Journal Of the Iraqia University (73-10) August (2025)

ISSN(Print): 1813-4521 OnIine ISSN:2663-7502
Journal Of the Iraqia University
available online at: https://www.mabdaa.edu.iq

# استراتيجيات وقائية للإمارات وإيران لمكافحة جرائم العملات المشفرة

بهجت عبد الواحد رحيم[1*]

الدكتور سعيد قماشي[2]

[1]طالب دكتوراه قانون جنائي, جامعة كاشان الحكومية, أصفهان, ايران

[2] دكتوراه قانون جنائي, جامعة كاشان الحكومية, أصفهان, ايران

# Preventive Strategies for the UAE and Iran to Combat Cryptocurrency Crimes

**Bahjat Abdulwahid Raheem[1*], Dr. Saeed Qamashi[2]**

**[1]PhD Student in Criminal Law, Kashan State University, Isfahan, Iran**

**[2]PhD in Criminal Law, Kashan State University, Isfahan, Iran**

**Corresponding Author email: bahjatabdulwahid1993@gmail.com**

## الملخص

مع التوسع المتزايد في التكنولوجيا الرقمية وظهور العملات المشفرة، تواجه العديد من الدول، بما في ذلك الإمارات العربية المتحدة وإيران، تحديات جديدة في مجال الجرائم السيبرانية وغسيل الأموال. تسعى الإمارات العربية المتحدة إلى الحد من الجرائم المرتبطة بالعملات الرقمية وإدارتها من خلال وضع لوائح صارمة واعتماد تدابير وقائية. تهدف هذه الدراسة إلى تحليل استراتيجيات الإمارات وإيران في منع الجرائم المتعلقة بالعملات الرقمية، مع التركيز على الإجراءات القانونية والتنفيذية التي تتخذها كلتا الدولتين. تعتمد السياسات الإماراتية على الإشراف والتقييس ضمن ثلاثة محاور رئيسية: حماية حقوق المستخدمين، تقليل المخاطر الاقتصادية، وتعزيز الثقة لجذب الاستثمارات. ومن بين الأدوات التنفيذية المعتمدة في هذا الإطار، فرض التزام منصات التداول الرقمية بالامتثال للوائح معرفة العميل (KYC)، تطبيق الرقابة المستمرة، وإنشاء أنظمة الإبلاغ عن المعاملات المشبوهة. كما تركز الدولة على التعاون الدولي والاستفادة من التقنيات المتقدمة مثل البلوكتشين والذكاء الاصطناعي لمكافحة غسيل الأموال، تمويل الإرهاب، وأنواع الاحتيال الرقمي المختلفة. وتكشف نتائج هذه الدراسة أن الجمع بين التدابير القانونية والتكنولوجيا الحديثة قد أسهم في الحد من التهديدات المتعلقة بالعملات الرقمية في الإمارات، مما جعلها إحدى الدول الرائدة في مجال تنظيم هذا القطاع. ومع ذلك، لا تزال هناك تحديات قائمة، مثل الحاجة إلى قوانين أكثر وضوحًا وتحقيق توازن بين التنظيم والابتكار الاقتصادي. لذلك، يُوصى بأن تستمر الدولتان، لا سيما الإمارات، في مواءمة لوائحها بشكل مستمر مع المعايير الدولية لحماية نفسها من التهديدات المستجدة في مجال الجرائم السيبرانية.

الكلمات المفتاحية: التدابير الوقائية، التجريم، الجرائم السيبرانية، العملات الرقمية، القانون الجنائي الإماراتي، القانون الجنائي.

## Abstract

Preventive Strategies of the United Arab Emirates and Iran in Combating Digital Currency Crimes

With the rapid expansion of digital technologies and the emergence of cryptocurrencies, many countries, including the United Arab Emirates and Iran, have faced new challenges in cybercrime and money laundering. The UAE, through the enactment of stringent regulations and the adoption of preventive measures, seeks to control and manage crimes related to digital currencies. This study examines the strategies of the UAE and Iran in preventing digital currency crimes and analyzes the legal and executive measures undertaken by both countries. According to UAE policies, oversight and standardization are pursued through three main pillars: protecting users' rights, mitigating economic risks, and fostering trust to attract investment. Among the key executive measures in the UAE are mandating digital exchanges to comply with Know Your Customer (KYC) regulations, implementing continuous monitoring, and establishing reporting systems for suspicious transactions. International cooperation and the utilization of advanced technologies such as blockchain and

artificial intelligence are also prioritized to combat money laundering, terrorist financing, and various forms of digital fraud. The findings of this study indicate that the combination of legal measures and advanced technologies has significantly reduced digital currency-related threats in the UAE, positioning it as one of the leading regulators in this domain. However, challenges remain, such as the need for clearer regulations and achieving a balance between regulatory enforcement and economic innovation. Therefore, it is recommended that both countries, particularly the UAE, continuously align their regulations with international standards to remain resilient against emerging cybercrime threats.**Keywords:** Preventive Measures, Criminalization, Cybercrime, Digital Currency, UAE Criminal Law, Criminal Law.

## المقدمة

في السنوات الأخيرة، أدى توسع التكنولوجيا المالية وظهور العملات الرقمية إلى توفير فرص اقتصادية جديدة، إلا أنه في الوقت ذاته أفرز تحديات قانونية وأمنية متعددة. فالعملات المشفرة، لا سيما العملات الرقمية اللامركزية مثل البيتكوين والإيثريوم، وبسبب طبيعتها المجهولة وغير القابلة للتتبع، أصبحت بيئة خصبة لارتكاب الجرائم السيبرانية، وغسل الأموال، وتمويل الإرهاب، وعمليات الاحتيال الإلكتروني. وقد دفعت هذه الخصائص الأنظمة القانونية المختلفة إلى سن تشريعات وإصدار لوائح جديدة لوضع أطر رقابية وجنائية تُمكن من السيطرة على هذه الظاهرة وإدارتها بفاعلية. تبنّت كل من دولة الإمارات العربية المتحدة وإيران، باعتبارهما دولتين متقدمتين في مجال التكنولوجيا المالية والتجارة الإلكترونية، تدابير وقائية لمواجهة الجرائم المرتبطة بالعملات الرقمية. فقد سعت الإمارات العربية المتحدة، من خلال سنّ قوانين جنائية خاصة ووضع لوائح تنظيمية صارمة، إلى تحقيق توازن بين التنمية الاقتصادية والأمن المالي. ومن أبرز القوانين التي تم إقرارها في هذا السياق، القانون الاتحادي رقم ١٤ لسنة ٢٠١٨ بشأن المصرف المركزي والسياسة النقدية، الذي نصّ في مادته ٥٤ على أن الدرهم هو الوحدة النقدية الرسمية الوحيدة في الدولة، وحظر استخدام أي عملة رقمية كبديل للعملة الوطنية.كما ألزم قانون مكافحة غسل الأموال وتمويل الإرهاب (القانون الاتحادي رقم ٢٠ لسنة ٢٠١٨) منصات تبادل العملات الرقمية بالامتثال للوائح معرفة العميل (KYC) وتقديم التقارير المالية المشبوهة إلى وحدة المعلومات المالية (FIU). بالإضافة إلى ذلك، أصدرت هيئة تنظيم الأوراق المالية والسلع (SCA) في الإمارات توجيهات خاصة تحدد الأطر التنظيمية الجديدة لأنشطة منصات تداول العملات الرقمية ومقدمي الخدمات ذات الصلة. علاوة على ذلك، جرّم قانون الجرائم الإلكترونية (القانون الاتحادي رقم ٥ لسنة ٢٠١٢) في تعديلاته الأخيرة أي استخدام غير قانوني للعملات الرقمية وإنشاء منصات تداول غير مرخصة، مع فرض عقوبات صارمة على المخالفين.في المقابل، اتخذت إيران أيضًا إجراءات واسعة النطاق لتنظيم مجال العملات الرقمية. فقد نصّ قانون مكافحة غسل الأموال الإيراني الصادر عام ١٣٨٦هـ.ش ولوائحه التنفيذية على آليات خاصة لتتبع ومنع إساءة استخدام العملات الرقمية في الأنشطة غير القانونية. كما أصدر البنك المركزي الإيراني تعليمات خاصة بالعملات الرقمية، حظر بموجبها استخدام هذه العملات في عمليات الدفع الداخلية، لكنه في الوقت نفسه أضفى طابعًا قانونيًا على عملية التعدين (الماينينغ) وفق شروط محددة.من جهة أخرى، يُعدّ قانون الجرائم الإلكترونية الصادر عام ١٣٨٨هـ.ش أحد الأدوات القانونية الأساسية لمكافحة الجرائم السيبرانية المرتبطة بالعملات الرقمية. فقد فرض هذا القانون عقوبات على الأنشطة غير المشروعة في مجال العملات المشفرة، بما في ذلك إنشاء منصات غير مرخصة وإساءة استخدام البيانات المالية.تهدف هذه الدراسة إلى تحليل التدابير الوقائية التي اتخذتها كل من الإمارات العربية المتحدة وإيران لمكافحة الجرائم المرتبطة بالعملات الرقمية، وتسعى للإجابة عن السؤال التالي: كيف تمكنت الدولتان، من خلال الأدوات القانونية والتقنيات الحديثة، من منع الجرائم السيبرانية في هذا المجال؟ كما تتناول هذه الدراسة التحديات القانونية والتنفيذية القائمة، وتقدم مقترحات لتحسين الأطر القانونية والرقابية المعتمدة.

## المبحث الأول: الإطار النظري

في هذا القسم، سنتناول الإطار النظري لهذه الدراسة، مع التأكيد على أهمية التمهيد لمفهوم الشفافية، وأنواع العملات الرقمية، بالإضافة إلى الفئات المختلفة للجرائم المرتبطة بها.

### المطلب الأول: التمهيد لمفهوم الشفافية

يستلزم الدخول إلى هذا المجال فهماً دقيقاً للمسار، وإنشاء البنى التحتية اللازمة، وإزالة العقبات الموجودة. وكما أُشير في بداية هذا الفصل، فإن تحديد المسار الصحيح يُعدّ الخطوة الأولى والأهم نحو تحقيق النجاح في هذا المجال.ومن الجدير بالذكر أن تقنية البلوكشين، بخصائصها المتميزة مثل الشفافية، وعدم قابلية البيانات للتغيير، وإمكانية التسجيل والتتبع الدائم للمعلومات، أصبحت أداة فعالة لتعزيز حقوق الملكية الفكرية. حيث

يمكن أن تُحدث هذه التقنية تحولًا كبيرًا في مجالات مثل تسجيل وتتبع الملكية، وإدارة العقود الذكية، والحد من التوزيع غير القانوني للأعمال الفنية والعلمية.[1] يمكن تصنيف أنواع الرقابة ووضع المعايير في مجال البلوكشين والعملات الرقمية على النحو التالي:

أ. وضع معايير تهدف بشكل أساسي إلى حماية حقوق وأمن المستخدمين.

