الإحتيال المالي السيبيراني بإستخدام الأصول المشفرة

Cyber financial fraud using crypto assets

د. مناصرة يوسف[1]،

menasra@hotmail.com

تاريخ الإرسال: 2023/10/19 تاريخ القبول: 2024/01/17 تاريخ النشر: 2024/01/24

ملخص:

تمثل الأصول المشفرة مثل البيتكوين والإيثيريوم تكنولوجيا مبتكرة واعدةً بتحويل النظام المالي التقليدي، ومع ذلك فإن هذا التحول يأتي مع تحديات متزايدة من جراء الاحتيال المالي السيبيراني مثل عمليات التعدين الخفي و جمع التمويل عبر عروض العملات الأولية *ICO* ، وعمليات الاحتيال بين المستخدمين على منصات تداول العملات المشفرة، وتزوير المحافظ الرقمية لسرقة الأصول..الخ، يشكل هذا النوع من الاحتيال تهديدًا خطيرًا للاستثمارات والأمان المالي، ويتطلب استراتيجيات وتدابير لمكافحته. في هذا المقال، سنلقي نظرة على مفهوم الاحتيال المالي السيبيراني باستخدام الأصول المشفرة، ونتناول الأساليب الرئيسية المستخدمة في هذا النوع من الاحتيال، ونقدم بعض الحلول المحتملة.

كلمات مفتاحية:إحتيال سيبيراني،الأصول مشفرة، العملة الرقمية، التعدين الخفي، عروض العملات الأولية.

Abstract:

Cryptoassets such as Bitcoin and Ethereum represent an innovative technology that promises to transform the traditional financial system. However, this transformation comes with increasing challenges from financial cyber fraud such as cryptojacking, initial coin offering ICO fundraising, and fraud among users on trading platforms. Cryptocurrencies, counterfeiting digital wallets to steal assets..etc. This

type of fraud poses a serious threat to investments and financial security, and requires strategies and measures to combat it. In this article, we will take a look at the concept of financial cyber fraud using crypto assets, go over the main methods used in this type of fraud, and present some potential solutions.

Keywords: *Cyber fraud; crypto assets; digital currency; cryptojacking; initial coin offerings.*

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

مقدمة :

يوفر الإنترنت إمكانيات متعددة للمجرمين للوصول إلى عدد كبير من الضحايا المحتملين و ذلك بتكلفة منخفضة للغاية وبمزايا عديدة تساهم في تسهيل إرتكابها كبعد المسافة بين مقترفي الجرائم السيبيرانية و الضحايا و مرونة التبادلات الميسرة والمشفرة و إخفاء الهوية و طبيعة العالم الإفتراضي الذي يسهل إختراق الحدود و تجاوز الأقاليم الجغرافية للبلدان و صعوبة تقفي الآثار الرقمية و سهولة طمس الأدلة الجزائية مصحوبة بإخفاء وجهة الأموال المتحصل عليها بزيادة الاحتمالات المتعددة لتبييض الأموال من أنشطتهم غير المشروعة. و بالتالي بوسائل تقنية حديثة و بسيطة يُمكن إحداث مخاطر كبيرة للغاية قد تصل إلى مئات الملايين أو حتى مليارات اليورو من القيمة السوقية المفقودة مؤقتًا. لذا فإن استخدام الشبكات الرقمية يسهل الاستغلال المتزايد للمخططات الاحتيالية الكلاسيكية و يؤدي إلى ظهور أنماط عمل إجرامية جديدة تمتد إلى قطاع المالية و الإقتصاد.

حالياً، إمتدت دلالة "سيبرانية" إلى الجريمة الاقتصادية والمالية مثل جميع الأنشطة غير المشروعة مع تطور الإنترنت والشبكات الرقمية. وفي الواقع،

يؤدي النمو السريع للاتصال العالمي إلى ارتفاع جرائم الكمبيوتر التي تشكل واحدة من بين أخطر الجرائم العابرة للحدود، وبالتالي تستخدم الممارسات الاحتيالية الآن الموارد الرقمية على نطاق واسع.

