protection/

15- RAND Corporation. (2020). National Security Implications of Virtual Currency. RAND Report.

16-ResearchGate. (2026). "Conflicts of Laws and Codes: Defining the Boundaries of Digital Jurisdictions." Retrieved from https://www.researchgate.net/publication/335306527_Conflicts_of_Laws_and_Codes_Defining_the_Boundaries_of_Digital_Jurisdictions

17-The Block. (2026, March 8). "Treasury tells Congress mixers have valid privacy uses, recommends hold law for suspicious crypto." Retrieved from https://www.theblock.co/post/392769/treasury-tells-congress-mixers-have-valid-privacy-uses-recommends-hold-law-for-suspicious-crypto

18-United Nations Office on Drugs and Crime (UNODC). (2021). Terrorism Financing in the Digital Age. UNODC Report.

19-Wang, Z., Chaliasos, S., Qin, K., Zhou, L., & Gao, L. (2023). "On how zero-knowledge proof blockchain mixers improve, and worsen user privacy." Proceedings of the ACM Conference on Computer and Communications Security.

Sources

First/ Books:

[1]Al-Najjar, A. (2019). Encrypted Virtual Currencies: An Economic and Sharia Comparative Study. Dar Al-Nafaes, Amman.

[2]Al-Hinnawi, M. S., & Al-Shahawi, T. (2012). Investment in Securities. Al-Dar Al-Jami'iyah.

Second/ Journal Articles and Research Papers:

[3]Ibrahim, M. J. (2022). "The Crime of Dealing in Encrypted Currencies or Digital Money: A Comparative Study". Journal of Legal and Economic Research, No. 79, p. 1040.

[4]Bin Sulayman, A. (2018). "Virtual Currencies: Their Concept, Types and Economic Impacts". Research Paper submitted to the Research Excellence Center in Contemporary Jurisprudence Issues, Imam Muhammad Ibn Saud Islamic University.

[5]Al-Hayyad, H. H., & Rashid, O. H. (2025). "The Role of Encrypted Virtual Currencies in Financing Terrorism Crimes". Journal of Anbar University for Legal and Political Sciences, 2(01), pp. 1399-1410.

[6]Al-Khadr, Z. (2017). "Analysis of Risks and Challenges in Developing and Using Distributed Ledger Virtual Currencies". Journal of Economic Sciences, Vol. 12, No. 2, p. 34.

[7]Al-Sayed Ahmad, H. F. (2024). "Digital Currencies". Political Encyclopedia. Available at: https://political-encyclopedia.org/dictionary/ (Last accessed: 2025-03-04).

[8]Al-Abbas, I. K., & Khadr, N. H. (2022). "Encrypted Currencies: Challenges, Risks and Confrontation Methods". Nottingham Technology University Journal of Administrative and Human Sciences, Vol. 2, No. 3, p. 4.

[9]Al-Attar, S. M., & Al-Nuwaysah, A. I. (2024). "Criminal Protection for Users of Virtual Digital Currencies in UAE Law". University of Sharjah Journal of Legal Sciences, p. 219.

[10]Atiyyah, K. (2006). "Payment by Electronic Money: Problems and Solutions". Journal of Comparative Law, No. 39, p. 99.

[11]Ali, Y. H. (2022). "International Financial Risks of Dealing with Encrypted Digital Currencies: Bitcoin as a Model". Journal of the College of Law, Al-Nahrain University, Vol. 24, No. 2, p. 163.

[12]Faraj, A. Q. (2019). "Virtual Currencies in the United Arab Emirates: The Need for a Legal Framework to Address Their Risks, A Comparative Study". University of Sharjah Journal, No. 2, p. 698.

[13]Al-Fahd, A. Y. (2022). "The Impact of Encrypted and Legal Digital Currencies on the Effectiveness of International Monetary Policies". Journal of Leadership for Finance and Business, Vol. 3, No. 3, p. 183.

[14]Al-Ketbi, A. O., & Al-Ani, M. S. (2025). "Security Council Sanctions Related to Terrorism Financing". University of Sharjah Journal of Legal Sciences.

[15]Al-Nasiri, M. A. Q. (2018). "Digital Currencies... and the Virtual Threat". Al-Ahram Newspaper, October 24.

[16]Muhammad, A. Y. (2021). "Digital Currencies: Their Origin, Development and Risks of Dealing with Them". Scientific Journal, Assiut University College of Commerce, Egypt, No. 73.

[17]Mahdi, M. A., & Hussein, I. I. (n.d.). "Tax Regulation of Digital Currencies: A Financial and Criminal Perspective". Al-Qadisiyah University Journal.