ب. تصميم معايير لحماية الأفراد الذين ليسوا مستخدمين مباشرين لهذا المجال، ولكن قد يتأثرون بأنشطته.

ج. تقليل التكاليف التشغيلية وتعزيز الثقة لدى الأفراد لجذب المستثمرين المحليين والأجانب.تُعدّ كل واحدة من هذه النقاط الثلاث التزامًا لا يمكن التغاضي عنه لضمان تطوير هذا المجال وسلامته. فعلى سبيل المثال، فيما يتعلق بالبند "أ"، فإن مستوى الحماية المتوفرة للمستخدمين حاليًا يكاد يكون معدومًا، مما يدفع العديد من المستخدمين إلى اللجوء إلى منصات تداول خارجية بسبب ضعف وتخلف المنصات المحلية. وغالبًا ما تكون هذه المنصات الخارجية مجرد مواقع إلكترونية دون وجود مقارّ رئيسية معروفة، الأمر الذي يزيد من مخاطر فقدان المستخدمين لكامل أصولهم الرقمية في حال قررت إدارة المنصة الاستيلاء عليها.على سبيل المثال، يمكن الإشارة إلى حالة منصّة تداول تركية، حيث قام مالكوها بسحب ما يقارب ٢ مليار دولار أمريكي من حسابات المستخدمين، مما أدى إلى خسائر فادحة للمستثمرين.لذلك، يُعدّ وضع معايير داخلية وتقديم حوافز تشجّع المستخدمين على استخدام المنصات المحلية أمرًا ضروريًا. وإذا لم يكن تحقيق هذا الهدف ممكنًا، فإن التعاون مع منصات التداول الخارجية الموثوقة والمعروفة يُعتبر خيارًا مهمًا يمكن أن يُسهم بشكل كبير في تقليل المخاطر المرتبطة بهذا المجال.أما فيما يتعلق بالبند "ب"، فهو يتضمن بُعدين أساسيين، يرتبط كلاهما بشكل مباشر بالمؤسسات المعنية. البُعد الأول يتمثل في إنشاء بنية تحتية قوية ومحصنة لمنع عمليات الاختراق وحماية بيانات المستخدمين من الضياع. ويتطلب ذلك تعزيز أمن الأنظمة واتخاذ تدابير استباقية لمنع الاختراقات المحتملة. أما البُعد الثاني، فيتعلق بتوعية المستخدمين، حيث يجب عليهم الامتناع عن مشاركة بياناتهم الحساسة مع الآخرين. بالإضافة إلى ذلك، ينبغي على الجهات المختصة إصدار تحذيرات واضحة حول العواقب المترتبة على السلوكيات غير المسؤولة. فعلى سبيل المثال، كما يدرك الأفراد المخاطر المرتبطة باستخدام دفاتر الشيكات، مثل عدم تغطية الرصيد أو العواقب القانونية لعدم الوفاء بالالتزامات، ينبغي أن يكون هناك مستوى مماثل من التوعية والإرشاد فيما يخص العملات الرقمية[2].أما البند "ج"، فيمكن اعتباره مزيجًا بين البندين "أ" و "ب"، لكنه يختلف في كونه يفترض أن جميع المستخدمين قد امتثلوا لمسؤولياتهم والتزموا بالقوانين. وفي هذه الحالة، تقع على عاتق الدولة مسؤولية التعامل بحزم مع الأفراد الذين يسعون إلى ارتكاب الجرائم في هذا المجال. ويرتبط هذا الأمر بشكل مباشر بالجانب التشريعي، حيث يجب أن توفر المنظومة القانونية الأدوات اللازمة للرقابة والمساءلة الفعالة. وسيتم تناول هذا الجانب بمزيد من التفصيل في القسم الخاص بالتشريعات القانونية.بالإضافة إلى المسؤوليات المذكورة، التي تمثل جزءًا فقط من التزامات الهيئات الحاكمة، هناك حاجة واضحة إلى اتخاذ تدابير استشرافية ووضع خطط طويلة الأمد. ويؤدي هذا المنظور المستقبلي إلى نشوء مسؤوليتين أساسيتين: الأولى تقع على عاتق الدولة، وتشمل التعليم وإصدار التحذيرات اللازمة، والثانية تخص المستخدمين وحتى المواطنين الذين لم يدخلوا بعد هذا المجال[3].في هذا السياق، تتحمل الدولة المسؤولية الرئيسية، ويمكن تعريف هذه المسؤولية تحت مفهوم "الشفافية". تعني الشفافية تقديم المعلومات الكاملة والضرورية للمواطنين حول مختلف أبعاد العملات الرقمية، لا سيما الجوانب الإجرامية المرتبطة بها. ويُعدّ هذا الأمر جزءًا من عملية التنظيم القانوني، حيث يهدف إلى توعية المستخدمين ومنعهم من الدخول، عن غير قصد، في مناطق محفوفة بالمخاطر أو أعمال تُجرّمها القوانين.على سبيل المثال، قد يعتقد مواطن عادي أن السماح للآخرين باستخدام حسابه الشخصي لإجراء معاملات مالية هو أمر غير ذي أهمية أو لا ينطوي على أي مخالفة قانونية. ولكن الشخص المطلع يدرك أن هذا الحساب يمكن استغلاله في ارتكاب جرائم خطيرة مثل تمويل الإرهاب، وغسل الأموال، ودفع الرشاوى، والاحتيال، والعديد من الجرائم الأخرى. لذلك، تلعب التوعية والتثقيف دورًا محوريًا في الوقاية من الجرائم غير المقصودة، كما تسهم في حماية المواطنين من الوقوع في المخاطر القانونية دون علمهم.

### المطلب الثاني: أنواع العملات الرقمية

تُعدّ العملات الرقمية من الظواهر الحديثة واسعة الانتشار في العالم اليوم، حيث أحدثت تغييرات جوهرية في الأنظمة المالية والاقتصادية والتكنولوجية. وبفضل تنوعها وخصائصها الفريدة، تلعب العملات الرقمية دورًا رئيسيًا في إعادة تشكيل الأنظمة المالية والاقتصادية. فمن العملات الافتراضية التي تُستخدم في بيئات محددة، إلى العملات المشفرة اللامركزية مثل البيتكوين، وصولًا إلى العملات الرقمية الوطنية التي تُدار من قبل الحكومات، يُساهم كل نوع منها في تغيير آليات التبادل المالي بطرق مختلفة.

١. العملات الافتراضية تُعدّ العملة الافتراضية إحدى الفئات الرئيسية للعملات الرقمية. وبسبب طبيعتها غير الملموسة والرقمية، تندرج ضمن مفهوم العملات الرقمية، إلا أنها تختلف عنها من حيث البنية والوظيفة. فهذه العملات تُنشأ عادة من قبل كيانات غير رسمية وتُستخدم في بيئات محددة، مثل ألعاب الفيديو أو المنصات الإلكترونية. وعلى عكس العملات المشفرة، فإن العملات الافتراضية غالبًا ما تفتقر إلى تقنية البلوكشين أو الأنظمة اللامركزية، مما يجعلها أقل أمانًا وشفافية مقارنة بالعملات المشفرة. كما أن غياب بنية تنظيمية قوية لهذه العملات يُعرض مستخدميها لمخاطر أكبر، خاصة فيما يتعلق بالاحتيال أو فقدان الأصول الرقمية. [٤]

٢. العملات المشفرة تُعدّ العملات المشفرة (الرمزارزات) نوعًا آخر من العملات الرقمية، وتتميز بخصائص فريدة جعلتها من أهم الأدوات المالية في العالم. ورغم إمكانية اعتبارها فئة فرعية من العملات الافتراضية، إلا أنها تختلف عنها من حيث الهيكل والوظيفة بشكل جوهري.

أ. العملات الرقمية (الكوينات)[٥]تُعرف الكوينات بأنها العملات المشفرة الدولية أو العالمية. ومن أبرز الأمثلة على ذلك: البيتكوين[٦]، اللايتكوين[٧]، الإيثريوم[٨] وغيرها من العملات التي تعتمد على تقنية البلوكشين. وتتميز هذه العملات باستقلاليتها، حيث تمتلك شبكات بلوكشين خاصة بها تعمل بشكل لامركزي، ما يعزز الأمان والشفافية في عمليات التحويل والتخزين. [٩]

ب. التوكنات[١٠]التوكنات هي نوع آخر من العملات الرقمية، لكنها تختلف عن الكوينات في عدة جوانب أساسية. فعلى عكس الكوينات، لا تمتلك التوكنات شبكة بلوكشين خاصة بها، وإنما تعتمد على شبكات بلوكشين أخرى، مثل شبكة الإيثريوم. [١١]

ج. العملات الرقمية الوطنية (CBDC)العملات الرقمية الوطنية، أو العملات الرقمية للبنك المركزي (CBDC)، تُصدر وتُدار من قبل الحكومات والجهات الرسمية. وعلى عكس الكوينات والتوكنات، فإن هذه العملات تخضع بالكامل لرقابة السلطات الحكومية، وعادةً ما تُصمم لتعزيز الأنظمة النقدية والمصرفية التقليدية. [١٢]

د. العملات المشفرة المدعومة بأصول[١٣]العملات المشفرة المدعومة بأصول هي نوع من العملات الرقمية التي تستمد قيمتها من أصول حقيقية أو سلع مستقرة، مثل الدولار الأمريكي، الذهب، النفط، أو حتى العملات الرقمية الأخرى. تُعتبر هذه العملات خيارًا جذابًا للمستثمرين الذين يسعون إلى مزيد من الاستقرار والأمان في استثماراتهم، نظرًا لقدرتها على الحد من التقلبات الحادة في سوق العملات الرقمية.تنقسم هذه الفئة إلى قسمين رئيسيين:العملات المشفرة المركزية المدعومة بأصول العملات المشفرة اللامركزية المدعومة بأصول لكل من هذين النوعين خصائصه الخاصة، ويقدمان مزايا وعيوبًا مختلفة وفقًا لاحتياجات المستخدمين.[١٤]العملات المشفرة المركزية المدعومة بأصول تُدار من قبل جهات محددة، وترتبط قيمتها بأصول معينة مثل الدولار أو سلع مثل النفط. يتم الاحتفاظ بهذه الأصول في صناديق خاصة لضمان استقرار قيمة العملة المشفرة. أما العملات المشفرة اللامركزية المدعومة بأصول، فهي تعمل دون رقابة من أي جهة مركزية، ويتم ضمان قيمتها من خلال آليات لامركزية.