و تكمن **أهمية الموضوع** في دراسة الجرائم السيبرانية الجديدة المنبثقة من التطورات الرقمية الحديثة في التأثير البارز لتكنولوجيا المعلومات والاتصالات على مجالات متعددة في المجتمع، إذ تساعد في توسيع فهمنا للتهديدات الجديدة التي تنشأ نتيجة للتكنولوجيا الحديثة، مما يمكن الجهات الأمنية والمجتمع بشكل عام من الاستعداد للتحديات المستقبلية، كما تمكن هذه الدراسة من لفت الإنتباه من أجل تطوير استراتيجيات الأمان والحماية السيبرانية لمواجهة الجرائم الرقمية المتقدمة والمتطورة التي تعزوها بلادنا و تتوجب علينا لضمان الأمن القانوني تحسين التشريعات والسياسات لتكون أكثر فعالية في مجال مكافحة الجريمة السيبرانية. و تساعد هذه الدراسة على مواكبة التطورات التكنولوجية وفهم كيف يمكن استغلالها في أغراض غير أخلاقية أو غير قانونية على الصعيدين الوطني و الدولي و تعزز التفاهم الدولي حول التحديات السيبرانية والتعاون بين الدول في مجال مكافحة الجرائم الرقمية. بشكل عام، يمكن القول إن فهم ودراسة الجرائم السيبرانية المستجدة تسهم في تكوين استراتيجيات فعّالة لمواجهة التحديات الأمانية الحديثة وضمان استفادة إيجابية من التقنيات الرقمية.

أما **الأهداف المتوخاة** من هذا البحث، فتتمثل في:

- تحديد وفهم التهديدات السيبرانية المالية الجديدة التي تظهر نتيجة للتطورات التكنولوجية، وتحليل طبيعتها وأساليبها.
- تقديم الأساس التشريعي و التنظيمي و الفني لتطوير سياسات وإجراءات الأمان السيبراني لمواجهة التحديات المستجدة والتغيرات في طبيعة الجرائم الرقمية.

- تقديم الأمثلة المقارنة والمعلومات الضرورية لتحسين التشريعات ذات الصلة بالجرائم السيبرانية، مما يمكن من معاقبة المرتكبين وتحسين الردع القانوني.
- تشجيع على التعاون الدولي في مجال مكافحة الجرائم السيبرانية، وتسليط الضوء على الضرورة الملحة للتعاون بين الدول في هذا السياق.
- توجيه جهود توعية نحو الجمهور لزيادة الوعي حول مخاطر الأمان السيبراني والوقاية منها.

في المجمل، تسعى دراسة الإحتيال المالي السيبيراني باستخدام الأصول المشفرة إلى تطوير الفهم والاستعداد للتحديات الأمنية الحديثة التي تنشأ من تقدم التكنولوجيا الرقمية.

وسنحاول الإجابة على **الإشكالية** الرئيسية حول التحديات الأخلاقية والقانونية المرتبطة بالاستخدام السيء للتكنولوجيا، بالبحث إذا ماكانت التشريعات القانونية والسياسات الجزائية كافية أم غير مُحدثة و مُطَورة لمعالجة الجرائم السيبرانية الجديدة و هل يتطلب ذلك التدخل التشريعي لإصلاحها وتطويرها؟.

سوف يتم الإجابة على الإشكالية المطروخة للنقاش تبعا **لمنهجية** وصفية تحليلة تتناول محورين رئيسين، حيث يتناول المحور الأول مسألة الاحتيال السيبراني المرتبط بالأصول المشفرة، ينما المحور الثاني يُسلط الضوء على أسلوبين للإحتيال السيبيراني جد متفاقمين ألا و هما التعدين الخفي و عروض العملات الأولية.

1. الاحتيال السيبراني المرتبط بالأصول المشفرة

في ظل الارتفاع المستمر للتبادل الرقمي واستخدام العملات المشفرة، أصبحت جرائم الاحتيال السيبراني المرتبطة بالأصول المشفرة تحديًا متناميًا. يشمل الاحتيال و النصب المستمر استخدام التكنولوجيا لأغراض غير قانونية، مثل إطلاق عروض الاستثمار الزائفة وجمع الأموال بشكل غير قانوني من

خلال ICOs المزيفة و يتسم الاحتيال أيضًا بتقنيات متقدمة مثل اختراق المحافظ الرقمية والتلاعب في أسعار العملات بشكل صناعي.