[18]Al-Huwayden, A. M. B., & Al-Hiti, N. A. (2023). "The Effectiveness of Interpol Means in Combating Organized Crime". University of Sharjah Journal of Legal Sciences, p. 39.

Third/ Conventions, Resolutions and Legislation:

[19]International Convention for the Suppression of the Financing of Terrorism, 1999.

[20]European Union. (2023). "Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets". Official Journal of the European Union, L 150/40, 9 June 2023.

[21]European Union. Directive (EU) 2018/834 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

[22]Dubai International Financial Centre. (2022). Virtual Assets Regulatory Law, Law No. 4 of 2022.

[23]United Nations Security Council. (2001). Resolution 1373 (2001), adopted unanimously on 28 September 2001.

IV. Reports and Foreign Sources

[24]Aruan, A. R., Toha, K., & Nurdin, A. R. (2025). "Digital Governance for Confiscating Crypto-Assets to Settle Tax Liabilities". Aptisi Transactions on Technopreneurship.

[25]Aurum Law. (2026). "Digital Assets 2026: Nine Trends That Shape Web3 - A Legal Practitioner's View". Retrieved from: https://aurum.law/newsroom/digital-assets-2026-nine-trends-that-shape-web3-a-legal-practitioners-view

[26]Bansod, S. (2022). "Challenges in making blockchain privacy compliant for..."PMC.Retrievedfrom: https://pmc.ncbi.nlm.nih.gov/articles/PMC9387419/

[27]BlockSec. (2026). "DeFi Compliance in 2026: A Technical Framework for Protocol Resilience". Retrieved from: https://blocksec.com/blog/defi-compliance-in-2026-a-technical-framework-for-protocol-resilience

[28]Chainalysis. (2023). Middle East and North Africa Crypto Report. New York: Chainalysis Inc.

[29]Chainalysis. (2024). Crypto Crime Report: Terrorist Financing and Asset Freezing. New York: Chainalysis Inc.

[30]CoinDesk. (2026, March 9). "U.S. Treasury signals shift on crypto mixers, acknowledges legitimate privacy uses". Retrieved from:

https://www.coindesk.com/policy/2026/03/09/u-s-treasury-signals-shift-on-crypto-mixers-acknowledges-legitimate-privacy-uses

[31]Elliptic. (2023). The State of DeFi Crime. London: Elliptic Enterprises Ltd.

[32]Financial Action Task Force (FATF). (2019). Guidance for a Risk-Based Approach to Virtual Assets and VASPs. Paris: FATF.

[33]Financial Action Task Force (FATF). (2023). Mutual Evaluation Report: United Arab Emirates. Paris: FATF.

[34]Harvey, C. R., Hasbrouck, J., & Saleh, F. (2026). "The evolution of decentralized exchange: Risks, benefits, and oversight". Research Policy, 55(1).

[35]He, D., Habermeier, K., Leckow, R., Haksar, V., Almeida, Y., Kashima, M., Kyriakos-saad, N., Oura, H., Sedik, T. S., & Stetsenko, N. (2016). Virtual Currencies and Beyond: Initial Considerations (SDN/16/13; Staff Discussion Notes). International Monetary Fund.

[36]Houben, R. (2018). Cryptocurrencies and blockchain. European Parliament.

[37]KYC-Chain. (2026). "The Stablecoin Freeze Alert: Protect Your Treasury". Retrieved from: https://kyc-chain.com/stablecoin-freeze-tainted-usdt-treasury-protection/

[38]RAND Corporation. (2020). National Security Implications of Virtual Currency. RAND Report.

[39]ResearchGate. (2026). "Conflicts of Laws and Codes: Defining the Boundaries of Digital Jurisdictions". Retrieved from: https://www.researchgate.net/publication/335306527_Conflicts_of_Laws_and_Codes_Defining_the_Boundaries_of_Digital_Jurisdictions

[40]The Block. (2026, March 8). "Treasury tells Congress mixers have valid privacy uses, recommends hold law for suspicious crypto". Retrieved from:

https://www.theblock.co/post/392769/treasury-tells-congress-mixers-have-valid-privacy-uses-recommends-hold-law-for-suspicious-crypto

[41]United Nations Office on Drugs and Crime (UNODC). (2021). Terrorism Financing in the Digital Age. UNODC Report.

[42]Wang, Z., Chaliasos, S., Qin, K., Zhou, L., & Gao, L. (2023). "On how zero-knowledge proof blockchain mixers improve, and worsen user privacy". Proceedings of the ACM Conference on Computer and Communications Security.