٣. العملة الرقمية للبنك المركزي (CBDC)العملة الرقمية للبنك المركزي (CBDC) هي أحد المفاهيم الحديثة في المجال المالي والتكنولوجي، وقد طُوّرت من قبل الحكومات والبنوك المركزية استجابةً لظهور العملات المشفرة مثل البيتكوين. لقد أدّى ظهور تقنية البلوكشين والعملات المشفرة إلى تحدي البنى التقليدية للنظامين النقدي والمالي، مما دفع الحكومات إلى البحث عن حلول جديدة للحفاظ على السيطرة على الأنظمة النقدية.على الرغم من أن العملات المشفرة مثل البيتكوين قُدّمت كابتكار في صناعة المدفوعات، إلا أنها لم تتمكن من أن تصبح أداة دفع واسعة الانتشار في الحياة اليومية، بل استُخدمت بشكل رئيسي كوسيلة للحفاظ على قيمة الأصول والاستثمار.[١٥] إحدى أبرز سمات العملات الرقمية الوطنية هي ارتباطها بالعملة الورقية[١٦]حيث تخضع هذه العملات لسيطرة البنوك المركزية أو الهيئات الحكومية، وتستمد قيمتها من أصول مثل الدولا أو العملة الوطنية للدولة المُصدِرة. وعلى عكس العملات المشفرة اللامركزية، فإن هذه الأنظمة تخضع لمراقبة كاملة على المعاملات، حيث تتيح للبنوك المركزية إمكانية الوصول إلى حسابات المستخدمين. هذه الخاصية، ورغم توفيرها للأمان والشفافية، تُثير تحديات تتعلق بالخصوصية المالية.

### المطلب الثالث: تصنيف الجرائم المرتبطة بالعملات الرقمية

أحدثت تقنية العملات المشفرة، بخصائصها الفريدة، تحولات هائلة في المجالات الاقتصادية والاجتماعية. ولم يقتصر تأثيرها على مصالح الأفراد والمؤسسات المالية فحسب، بل أدت أيضًا إلى ظهور تهديدات عبر وطنية فرضت تحديات متعددة على المجتمع الدولي.وبتحليل السمات الخاصة لهذه التقنية ودراسة دور العملات المشفرة في الجرائم المختلفة، يمكن تصنيف الجرائم المرتبطة بها إلى ثلاث فئات رئيسية:الجرائم التي يكون موضوعها العملات المشفرة.الجرائم التي تُستخدم فيها العملات المشفرة كوسيلة لتسهيل ارتكاب الجريمة.الجرائم التي تستهدف العملات المشفرة ذاتها.

١- الجرائم التي تكون العملات المشفرة موضوعًا للجريمة إحدى الجرائم الشائعة المرتبطة بالعملات المشفرة هي سرقة هذه الأصول. ففي هذا النوع من الجرائم، يستهدف المجرمون البنية التحتية والأدوات المرتبطة بالعملات المشفرة بهدف الاستيلاء عليها. وتشمل هذه الجرائم الهجمات السيبرانية على الخوادم، ومجمعات التعدين، والمحافظ الرقمية، ومنصات تبادل العملات المشفرة عبر الإنترنت. [١٧]في مثل هذه الحالات، يقوم المهاجمون باختراق الأنظمة الأمنية أو الوصول غير المصرح به إلى المفاتيح الخاصة للمستخدمين، مما يتيح لهم السيطرة على أصولهم الرقمية. يُعتبر المفتاح الخاص آلية التحقق والتصديق على ملكية العملات المشفرة، ويتم تخزينه رقميًا. وإذا تمكن أحد المهاجمين من الاستحواذ على هذا المفتاح، فإن ملكية العملة المشفرة تنتقل إليه، مما يجعل استعادة الأصول المسروقة أمرًا شبه مستحيل. [١٨]اتخذت دولة الإمارات العربية المتحدة خطوات فعالة في هذا المجال من خلال تبني سياسات شفافة وسنّ قوانين خاصة لمكافحة هذه الجرائم. فقد أنشأت هيئات رقابية وتنظيمية تُشرف على منصات تداول العملات الرقمية والمحافظ الإلكترونية، كما تستخدم تقنيات متقدمة لرصد وتتبع المعاملات المشبوهة.تُشكل الجرائم التي تكون العملات المشفرة موضوعها الأساسي تحديات كبيرة لصنّاع السياسات وجهات إنفاذ القانون، نظرًا للطبيعة اللامركزية والمجهولة لهذه التكنولوجيا. لذلك، فإن الفهم الدقيق لهذه الجرائم، إلى جانب سنّ تشريعات ملائمة والاستفادة من التقنيات المتطورة، يمكن أن يسهم في تقليل المخاطر والتهديدات الناجمة عنها.

٢- استخدام العملات المشفرة كأداة تسهيل ووسيلة لارتكاب الجريمة تمكنت تقنية العملات المشفرة، بخصائصها الفريدة مثل اللامركزية، الأمان العالي، وإمكانية الحفاظ على إخفاء الهوية المستخدمين، من لعب دور فعال في العديد من المعاملات المالية. إلا أن هذه الميزات، إلى جانب فوائدها، قد تسببت أيضًا في ظهور تحديات كبيرة. فقد تحولت العملات المشفرة من مجرد وسيلة لتسهيل المعاملات إلى أداة لتعزيز وتوسيع نطاق الجرائم المنظمة، بما في ذلك غسل الأموال وتمويل الإرهاب. وقد أثار هذا التحول مخاوف جدية على المستويين الوطني والدولي، حيث تواجه العديد من الدول، بما فيها الإمارات العربية المتحدة، تحديات قانونية ورقابية معقدة.إحدى التحديات البارزة الأخرى تتمثل في استخدام العملات الرقمية في عمليات غسل الأموال. نظرًا لعدم إمكانية تتبع العديد من المعاملات المشفرة، أصبحت هذه العملات أداة جذابة للمجرمين. فمن خلال تقنيات مثل إخفاء عناوين بروتوكول الإنترنت (IP) واستخدام حسابات متعددة، يستطيع الجناة إخفاء هويتهم بشكل فعال. يتطلب هذا الوضع تدابير وقائية صارمة وتعاونًا دوليًا فعالًا. وتسعى الدول المختلفة، من خلال توجيهات منظمات مثل مجموعة العمل المالي (FATF)، إلى تطوير حلول فعالة لمكافحة غسل الأموال عبر العملات الرقمية.[١٩] في هذا السياق، أصبح الإطار الضريبي للعملات الرقمية تحديًا خطيرًا أيضًا. فمن خلال المحافظ الرقمية، يمكن للمستخدمين نقل أصولهم دون دفع الضرائب المستحقة، مما يؤدي إلى تراجع الإيرادات الحكومية وزيادة معدلات التهرب الضريبي. وتعمل الدول الرائدة، مثل الإمارات العربية المتحدة، على مواجهة هذه المشكلة عبر سنّ قوانين واضحة واعتماد أنظمة رقابية متقدمة لضبط العمليات المالية الرقمية. [٢٠] إحدى النتائج السلبية الإضافية للعملات المشفرة هي زيادة احتمالات التهرب الضريبي. إذ يمكن للمستخدمين، باستخدام المحافظ الرقمية، إخفاء دخلهم الحقيقي عن الجهات الضريبية. ويُلاحظ هذا الأمر بشكل خاص في البلدان التي تعاني من أنظمة ضريبية ضعيفة أو قوانين غير فعالة، مما يؤدي إلى صعوبة مراقبة المعاملات الرقمية وتحقيق العدالة الضريبية.[٢١]

٣- العملات الرقمية كهدف للجرائم تُعدّ الهجمات السيبرانية التي تستهدف العملات الرقمية أحد التحديات الرئيسية التي تواجه هذه التكنولوجيا. حيث يستغل مجرمو الإنترنت الفيروسات والبرمجيات الخبيثة لاستهداف المحافظ الرقمية للمستخدمين. وتشمل الأساليب المستخدمة في هذه الجرائم هجمات حجب الخدمة الموزعة (DDoS)، وهجمات التصيد الاحتيالي (Phishing)، بالإضافة إلى عمليات تشفير واحتجاز البيانات على الأجهزة الحاسوبية.لمواجهة هذه التهديدات، يُعدّ تعزيز الأمن السيبراني، وتوعية المستخدمين بطرق حماية محافظهم الرقمية، وتطوير أدوات متقدمة لرصد التهديدات، من التدابير الضرورية. إضافةً إلى ذلك، فإن التعاون الدولي لتعقب الهجمات السيبرانية واتخاذ إجراءات قانونية صارمة ضد مرتكبيها، يمكن أن يلعب دورًا مهمًا في الحد من هذه الجرائم.[٢٢]

٤- استخدام العملات المشفرة في أنواع الجرائم أدى تطور تقنية العملات المشفرة، كأحد إنجازات العصر الرقمي، إلى تأثيرات كبيرة على أساليب ارتكاب الجرائم. فبفضل خصائصها مثل إخفاء الهوية، اللامركزية، وإمكانية تحويل الأموال بسرعة وبدون وسطاء، أصبحت هذه التكنولوجيا بيئةً مثاليةً لتوسيع الأنشطة الإجرامية. كما أن الفضاء السيبراني، بصفته بيئةً افتراضية، قد وفر ساحة ملائمة لتحوّل الجرائم التقليدية وظهور أنواع جديدة من الجرائم. وقد لعبت تقنية العملات المشفرة دورًا مهمًا في هذه التغيرات من خلال تسهيل الوصول إلى مصادر مالية غير قابلة للتتبع.