التحدي الرئيسي يكمن في استغلال الثغرات الأمنية بالأنظمة المعلوماتية للوصول إلى المحافظ والمعطيات الشخصية، مما يؤدي إلى خسائر مالية جسيمة للمستثمرين، إلى جانب ذلك يستخدم المحتالون تقنيات الهندسة الاجتماعية ووسائل التواصل الاجتماعي لتضليل الضحايا وجعلهم يسقطون في فخ الاحتيال[1]. يبرز هذا الوضع أهمية تعزيز الوعي الرقمي وتحسين أمان البنية التحتية لتكنولوجيا العملات المشفرة لضمان استدامة وثقة المستخدمين في هذا النظام المالي الرقمي المتطور.

1.1. الأصول المشفرة Cryptoactivities:

تتطور الجريمة المرتبطة بالأصول المشفرة في شكل تعدين العملات المشفرة[2] (التعدين السري) ، والهجمات على منصات التبادل، وجمع الأموال من الطرح الأولي للعملات[3] ICO، واستخدام Bitcards، وعمليات الاحتيال الهرمية القائمة على الأصول المشفرة وهي تتجه إلى الأصول المشفرة بمعاملات معقدة مبنية على تورية الهوية بشكل كبير، وقد تميزت هذه الظاهرة باستمرار عمليات الاحتيال الاستثمارية المزيفة في سوق الصرف الأجنبي FOREX[4] وعودة عمليات الاحتيال المرتبطة بالاستثمارات المرتبطة بالعملات المشفرة ، كما يتوسع استخدام الأصول المشفرة لأغراض تبييض الأموال لإخفاء عائدات الاحتيال و الاحتيال عبر برامج الفدية Rançongiciels ، أو قضايا الاتجار بالمخدرات وتعتمد هذه العمليات الإحتيالية أساساًعلى إخفاء الهوية التي تميزها.

تعتمد هذه الوسائل المالية الجديدة على تقنية البلوكشين التي تثير مخاوف تتعلق بسمعتها ك"عملات إجرامية" بسبب عمليات تبييض الأموال التي يمكن أن تشجعها نظرا لإفتقارها لمعيار الإئتمان و الثقة البنكية، و هو الأمر الذي أدى

بالمشرع الجزائري لحظر التعاملات بالعملة الافتراضية في قانون المالية لعام 2018، طبقا للمادة 117 منه التي تنص "*يُمنع شراء العملة الافتراضية وبيعها وحيازتها*". وأضافت ي الفقرة الثانية "*العملة الإفتراضية هي تلك التي يستعملها مستخدمو الانترنيت عبر الشبكة العنكبوتية، وهي تتميز بغياب الدعامة المادية كالقطع والأوراق النقدية، وعمليات الدفع بالصك أو بالبطاقة البنكية*" و ينجر عن كل مخالفة لهذا الحكم بالعقاب طبقا للقوانين والتنظيمات المعمول بها. لكن الملاحظ في التشريعات و التنظيمات اللاحقة، أن المشرع الجزائري لم يبين طبيعة العقاب بشكل واضح لا لبس فيه مما يجعلنا بالضرورة نلجأ للقواعد الكلاسيكية في التجريم و المتابعة الجزائية بجريمة النصب (الإحتيال) طبقا لنص المادة 372 من قانون العقوبات، و حتى القانون النقدي و المصرفي رقم 23-09 المؤرخ في 12 جوان 2023 لم يتطرق للعملات الإلكترونية بشكل واضح و اكتفى في المادة 59 بالحديث عن وسائل الدفع غيرالعملة الائتمانية، و لم يُبين ماهية العملات الالكترونية في المادة 74 التي عدَت العملة الإلكترونية وسيلة من وسائل الدفع على شاكلة الدينار الرقمي.