مع بداية ظهور العملات المشفرة، أصدر الخبراء العديد من التحذيرات بشأن إمكانية إساءة استخدام هذه التقنية في الجرائم السيبرانية. ومع ذلك، فإن عدم الجدية في التعامل مع هذه التحذيرات أدى إلى ازدياد استخدام العملات المشفرة في الأنشطة الإجرامية. [٢٣] ووفقًا للتقارير المنشورة في

عام ٢٠١٠، تم رصد موجة من الجرائم المرتبطة بهذه التكنولوجيا. ومع مرور الوقت، شهدت هذه الجرائم ارتفاعًا ملحوظًا، مما دفع الهيئات الدولية، مثل وكالة الشرطة الأوروبية (يوروبول) ومجموعة العمل المالي (FATF)، إلى إصدار إرشادات لمكافحة هذا النوع من الجرائم.[٢٤]

أتاحت تقنية العملات المشفرة، بسبب خاصية إخفاء الهوية، إمكانية الوصول غير القانوني إلى الموارد المالية للجماعات الإرهابية. حيث تستطيع هذه الجماعات، من خلال الشبكات السيبرانية والعملات المشفرة، تمويل أنشطتها من أي مكان في العالم. وقد أثار هذا الأمر مخاوف دولية كبيرة، مما دفع منظمات مثل وكالة الشرطة الأوروبية (يوروبول) ومجموعة العمل المالي (FATF) إلى إصدار إرشادات تهدف إلى مراقبة وضبط المعاملات المرتبطة بتمويل الإرهاب.[٢٥]مع توسع تقنية العملات المشفرة، ظهرت أسواق غير قانونية عبر الإنترنت، حيث يتم بيع وشراء سلع وخدمات غير قانونية مثل المخدرات، الأسلحة، والخدمات غير المشروعة الأخرى. وقد تمكنت هذه الأسواق، بفضل استخدام العملات المشفرة وشبكات مجهولة الهوية مثل الدارك ويب، من التهرب من رقابة الجهات القانونية. ومن الأمثلة البارزة على ذلك، سوق "سيلك رود"، الذي كان أحد أشهر الأسواق غير القانونية، حيث كانت تتم جميع معاملاته باستخدام البيتكوين. [٢٦]

## المبحث الثاني: التدابير الوقائية

في هذا القسم، الذي يمثل جوهر هذه الدراسة، سيتم تحليل التدابير الوقائية التي اتخذتها كل من الإمارات العربية المتحدة وإيران لمكافحة الجرائم المرتبطة بالعملات الرقمية.

### المطلب الأول: التنظيم الجنائي لجرائم العملات الرقمية

في الأنظمة المالية والاقتصادية، يُعدّ احتكار الدولة لإصدار العملات الوطنية أحد المبادئ الأساسية للسيادة، حيث يُعتبر هذا المبدأ، الذي تلتزم به معظم الأنظمة القانونية في العالم، ضمانًا للاستقرار الاقتصادي وحمايةً للمصلحة العامة. وفي الإمارات العربية المتحدة، تم تعريف هذا الحق الحصري بوضوح في القوانين الاتحادية. وبموجب القانون الاتحادي رقم ١٤ لسنة ٢٠١٨، الخاص بالمصرف المركزي والسياسة النقدية للدولة، فإن مصرف الإمارات المركزي هو الجهة الرسمية الحصرية المسؤولة عن إدارة السياسة النقدية والإشراف على إصدار العملات.[27]وفقًا للمادة ٥٥ من هذا القانون، فإن إصدار العملة هو حق حصري للدولة، ويتولى المصرف المركزي هذه المسؤولية بشكل حصري. وتنص هذه المادة على أنه لا يجوز لأي جهة أو فرد إصدار عملة دون ترخيص قانوني، حيث يُعدّ انتهاك هذا القانون جريمة تستوجب عقوبات قانونية صارمة.[٢٨]أما في الجمهورية الإسلامية الإيرانية، فإن أول إجراء تنظيمي في مجال العملات المشفرة يعود إلى قرار الجلسة الثلاثين للمجلس الأعلى لمكافحة غسل الأموال، الصادر بتاريخ ٩ دي ١٣٩٦ (٣٠ ديسمبر ٢٠١٧). وقد نص هذا القرار بوضوح على حظر التعامل بالعملات المشفرة، مشددًا على ضرورة منع استغلال هذه الأدوات في الأنشطة غير القانونية.وجاء في نص القرار ما يلي: "نظرًا إلى أن أنواع العملات الافتراضية قد تصبح أداةً لغسل الأموال، وتمويل الإرهاب، وتحويل الأموال غير المشروعة، فقد أصدر البنك المركزي تعليمات تحظر استخدام هذه العملات، وذلك لمنع وقوع الجرائم المالية من خلال هذه الأدوات. وبناءً عليه، فإن جميع فروع ووحدات البنوك، والمؤسسات الائتمانية، وشركات الصرافة، ملزمة بالامتناع كليًا عن بيع أو شراء هذه العملات أو القيام بأي إجراء يسهم في تسهيل أو ترويج استخدامها. كما تم التأكيد على ضرورة التعامل مع المخالفين وفق القوانين واللوائح ذات الصلة." [٢٩]يتولى البنك المركزي الإيراني، في إطار مهامه المتعلقة بالسياسات النقدية والمصرفية، وضع السياسات اللازمة للأنشطة التي قد تؤثر على النظام المالي والنقدي في البلاد. وبناءً على ذلك، دخل البنك المركزي مجال تنظيم العملات المشفرة، رغم أن هذا المسار لا يزال في مراحله الأولية.في هذا السياق، قام البنك المركزي، من خلال معاونية التقنيات الحديثة لإدارة أنظمة الدفع، في عام ١٣٩٧هـ.ش (٢٠١٨م)، بإصدار الضوابط والمتطلبات المتعلقة بالعملات المشفرة. وقد تم وضع هذه الضوابط بهدف تشجيع استخدام العملات المشفرة مع إدارة تأثيراتها المحتملة على السياسات النقدية والمالية في البلاد، بحيث يتم خلق فرص جديدة للمستخدمين مع توعيتهم بالمخاطر والتهديدات المرتبطة بهذه الفئة من الأصول.كما قام البنك المركزي، بهدف منع الخسائر المحتملة، وحماية حقوق المستهلكين، وتسهيل الأنشطة التجارية في هذا المجال، بنشر الإطار التنظيمي الأولي للعملات المشفرة، الذي تمت الموافقة عليه من قبل مجلس النقد والائتمان. ويتضمن هذا الإطار تعريفًا دقيقًا لأنواع العملات المشفرة المختلفة، وذلك تمهيدًا لتنظيم هذا القطاع بشكل أكثر تفصيلًا في المستقبل.[٣٠]لتعزيز احتكار الدولة في إصدار العملة ومنع المخالفات، فرض المشرّع الإماراتي عقوبات صارمة على منتهكي القوانين المتعلقة بإصدار العملات.[31] الأفراد الذين يخالفون هذه القوانين قد يواجهون عقوبة بالسجن لمدة تصل إلى ٢٠ عامًا، أو غرامة مالية تصل إلى ١٠٠ مليون درهم، وفي بعض الحالات، يمكن تطبيق العقوبتين معًا. تعكس هذه العقوبات النهج الحازم الذي تتبعه الإمارات في التصدي للأنشطة غير القانونية المتعلقة بإصدار العملات الرقمية.[٣٢]

يتعين على البنك المركزي الإماراتي ضمان أن تكون السيولة المتداولة والودائع المصرفية مدعومة دائمًا بمصادر مالية مستقرة. ويُعتبر هذا الالتزام أحد الأسس الرئيسية للحفاظ على الاستقرار النقدي ومنع الأزمات المالية.[33] وفقًا للمادة ٥٤ من القانون الاتحادي لدولة الإمارات العربية المتحدة، تم تعريف الدرهم باعتباره الوحدة النقدية الرسمية للدولة. وتؤكد هذه المادة على أن الدرهم هو العملة القانونية والرسمية الوحيدة في البلاد، وأي عملة أخرى تُطرح كبديل تُعتبر غير قانونية وغير معترف بها رسميًا. [٣٤]أعلن البنك المركزي الإماراتي عن حظر استخدام العملات الرقمية غير الرسمية، مثل البيتكوين والعملات المشابهة. ويرجع السبب الرئيسي لهذا الحظر إلى حماية السيادة النقدية ومنع التأثيرات السلبية المحتملة على قيمة الدرهم باعتباره العملة الرسمية للدولة. كما أكد البنك المركزي أن قبول أو رفض العملات الرقمية يتطلب دراسات شاملة وتحليلًا دقيقًا لتأثيراتها على النظام المالي والاقتصادي للبلاد.تُعد إمارة دبي واحدة من الرواد العالميين في استخدام تقنية البلوكشين، وقد قامت بإطلاق أول عملة رقمية رسمية تحت اسم "إم كاش" (EMCASH). وتُعتبر هذه العملة الرقمية مدعومة بالدرهم الإماراتي، وهي مصممة ضمن إطار قانوني واضح وتحت إشراف البنك المركزي. وتتميز "إم كاش" بخصائص تجعلها مختلفة تمامًا عن العملات غير الرسمية مثل البيتكوين. [٣٥]أما في إيران، فقد اتبعت الدولة نهجًا محافظًا فيما يتعلق بالملكية الفكرية وتكنولوجيا البلوكشين. خلال السنوات الأخيرة، أبدت بعض المؤسسات الإيرانية، لا سيما في المجالات الأكاديمية والبحثية، اهتمامًا باستخدام تقنية البلوكشين لحفظ وتوثيق حقوق الملكية الفكرية والعلمية. ومع ذلك، فإن غياب البنية التحتية القانونية المناسبة، وعدم وجود أطر تنظيمية واضحة لاعتماد هذه التقنية، قد أعاق تقدم إيران في هذا المجال.في الوقت ذاته، التزمت إيران ببعض الاتفاقيات الدولية المتعلقة بحماية الملكية الفكرية، إلا أن التنفيذ الفعلي لهذه الالتزامات يواجه تحديات بسبب ضعف البنية التحتية والعقوبات الاقتصادية المفروضة على البلاد.من ناحية أخرى، تُعد الإمارات العربية المتحدة من الدول الرائدة في تبني تقنية البلوكشين وحماية حقوق الملكية الفكرية. فقد قامت الدولة بإنشاء مناطق اقتصادية حرة مثل مركز دبي المالي العالمي (DIFC) وسوق أبوظبي العالمي (ADGM)، مما وفر بيئة مناسبة لتطوير تقنية البلوكشين وتوظيفها في حماية الملكية الفكرية.[36] وفي مايو ٢٠١٧، تم في دبي إطلاق أول عملة رقمية متوافقة مع الشريعة الإسلامية تحت اسم "وان غرام" (OneGram). وتتميز هذه العملة بأنها مدعومة باحتياطي حقيقي من الذهب، وتهدف إلى تقديم بديل إسلامي للعملات الرقمية التقليدية. وتعكس هذه المبادرات جهود الإمارات في مواءمة الابتكارات المالية مع المبادئ الدينية والثقافية. [٣٧]

### المطلب الثاني: نظام الإبلاغ والشفافية ومتطلباته

تركز الإمارات العربية المتحدة على إنشاء نظام فعال للإبلاغ والشفافية في المعاملات المتعلقة بالعملات الرقمية، وذلك لضمان الاستقرار الاقتصادي ومكافحة الجرائم المرتبطة بهذه العملات. وقد فرضت الدولة على منصات تداول العملات الرقمية ومقدمي الخدمات المالية الامتثال للوائح معرفة العميل (KYC) والإبلاغ عن المعاملات المشبوهة (STR)، بهدف الكشف السريع عن أي انتهاكات أو حالات استغلال محتملة وملاحقتها. وفي هذا السياق، أصدرت هيئات مثل المصرف المركزي الإماراتي وهيئة الأوراق المالية والسلع (SCA) إرشادات خاصة بشأن كيفية الإبلاغ وإدارة بيانات المعاملات الرقمية، وذلك لتعزيز أقصى درجات الشفافية في بيئة العملات الرقمية.[٣٨]إحدى الركائز الأساسية في نظام التقارير في الإمارات هي التعاون الوثيق بين منصات تداول العملات الرقمية ووحدة المعلومات المالية (FIU). يجب على هذه المنصات الإبلاغ عن أي معاملات غير عادية أو غامضة إلى الوحدة، حتى تُجرى التحقيقات القضائية اللازمة في حال ثبوت احتمال ارتكاب جريمة. كما أن استخدام التقنيات الحديثة مثل البلوكشين الخاص، وأدوات تحليل البيانات الكبيرة (Big Data)، والذكاء الاصطناعي يُسهم في تسريع عملية الكشف عن المعاملات المشبوهة. علاوة على ذلك، تقوم شرطة الإنترنت الإماراتية برصد المعلومات المتعلقة بالمحافظ الرقمية المشبوهة والوجهات النهائية للعملات الرقمية، من خلال تفاعل مستمر مع هذه المنصات والمؤسسات المالية الأخرى. إن تطوير وتعزيز نظام التقارير في الإمارات، إلى جانب خلق الشفافية والأمان، يضفي مصداقية على البلاد على المستوى الدولي. إن التعاون عبر الحدود مع منظمات مثل الإنتربول (Interpol) أو مجموعة العمل المالي (FATF) يُظهر أن نهج الإمارات لا يقتصر فقط على الوقاية والقمع للجرائم داخل حدودها، بل يأخذ في الاعتبار أيضًا المعايير العالمية. كما تسعى الإمارات، من خلال تبادل المعلومات وإبرام الاتفاقيات الثنائية أو المتعددة الأطراف، إلى القضاء على الثغرات المحتملة في تتبع المعاملات الرقمية، وفي الوقت نفسه خلق بيئة آمنة للمستثمرين الأجانب والنشاط الاقتصادي والمستخدمين العاديين مع ازدهار الأسواق الرقمية.[٣٩]في إيران، شهدت السياسات المتعلقة بالعملات الرقمية تحولًا من الحظر المطلق إلى التقنين المحدود ضمن أطر محددة. ففي عامي ١٣٩٦ و ١٣٩٧ هـ.ش، حظر البنك المركزي الإيراني جميع المؤسسات المالية، بما في ذلك البنوك وشركات الصرافة الرسمية، من أي أنشطة مرتبطة بالعملات الرقمية، بحجة أن هذه التكنولوجيا قد تُستخدم كأداة لغسل الأموال وتمويل الإرهاب. استمر هذا الحظر حتى عام ١٣٩٨ هـ.ش، ولكن بسبب التحديات الناجمة عن العقوبات، بدأت الحكومة الإيرانية في تخفيف القيود، حيث أقرت اللائحة التنفيذية لاستخراج المنتجات

المشفرة، مما سمح بتعدين العملات الرقمية بشكل قانوني بعد الحصول على ترخيص من وزارة الصناعة والمناجم والتجارة (صمت). ومع ذلك، لا يزال استخدام العملات الرقمية كوسيلة للدفع داخل البلاد غير قانوني، كما أن الحكومة والنظام المصرفي لا يقدمان أي ضمانات بشأن قيمة هذه العملات. بالإضافة إلى ذلك، وفقًا للقوانين الجديدة، فإن استيراد وتصنيع وتشغيل معدات التعدين يتطلب الحصول على تصريح رسمي من وزارة "صمت" والامتثال للوائح الجمركية المعمول بها.التنسيق والاتصالات الدولية أهمية التنسيق مع اللوائح الدولية في عصر التوسع المستمر في تكنولوجيا المعلومات، وخاصة على الصعيد العالمي، أصبحت أكثر وضوحًا. يعود ذلك إلى أن العديد من الجرائم التي تُرتكب في هذا المجال لها صلة مباشرة خارج حدود الدولة. فعلاً، لا يمكن للحدود الجغرافية أن تعمل بعد الآن كعائق لارتكاب الجرائم الإلكترونية، لأن الفضاء الرقمي لا يقتصر على دولة أو منطقة محددة. إن الفضاء السيبراني هو بيئة بلا حدود، ولا يخضع للقوانين التقليدية التي وضعها السياسيون، وعلى خلاف الحدود الطبيعية، لا يمكن تقسيمه أو تحديده. اليوم، جزء كبير من الجرائم المنظمة، مثل غسيل الأموال والاتجار، يُنفذ كليًا أو جزئيًا من خلال الكمبيوترات ومن خلال الفضاء السيبراني. وهذا يعكس الحاجة إلى التنسيق والتعاون الواسعين بين الدول لمكافحة هذا النوع من الجرائم. لفهم أفضل لهذه المسألة، يجب أن نأخذ في الاعتبار أن الجرائم الإلكترونية بسبب طبيعتها العابرة للحدود، غالبًا ما تشمل دولًا عديدة. على سبيل المثال، يمكن الإشارة إلى الجرائم التي ينطلق فيها الفاعلون المجرمون من دولة معينة، وتؤثر نتائجها في دول أو مناطق أخرى. فمثل هذه الظروف تجعل التعاون الدولي والتكامل بين الدول ضرورة حتمية: تم تلقي بريد إلكتروني تهديدي يتضمن تهديدًا بتفجير متجر للمواد الغذائية في لاتفيا. وبعد تحقيقات واسعة، تبين أن الجاني كان يقيم في إستونيا وكان يستخدم الفضاء السيبراني لتنفيذ أعماله. في مثال آخر، تم تهديد مقر الشرطة النرويجية عبر رسائل البريد الإلكتروني. وعلى الرغم من الجهود الأولية، فلم يتم التعرف على الجاني. لكن الشرطة النرويجية وبمساعدة الشرطة الجنائية الدولية "الإنتربول"، وبعد التحقيقات المكثفة، أعلنت الحكومة الكندية أن الشخص المعني قام بتسجيل نطاقه في كندا وكان يستخدم خطوط الإنترنت هناك. ومع ذلك، خلافًا لتوقعات الإنتربول بأن الجاني كان يقيم في كندا، تبين أن الجاني كان يقيم في النرويج وعلى نفس الشارع الذي يقع فيه مقر الشرطة النرويجية.أصبحت أهمية التنسيق مع اللوائح الدولية في عصر التوسع المتزايد لتكنولوجيا المعلومات، لا سيما على المستوى العالمي، أكثر وضوحًا من أي وقت مضى. ويرجع ذلك إلى أن العديد من الجرائم المرتكبة في هذا المجال ترتبط مباشرة بما يحدث خارج حدود الدولة. في الواقع، لم تعد الحدود الجغرافية قادرة على العمل كعائق أمام ارتكاب الجرائم الإلكترونية، إذ إن الفضاء الرقمي لا يقتصر على دولة أو منطقة معينة.الفضاء السيبراني هو بيئة بلا حدود لا تلتزم بالقوانين التقليدية التي يحددها السياسيون، وعلى عكس الحدود الطبيعية، لا يمكن تقسيمه أو تقييده. اليوم، يتم تنفيذ جزء كبير من الجرائم المنظمة، مثل غسل الأموال والاتجار، بالكامل أو جزئيًا عبر أجهزة الكمبيوتر والفضاء السيبراني. وهذا يدل على الحاجة الملحة للتنسيق، وحتى التعاون الدولي الواسع، لمواجهة هذا النوع من الجرائم.لفهم هذه القضية بشكل أفضل، يجب الانتباه إلى أن الجرائم السيبرانية، نظرًا لطبيعتها العابرة للحدود، غالبًا ما تُشرك عدة دول. على سبيل المثال، يمكن الإشارة إلى الجرائم التي يبدأ فيها المجرمون نشاطهم من دولة ما وتنتشر تأثيراتها إلى دول أو مناطق أخرى. مثل هذه الظروف تجعل التعاون والتآزر الدولي ضرورة لا مفر منها:تم تلقي بريد إلكتروني تهديدي يتضمن تهديدًا بتفجير متجر لبيع المواد الغذائية في لاتفيا. وبعد تحقيقات موسعة، تبين أن الجاني كان مقيمًا في إستونيا وأنه استخدم الفضاء السيبراني لتنفيذ أعماله.وفي مثال آخر، قام شخص مجهول، من خلال بريد إلكتروني تهديدي، بتهديد مقر شرطة النرويج بتفجيره. ورغم الجهود الأولية، لم يتم تحديد هوية الشخص المعني. وبالتعاون مع شرطة الإنتربول ومن خلال المتابعات التي تمت، أعلنت الحكومة الكندية أن الشخص المعني قد سجل نطاقه في كندا وكان يستخدم خطوط الإنترنت التابعة لهذا البلد. ومع ذلك، وعلى عكس توقعات شرطة الإنتربول التي ظنت أن هذا الشخص مقيم في كندا، تبين أن الجاني كان مقيمًا في النرويج وعلى نفس الشارع الذي يقع فيه مقر شرطة النرويج.[٤٠]في جزء من "الدليل العملي لمنع الجريمة" الصادر عن الأمم المتحدة، وتحت عنوان "التعاون الفني"، تم التأكيد على ضرورة التعاون الدولي. وجاء في هذا الدليل: "يجب على الدول الأعضاء والمنظمات الدولية المسؤولة عن توفير التمويل اللازم أن توفر بيئة للتعاون المالي والفني من أجل تنفيذ المبادئ المتعلقة بضمان الأمن الجماعي ومنع الجريمة على المستويات الوطنية والإقليمية، وذلك من خلال تعزيز القدرات والهياكل وتوفير التدريب للدول النامية والمجموعات والمنظمات ذات الصلة."بناءً على ذلك، فإن استخدام التعريفات المعيارية العالمية، والاستفادة من تجارب الدول الأخرى، وإقامة التعاون الثنائي أو المتعدد الأطراف في مكافحة الجرائم السيبرانية، تعد من الشروط الأساسية لنجاح عملية تجريم هذا المجال. كما أن الفصل الثالث من اتفاقية الجرائم السيبرانية (٢٠٠١)، والذي يحمل عنوان "التعاون الدولي"، يحدد في المادة ٢٣ بعض المبادئ العامة التي ترسم إطار التعاون الدولي، وهي:

أ: يجب ضمان التعاون الدولي بين الدول الأعضاء على أوسع نطاق ممكن.

ب: يجب أن يشمل هذا التعاون جميع الجرائم المتعلقة بأنظمة الحاسوب، وكذلك جمع الأدلة الإلكترونية.

ج: ينبغي أن يتم هذا التعاون وفقًا للاتفاقيات الدولية الخاصة بالمسائل الجنائية، أو الترتيبات المتفق عليها استنادًا إلى قوانين موحدة أو ثنائية، بالإضافة إلى القوانين الوطنية.تبرز هذه المبادئ أهمية التعاون الدولي في مواجهة الجرائم السيبرانية، إذ إنه على الرغم من أن هذه الجرائم قد تبدو بسيطة عند اكتشافها، إلا أن هذه البساطة لا يجب أن تقلل من أهمية الاتفاقيات الدولية في هذا المجال. وكما ذكر سابقًا، فإن الجرائم السيبرانية لا تعترف بالحدود الجغرافية وليست مقتصرة على دولة بعينها.[٤١]حظر العملات المشفرة قررت بعض الدول حظر العملات الرقمية بالكامل بسبب طبيعتها غير المعروفة والتي يصعب السيطرة عليها. لم يقتصر هذا الحظر على المخاوف الاقتصادية فحسب، بل جاء أيضًا لمنع الاستخدامات غير القانونية لهذه العملات.أحد أهم أسباب حظر العملات الرقمية هو طبيعتها اللامركزية ومجهولية الهوية في المعاملات. هذه الخصائص تجعل من الصعب للغاية تتبع المعاملات وتحديد هوية المستخدمين، مما جعل العملات الرقمية أداة جذابة للأنشطة غير القانونية مثل غسل الأموال، وتمويل الإرهاب، والتهرب الضريبي. بالإضافة إلى ذلك، فإن إخفاء هوية المعاملات مكّن المحتالين والمجرمين من استغلال هذه العملات في عمليات الاحتيال المالي، وسرقة البيانات، وتمويل الأنشطة الإرهابية.ومن الأمثلة البارزة على سوء الاستخدام غير القانوني للعملات الرقمية، منصة ليبرتي ريزيرف (Liberty Reserve)، التي عملت بين عامي ٢٠٠٦ و٢٠١٣، وتمكنت من تحويل أكثر من ستة مليارات دولار من خلال معاملات غير قانونية، مما أثار مخاوف الدول بشأن استخدام هذه العملات في الجرائم المالية. كما يُعد سوق سيلك رود (Silk Road) نموذجًا آخر على استغلال العملات الرقمية في التجارة غير القانونية، حيث استخدم هذا السوق العملات الرقمية في بيع المخدرات، والأسلحة، وغيرها من السلع المحظورة، مما يبرز الإمكانات الكبيرة لهذه التقنية في تسهيل عمليات الاستغلال الإجرامي على نطاق واسع.[٤٢]آليات الحظر ومناهج الحكومات تجاه العملات الرقمية بناءً على المبررات المطروحة لدعم حظر العملات الرقمية، اتبعت الدول التي قررت منع استخدامها نهجين مختلفين. بعض الدول، مثل آيسلندا وروسيا، تبنت نهجًا صارمًا وفرضت حظرًا مطلقًا على استخدام وقبول العملات الرقمية. فقد منعت هذه الدول جميع الأفراد والكيانات الاقتصادية والمالية من أي نوع من التعاملات بهذه العملات، وأعلنت أن جميع الوحدات الرقمية والبدائل النقدية الافتراضية غير قانونية، بغض النظر عن نوعها.من ناحية أخرى، تبنت دول مثل الصين نهجًا أكثر نسبية. ففي الصين، تم حظر المؤسسات المالية والبنوك ومقدمي خدمات الدفع من استخدام أو تداول أو قبول العملات الرقمية. ومع ذلك، فقد سُمح للتجار والمستهلكين العاديين باستخدام هذه العملات على المستوى الشخصي وخارج الأطر الرسمية للحكومة. لكن هذه الحرية مشروطة بالتقيد بقيود صارمة تفرضها الحكومة الصينية. وضمن هذا الإطار، فإن أي خسائر ناجمة عن استخدام العملات الرقمية تقع على عاتق المستخدمين أنفسهم، إذ لا تتحمل الحكومة الصينية أي مسؤولية قانونية لحمايتهم.[٤٣]في إيران، ومع التوسع المتزايد في استخدام العملات الرقمية، ولا سيما البيتكوين، تبنى البنك المركزي لجمهورية إيران الإسلامية سياسات صارمة، حيث حظر استخدام العملات الرقمية في المراكز المالية والنقدية في البلاد. وفقًا لتعليمات البنك المركزي الصادرة بتاريخ ١٣٩٦/١٠/٠٩ هـ.ش، واستنادًا إلى إمكانية استخدام العملات الرقمية في غسل الأموال وتمويل الإرهاب، تم حظر أي استخدام لهذه العملات في الأنظمة المالية والنقدية داخل البلاد. وقد اتُخذ هذا الإجراء بهدف منع الاستغلالات المالية وضمان الأمن المالي الوطني، إلا أن هناك تحديات لا تزال قائمة فيما يتعلق بالتنفيذ الفعّال لهذه السياسات.[٤٤]في الإمارات العربية المتحدة، يمكن ملاحظة نهج يجمع بين الحظر المباشر، تحذير الجمهور، ومحاولة تنظيم العملات الرقمية. وفقًا للفقرة (٧.٣) من الإطار القانوني لنظم تخزين القيمة والدفع الإلكتروني، الذي أصدره البنك المركزي الإماراتي في ١ يناير ٢٠١٧، فقد تم الإعلان صراحة عن حظر جميع العملات الرقمية والمعاملات المرتبطة بها.يترافق هذا الحظر بشكل لافت مع التعريف الوارد في نفس الوثيقة (القسم A.١)، حيث لم يتم الاعتراف بالعملات الرقمية كوسيلة قانونية. ومع ذلك، فإن الوحدات الرقمية الوحيدة المسموح بها هي تلك التي يمكن استبدالها بالسلع، الخدمات، أو الخصومات في إطار برامج ولاء العملاء، ولكن بشرط ألا يتم تحويلها إلى عملة رقمية.[٤٥]على الرغم من القيود الصارمة المفروضة، فإن الفقرة (٤-ز) من القانون الاتحادي رقم ١٤ لسنة ٢٠١٨ في الإمارات العربية المتحدة تمنح البنك المركزي الصلاحية لوضع التنظيمات اللازمة لـ"النقد الرقمي". تنص هذه الفقرة على أن أحد أهداف البنك المركزي هو "تنظيم وتطوير البنية التحتية المالية، بما في ذلك أنظمة الدفع الإلكتروني والنقد الرقمي"، مما يفتح المجال أمام إمكانية قبول العملات الرقمية في المستقبل.بالإضافة إلى ذلك، فإن تصريحات رئيس البنك المركزي الإماراتي خلال اجتماع مجلس الخدمات المالية الإسلامية في أبوظبي تعكس تحولًا في الخطاب الرسمي نحو تحذير عام بشأن مخاطر العملات الرقمية. حيث أوضح أن اعتماد هذه العملات على العرض والطلب، إلى جانب المخاطر العالية وغياب الإشراف الحكومي، يسهل استخدامها ويمكن أن يؤدي إلى استغلالات غير قانونية. كما أُشير إلى أن الإطار القانوني الحالي لا ينطبق على عملات مثل البيتكوين، وأن البنك المركزي يواصل مراجعة هذا الموضوع لإصدار توجيهات خاصة عند

الضرورة. وقد تم التأكيد على أن الهدف الأساسي لهذا الإطار هو تسهيل اعتماد المدفوعات الرقمية في الإمارات العربية المتحدة.[٤٦]تعتمد سياسة الإمارات العربية المتحدة تجاه العملات الرقمية على مزيج من الحظر، التحذير، والاستعداد للتنظيم القانوني. فعلى الرغم من حظر استخدام العملات الرقمية كوسيلة نقدية، لا يزال إمكانية استخدامها كأصول رقمية متاحة. يعكس هذا النهج محاولة لموازنة المخاطر القانونية والاقتصادية المرتبطة بهذه التكنولوجيا، مع عدم إغفال الفرص المحتملة التي توفرها.[٤٧]على الرغم من فرض حظر شامل على جميع مقدمي خدمات الدفع الرقمية في الإمارات العربية المتحدة، إلا أن هذا التقييد لم يمنع الحكومات من الاستفادة من التكنولوجيا المالية التي تدعم العملات الرقمية. ومن الأمثلة البارزة على ذلك مشروع إنشاء عملة رقمية مشتركة بين الإمارات العربية المتحدة والمملكة العربية السعودية.تم تقديم هذا المشروع من قبل اللجنة التنفيذية لمجلس التنسيق السعودي–الإماراتي، ويهدف إلى إطلاق عملة رقمية موحدة تعتمد على تقنية البلوكشين لاستخدامها في النظام المصرفي لكلا البلدين. يعكس هذا الإجراء نهجًا مزدوجًا، حيث يتم فرض قيود تنظيمية صارمة، في الوقت الذي يتم فيه استغلال إمكانات التكنولوجيا الحديثة بشكل محدود وتحت إشراف دقيق.[٤٨]في سبتمبر ٢٠١٨، عُقد مؤتمر بعنوان "آفاق مستقبل العملات الرقمية وأبعادها الأمنية" في دبي. أوصى الخبراء الأمنيون والقانونيون والمصرفيون المشاركون في المؤتمر بأن تكون الإمارات العربية المتحدة رائدة في إصدار عملة رقمية وطنية قائمة على تقنية البلوكشين. وقد يتطلب هذا الإجراء تعديل القوانين المتعلقة بمكافحة غسل الأموال وتمويل الإرهاب للحد من الاستخدامات غير المشروعة لهذه العملات. كما شدد الخبراء على أن التعامل مع مخاطر العملات الرقمية يجب ألا يتم من خلال تجاهلها، بل عبر وضع أطر تنظيمية وضوابط شاملة لإدارتها ومراقبتها. [٤٩]مع دخول العالم في عصر الثورة الصناعية الرابعة، أصبح استخدام التقنيات الرقمية ونقل البيانات جزءًا لا يتجزأ من الأنشطة الاقتصادية. في هذا العصر، يُنظر إلى النقود المادية (الورقية والمعدنية) على أنها عبء مكلف بسبب تكاليف الطباعة، والنقل، والأمن. لذا، يمكن أن توفر العملات الرقمية بديلاً اقتصاديًا وعمليًا لمواجهة هذه التحديات.اعتمدت الإمارات العربية المتحدة نهجًا حذرًا ولكنه مستقبلي تجاه العملات الرقمية. وعلى الرغم من فرض قيود للحد من المخاطر الاقتصادية والقانونية لهذه التكنولوجيا، إلا أن المؤشرات تشير إلى أن الدولة تتجه نحو وضع أطر قانونية شاملة للاستفادة من المزايا الاقتصادية للعملات الرقمية. هذه الاستراتيجية قد تسهم في تعزيز مكانة الإمارات كمركز مالي رائد، وفي الوقت ذاته، تقليل المخاطر المرتبطة بالاستخدام غير القانوني لهذه التكنولوجيا.[٥٠]

## نتائج

١. الإمارات العربية المتحدة، من خلال اعتماد تدابير وقائية ووضع لوائح صارمة، تمكنت إلى حد كبير من منع وقوع الجرائم المرتبطة بالعملات الرقمية. إن إصدار قوانين مثل القانون الاتحادي رقم ١٤ لسنة ٢٠١٨ بشأن المصرف المركزي، والقانون الاتحادي رقم ٢٠ لسنة ٢٠١٨ لمكافحة غسل الأموال وتمويل الإرهاب، والتعديلات التي أُجريت على القانون الاتحادي رقم ٥ لسنة ٢٠١٢ بشأن الجرائم الإلكترونية، قد وفّر الإطار القانوني اللازم لمراقبة وتنظيم الأنشطة المتعلقة بالعملات الرقمية.

٢. إحدى أهم الاستراتيجيات التي تبنتها الإمارات في هذا المجال هي إلزام منصات تداول العملات الرقمية ومقدمي الخدمات المالية بالامتثال للوائح معرفة العميل (KYC) وتقديم تقارير عن المعاملات المشبوهة إلى وحدة المعلومات المالية (FIU). وقد ساهمت هذه الإجراءات في زيادة الشفافية في المعاملات المالية وتقليل فرص استغلال العملات الرقمية في غسل الأموال وتمويل الأنشطة غير القانونية.

٣. الإمارات العربية المتحدة، من خلال الاستفادة من التقنيات المتقدمة مثل البلوكشين الخاص والذكاء الاصطناعي، تمكنت من تتبع المعاملات المشبوهة بفعالية وتقليل الجرائم المرتبطة بها. كما أن تطوير أدوات تحليل البيانات الضخمة (Big Data) والتعاون الوثيق مع الهيئات الدولية مثل مجموعة العمل المالي (FATF) والإنتربول، لعب دورًا أساسيًا في تعزيز قدرة الدولة على التصدي للتهديدات العابرة للحدود.

٤. الإمارات العربية المتحدة، من خلال اعتماد سياسات صارمة ومراقبة دقيقة لسوق العملات الرقمية، نجحت في السيطرة على الجرائم المرتبطة بهذا المجال والحد منها. فقد أنشأت إطارًا رقابيًا متكاملًا من خلال إلزام منصات تداول العملات الرقمية بالامتثال للوائح معرفة العميل (KYC)، وتطبيق رقابة مستمرة، والتعاون مع الهيئات الدولية، مما ساهم في منع عمليات غسل الأموال والجرائم الإلكترونية. في المقابل، تبنت إيران نهجًا غير متسق، حيث انتقلت من حظر كامل للمعاملات الرقمية في السنوات الأولى، إلى تنظيم محدود لأنشطة تعدين العملات الرقمية. ومع ذلك، فإن عدم وجود إطار رقابي شامل وواضح لا يزال يؤدي إلى مخاطر اقتصادية وارتفاع المخالفات في هذا القطاع.

٥. الإمارات العربية المتحدة، من خلال الاستفادة من التقنيات الحديثة مثل البلوكشين والذكاء الاصطناعي، تعمل على تتبع المعاملات المشبوهة وتتمتع بتعاون وثيق مع هيئات دولية مثل مجموعة العمل المالي (FATF) والإنتربول. وقد جعلتها هذه السياسات إحدى الدول الرائدة في مكافحة غسل الأموال وتمويل الإرهاب باستخدام العملات الرقمية. في المقابل، تواجه إيران تحديات كبيرة بسبب القيود الدولية والعقوبات الاقتصادية، مما

قلل من قدرتها على إقامة شراكات دولية واسعة النطاق. وبدلًا من ذلك، تعتمد إيران على آليات داخلية، مثل البنك المركزي والشرطة الإلكترونية (فتا)، لمراقبة سوق العملات الرقمية. ومع ذلك، فإن عدم وضوح القوانين، والاستخدام المكثف للعملات الرقمية للالتفاف على العقوبات، يشكلان تحديًا رئيسيًا أمام تنفيذ سياسات رقابية فعالة.

٦. على الرغم من أن الإمارات العربية المتحدة تمكنت من خلق بيئة آمنة للاستثمار في مجال العملات الرقمية من خلال وضع قوانين شفافة وتعزيز المعايير التنظيمية، إلا أنها لا تزال تواجه تحديات مثل الحاجة إلى تنظيم أكثر دقة وإيجاد توازن بين الرقابة والابتكار الاقتصادي. إيران أيضًا، رغم توجهها نحو التشريعات التنظيمية، تواجه تحديات مثل نقص الشفافية في القوانين، وتداخل السياسات النقدية والاقتصادية، وزيادة المخالفات الناتجة عن الثغرات القانونية. يحتاج كلا البلدين إلى مراجعة مستمرة للقوانين وتكييفها مع المعايير الدولية لضمان الاستقرار المالي والاقتصادي، وفي الوقت ذاته الاستفادة من الإمكانات الإيجابية للعملات الرقمية في التنمية الاقتصادية.

## مصادر

### A) مصادر فارسی و عربی


١. عطاالله، إمام حسنين. جرائم تقنية المعلومات في التشريعات والصكوك العربية. ٢٠١٧.

٢. خسروی، عبدالحمید. «پولشویی و راهکارهای مبارزه با آن.» فصلنامه اقتصاد اسلامی، سال پنجم، زمستان ١٣٨٤، شماره ١٧.

٣. روشن، محمد و مظفری، مصطفی. «بررسی وضعیت فقهی و حقوقی بیت کوین.» نشریه تحقیقات حقوقی، شماره ٨٧، ١٣٩٧.

٤. بهره مند، حمید؛عامری ثانی، امیرکیا، «چالش ها و راهکارهای جرم یابی پولشویی از طریق ارزهای رمز نگاری شده»، مجله کارآگاه، شماره ٤٦، ١٣٩٨.

٥. فارابی، هیرو. «پول شویی نوین بر اساس سیستم مالی ارز دیجیتال.» ماهنامه اطلاع‌رسانی پژوهشی تحلیلی و فرهنگی، ١٣٩٤.

٦. نجفی ابرندآبادی، علی حسین. کیفرشناسی نو جرم‌شناسی نو، درآمدی بر سیاست جنایی خطرمدار. تهران: نشر میزان، ١٣٨٨.

٧. نوری، خادمان، و کوشا. بررسی وضعیت ارزهای دیجیتال در نظام حقوقی ایران. ١٤٠٠.

٨. نوری، نوابپور. حقوق کیفری و چالش‌های نوین در جرایم سایبری. ١٣٩٧.

٩. عمر عبید المرر. النظام القانوني للعملات الرقمية الافتراضية (دراسة تحليلية). پایان‌نامه، دانشگاه ابوظبی، ٢٠٢١.

١٠. آلاء يوسف، و السيد خليفة الحمادي. «التكييف القانوني للعملات الافتراضية–البتكوين نموذجاً (دراسة مقارنة).» مجلة جامعة الشارقة للعلوم القانونية، ١٩.٣ (٢٠٢٢).


### b) English sources


11. Al-Tawil, Tareq Na’el. "Anti-money laundering regulation of cryptocurrency: UAE and global approaches." Journal of Money Laundering Control, 26.6.(٢٠٢٣)

12. Al-Hajj, Muhammad Al-Hajj. "Regulating Virtual Currency in the Context of Sustainable Development and Economic Transformation-The United Arab Emirates as a Model." I-iECONS e-proceedings (2003)

13. Atiyah, Ghassan Adhab, Nazura Abdul Manap, and Saidatul Nadia Abd Aziz. "Legal Status of Cryptocurrency Circulation in Iraq: Lessons from the United Arab Emirates and the United States." Hasanuddin Law Review, 9.1.(٢٠٢٣)

14. AUSTRALIAN TRANSACTION REPORTS & ANALYSIS CTR. Typologies and Case Studies Report 2012 [AUSTRAC REPORT].

15. Bohme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. "Bitcoin: Economics, Technology, and Governance." Journal of Economic Perspectives, Volume 29, Number 2, Spring 2015.

16. Hardl, Harvey, & Reule. "The Role of Stable Coins in the Digital Economy." Spring 2020.

17. Huang, D. Y. "Profit-driven abuses of virtual currencies." University of California, San Diego.(٢٠١٣)

18. King, C., Walker, C., & Gurulé, J. (Eds.). The Palgrave Handbook of Criminal and Terrorism Financing Law. Palgrave Macmillan, 2018.

19. Kethineni, S., & Cao, Y. "The rise in popularity of cryptocurrency and associated criminal activity." International Criminal Justice Review, 2019.

20. MANISZEWSKA, K., & PIASECKA, P. "Security and Society." Vol 2, 30.01.2020.

21. Oxford Analytica. "Crypto will gain strength in the United Arab Emirates." Emerald Expert Briefings, 2024.

22. El Maknouzi, Mohammed El Hadi, and Hicham Sadok. "Regulation of Virtual Currencies in the United Arab Emirates: Accounting for the Emerging Public/Private Distinction." Development Studies Research, 8.1 .(٢٠٢١)
23. Ramasastry, A. "Bitcoin: If You Can't Ban It, Should You Regulate It? The Merits of Legalization." 2014, http://verdict.justia.com/2014/02/25/bitcoin--cant--ban- -regulate.
24. Westhuizen, Ch. Van Der. "Future Digital Money: The Legal Status and Regulation of Bitcoin in Australia." Theses, The University of Notre Dame Australia, 2017, https://researchonline.nd.edu.au/cgi/viewcontent.cgi?article=1166&context=theses.
c) Internet resources
25. https://www.int-comp.org/careers/your-career-in-financial-crime-prevention/what-is-financial-crime
26. https://www.scribd.com/document/336728717/Regulatory-Framework-for-StoredValues-and-Electronic-Payment-Systems-En
27. https://arabic.arabianbusiness.com/content/321738
28. https://www.jdsupra.com/legalnews/the-legal-status-of-bitcoin-in-the-82718/
29. http://alwatan.kuwait.tt/articledetails.aspx?id=581519&yearquarter=20191
30. https://www.emaratalyoum.com/local-section/accidents/2018-09-17-1.1135272

د) القوانين:

٣١.القانون اتحادي رقم ١٤ لسنة ٢٠١٨، المعدل بالقانون الاتحادي رقم ٢٥ لسنة ٢٠٢٠،

٣٢.القانون الاتحادي رقم ٢ لسنة ٢٠٢١.

٣٣.القانون اتحادي رقم ١٤ لسنة ٢٠١٨.

٣٤.دستورالعمل بانک مرکزی ایران مورخ ١٣٩٦/١٠/٠٩.

٣٥.آیین نامه استخراج رمز دارایی ها ایران مصوب ١٤٠١.

## هوامش البحث

[1] روشن، محمد و مظفری، مصطفی، بررسی وضعیت فقهی و حقوقی بیت کوین، نشریه تحقیقات حقوقی، شماره ٨٧، ١٣٩٧، ص١٩.

[2] عطا اللة، إمام حسنين. "جرائم تقنية المعلومات في التشريعات والصكوك العربية ".(٢٠١٧). ص١٨.

[3] همان، ص١٩.

[4] نوری و نوابپور, ١٣٩٧, ص٤

[5] Coin

[6] Bitcoin

[7] Litecoin

[8] Ethereum

[9] نوری, خادمان, و کوشا, ١٤٠٠, ص٣٥٢-٣٥٤

[10] Token

[11] نوری, خادمان, و کوشا, ١٤٠٠, ص٣٥٤-٣٥٢

[12] نوری, خادمان, & کوشا, ١٤٠٠, ص٣٥٤-٣٥٢

[13] Stable Coin

[14] Hardl, Harvey, & Reule, Spring 2020, pp. 9-10

[15] فارابی،هیرو «پول شویی نوین بر اساس سیستم مالی ارز دیجیتال». ماهنامه اطلاع رسانی پژوهشی تحلیلی و فرهنگی، ١٣٩٤، ص ٤٦.

[16] **پول فیات** :به پولی که هیچ گونه ارزش ذاتی ندارد، پول بدون پشتوانه و یا پول فیات می گویند، چرا که به فرمان دولت ایجاد شده و اگر مردم آن را برای مبادله قبول نکنند، دیگر ارزش نخواهد داشت. پول رایج بسیاری از کشورها مثل دلار ایالات متحده از همین گونه است (رضائی صدرآبادی1399, ,ص٦)

[17] Bitcoin: Economics, Technology, and Govermance Rainer Bohme, Nicolas Christin, Benjamin Edelman, and Tyler Moore Journal of Economic Perspectives-Volume 29, Number 2-Spring 2015-P 213-238

[18] Huang, D. Y. (2013). Profit-driven abuses of virtual currencies. University of California, San Diego, 14p17

[١٩] خسروی، عبدالحمید،«پولشویی و راهکارهای مبارزه با آن.» فصلنامه اقتصاد اسلامی، سال پنجم، زمستان ،١٣٨٤شماره .١٧ص.١٤

[٢٠] روشن، محمد و مظفری، مصطفی، بررسی وضعیت فقهی و حقوقی بیت کوین، نشریه تحقیقات حقوقی، شماره ٨٧، ١٣٩٧، ص٨

[٢١] فارابی،هیرو «پول شویی نوین بر اساس سیستم مالی ارز دیجیتال». ماهنامه اطلاع رسانی پژوهشی تحلیلی و فرهنگی، ،١٣٩٤ص .٤٦

[٢٢] ٢١. نجفی ابرندآبادی، علی حسین، کیفرشناسی نو جرم‌شناسی نو، درآمدری بر سیاست جنایی خطرمدار، تهران، نشر میزان، ١٣٨٨، ص٨١.

[23] King, C., Walker, C., & Gurulé, J. (Eds.). (2018). The Palgrave handbook of criminal and terrorism financing law. Palgrave Macmillan., 183-195

[24] Kethineni, S., & Cao, Y. (2019). The rise in popularity of cryptocurrency and associated criminal activity. International Criminal Justice Review, 1057567719827051. P 5-6

MANISZEWSKA, K., & PIASECKA, P. SECUR TY AND SOCIETY.vol 2,30.01.2020 p 137-138.

[25] AUSTRALIAN TRANSACTION REPORTS & ANALYSIS CTR., TYPOLOGIES AND CASE STUDIES REPORT 2012, at 19 (2012) [hereinafter AUSTRAC REPORT]. https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/typologies-and-case-studies-report-2012 #Case19

[26] King, C., Walker, C., & Gurulé, J. (Eds.). (2018). The Palgrave handbook of criminal and terrorism financing law. Palgrave Macmillan.,p 204- 211.

[27] نصت المادة الرابعة من المرسوم بقانون اتحادي رقم ( )١٤لسنة ٢٠١٨م في شأن المصرف المركزي وتنظيم المنشآت والأنشطة المالية المعدل بالمرسوم بقانون اتحادي رقم ( )٢٥لسنة ٢٠٢٠م والمعدل بالقانون الاتحادي رقم ( )٢لسنة ٢٠٢١م على أنه: "يتولى المصرف المركزي ممارسة المهام والاختصاصات الآتية: أ-وضع وتنفيذ السياسة النقدية، مع الأخذ بالاعتبار الاستراتيجية العامة للدولة."

[٢٨] المادة ٥٥، المرسوم بقانون اتحادى رقم ١٤ لسنة ٢٠١٨

[٢٩] (شوراي عالی مبارزه با پولشویی, ١٣٩٦)

[٣٠] شاهچرا، مهشید، طاهری، ماندانا و فرجی، مرجان؛ چهارچوب مقررات گذاری رمز ارزها در ایران: بررسی رویکردهای بین المللی و ارائه پیشنهاد، گزارش کارشناسی، پژوهشکده پولی و بانکی (وابسته به بانک مرکزی جمهوری اسلامی ایران،) ،١٤٠٠، ص ٣٨.

[31] نصت المادة ( )١٤٠من المرسوم بقانون اتحادي رقم ( )١٤لسنة ٢٠١٨م في شأن المصرف المركزي وتنظيم المنشآت والأنشطة المالية سالف الذكر على أن": يعاقب بالسجن كل من يقوم بإصدار النقد بالمخالفة لأحكام هذا المرسوم بقانون مدة لا تزيد عن عشرين ( )٢٠سنة وبغرامة لا تجاوز مائة مليون ( )١٠٠,٠٠٠,٠٠٠درهم، أو بإحدى هاتين العقوبتين"

[٣٢] المادة ٥٥، نفس القانون

[33] نصت المادة ( )٦٢من القانون ذاته على أن: " على المصرف المركزي أن يحتفظ في جميع الأوقات باحتياطيات من الأصول الأجنبية، لتغطية القاعدة النقدية، وفقًا لأحكام المادة ( )٦٣من هذا المرسوم بقانون، مكونة من واحدة أو أكثر من الأدوات الآتية": 1- "سبائك ذهبية ومعادن ثمينة أخرى". " -٢أموال وودائع نقدية وغيرها من الأدوات النقدية وأدوات الدفع المقومة بعملات أجنبية وقابلة للتحويل بحرية في الأسواق المالية العالمية." " -٣أوراق مالية مقومة بعملات أجنبية، وصادرة أو مضمونة من قبل حكومات أجنبية، ومن قبل الشركات والكيانات والمؤسسات والهيئات التابعة لها، أو من المؤسسات النقدية والمالية للدولية، أو من الشركات متعددة الجنسيات، وتكون قابلة للتداول في الأسواق المالية العالمية."

[34] King, C., Walker, C., & Gurulé, J. (Eds.). (2018). The Palgrave handbook of criminal and terrorism financing law. Palgrave Macmillan., p185.

[35] Cherniei, Volodymyr, et al. "Criminal liability for cryptocurrency transactions: Global experience." European Journal of Sustainable Development 10.4 (2021):p 304

[36] عمر عبيد المرر. النظام القانوني للعملات الرقمية الافتراضية (دراسة تحليلية).Diss. ABU DHABI UNIVERSITY, 2021 .، ص ١٩.

[٣٧] آلاء يوسف,السيد خليفة الحمادي. "التكييف القانوني للعملات الافتراضية-البتكوين نموذجاً (دراسة مقارنة)." مجلة جامعة الشارقة للعلوم القانونية ١٩.٣ (٢٠٢٢): ص ٤١.

[38] Al-Tawil, Tareq Na'el. "Anti-money laundering regulation of cryptocurrency: UAE and global approaches." Journal of Money Laundering Control 26.6 (2023): p12.

[39] El Maknouzi, Mohammed El Hadi, and Hicham Sadok. "Regulation of virtual currencies in the United Arab Emirates: accounting for the emerging public/private distinction." Development Studies Research 8.1 (2021): p10.

[40] Al, Al-Hajj Muhammad Al-Hajj. " تقنين العملة الافتراضية في ظل التنمية المستدامة و التحول الاقتصادي-دولة الإمارات العربية المتحدة أنموذجاً: REGULATING VIRTUAL CURRENCY IN THE CONTEXT OF SUSTAINABLE DEVELOPMENT AND ECONOMIC TRANSFORMATION-THE UNITED ARAB EMIRATES AS A MODEL." I-iECONS e-proceedings (2023): p19.

[41] Oxford Analytica. "Crypto will gain strength in the United Arab Emirates." Emerald Expert Briefings oxan-db (2024). p16

[42] Atiyah, Ghassan Adhab, Nazura Abdul Manap, and Saidatul Nadia Abd Aziz. "Legal Status of Cryptocurrency Circulation in Iraq: Lessons from the United Arab Emirates and the United States." Hasanuddin Law Review 9.1 (2023): p9.

[٤٣] أنظر في ذات الاتجاه

A. Ramasastry, "*Bitcoin: If you Can't Ban It, Should you Regulate it? The Merits of Legalization*", 2014, http://verdict.justia.com/2014/02/25/bitcoin--cant--ban- -regulate, 11/1/2019.

[٤٤] بهره مند، حمید؛عامری ثانی، امیرکیا، «چالش ها و راهکارهای جرم یابی پولشویی از طریق ارزهای رمز نگاری شده»، مجله کارآگاه، شماره ٤٦، ١٣٩٨، ص٣.

[45] https://www.scribd.com/document/336728717/Regulatory-Framework-for-StoredValues-and-Electronic-Payment-Systems-En, 11/1/2019.

[46] https://arabic.arabianbusiness.com/content/321738, 15/1/2019.

[47] https://www.jdsupra.com/legalnews/the-legal-status-of-bitcoin-in-the-82718/, 15/1/2019.

[48] http://alwatan.kuwait.tt/articledetails.aspx?id=581519&yearquarter=20191

[49] https://www.emaratalyoum.com/local-section/accidents/2018-09-17-1.1135272

[50] Ch. Van Der Westhuizen, "Future digital money: The legal status and regulation *of bitcoin in Australia*", Theses, The University of Notre Dame Australia, 2017, https://researchonline.nd.edu.au/cgi/viewcontent.cgi?article=1166&context=theses, 20/1/2019, p. 92.