بيد أن المشرع الجزائري تماشيا مع الالتزامات الدولية ذات الصلة بتبييض الأموال، سُرعان ما أقر عام 2012 [5] تعديل نظام الوقاية و مكافحة تبييض الأموال بتوسيع مفهوم الأموال لتشمل الممتلكات من أي طبيعة كانت،بما فيها القيم المالية الافتراضية ، أوغيرالمادية، أوغيرالملموسة التي يحصل عليها بأي وسيلة كانت وكذا السندات القانونية أيا كان شكلها، بما في ذلك وبصورة غيرحصرية،الشكل الإلكتروني أوالرقمي، والتي تدل على ملكية تلك الأموال أوالممتلكات أومصلحة فيها. و تفطن عام 2023 لما أضاف الأصول الافتراضية باعتبارها قيم رقمية التي يمكن تداولها رقمًيا أو تحويلها و يثمكن أن تستخدم لأغراض الدفع أو الاستثمار[6]. بشكل عام، الأصول المشفرة هي عبارة عن وسائل رقمية للتبادل تستند إلى تقنية البلوكشين Blockchain ، وهي تشمل العديد من العملات الرقمية المختلفة والتي يمكن تداولها عبر

الإنترنت، مثل البيتكوين Bitcoin وهي العملة الرقمية الأولى والأشهر في هذا المجال، ومن ثم تبعتها عدة عملات أخرى كالإيثيريوم ETH ،بيل XRP ،ليتكوين LTC ، بيتكوين كاش BCH ،كاردانو ADA ، ولكادوت DOT ، ستيلار XLM ، تيذر USDT و كريبتو كرينسي CRO وهناك العديد من العملات المشفرة الأخرى بالمئات، ويتم إطلاق عملات جديدة بشكل منتظم من خلال ما يعرف بـ Initial Coin Offerings(ICO) أو تقنية DeFi التمويل اللامركزي ، ما يهمنا التنويه إلى أن قيمة العملات المشفرة قد تتغير بشكل كبير وقد تكون متقلبة.

على غرار كثير من الدول، وضع التعديل التشريعي لقانون الوقاية من تبييض الأموال و تمويل الإرهاب مسايرة لتوجيهات مجموعة العمل المالي FATF نظامًا معياريًا كاملاً لإخضاع المهنيين في قطاع البنوك و المؤسسات المالية و المصرفية و الملزمين بالإخطار بالشبهه لالتزامات التبليغ تسهر على حسن تنفيذها عدة هيئات و مؤسسات عمومية ذات الصلة كلجنة الاستعلام المالي و المصرفي CTRF و الهيئة الوطنية للوقاية من الفساد و مكافحته و بنك الجزائر .

ويُراد بالأصول الرقمية مجموع الوحدات الإلكترونية ذات القيمة المخزنة على سلسلة كتل[7] "Blockchain" وهي مرتبطة بالمفاتيح الخاصة لمالكها، ويتم تبادلها عبر المفاتيح العامة[8]. يُمكن لصاحب المفتاح الخاص لإدارة محفظته وتنفيذ المعاملات استخدام برنامج مخصص مثبت على جهاز الكمبيوتر الخاص به مباشرة، أو الاتصال بمقدمي خدمة المحفظة و توفر هذه الخدمات حفظ مفاتيح التشفير الخاصة نيابة عن عملائها لأغراض الاحتفاظ بالأصول الرقمية وتخزينها ونقلها، إضافة لذلك يُمكن أيضًا استخدام الأصول الرقمية كجزء من إجراءات جمع الأموال التي يتم تنفيذها مباشرة على الإنترنت(*الطرح الأولي للعملة* أو ICO) [9] بما يتوافق مع السوق الأولية للأصول الرقمية .

يمكن تحويل الأصول الرقمية إلى عملة قانونية عبر منصات التبادل، مع حالات نادرة لمحطات السحب المادية Bornes de retrait physiques .

و تُعرف الأصول المشفرة على أنها "أصول افتراضية مخزنة على وسيط إلكتروني يسمح لمجموعة من المستخدمين بقبولها كدفعة لتنفيذ المعاملات دون الحاجة إلى اللجوء إلى عملة قانونية ."يغطي مفهوم الأصول المشفرة جميع الممتلكات الرقمية االامادية ومشتقاتها باستخدام تقنيات التشفير للتحقق من صحة المعاملات دون وساطة طرف ثالث موثوق به وتسجيل هذه العمليات في سجل موزع .على هذا النحو ، فإن الممتلكات التي تسمى بشكل غير صحيح عملات مشفرة مثل بيتكوين أو مونيرو ومنتجاتها المشتقة تشكل أصولًا مشفرة[10].

ويزداد هذا النوع من الجرائم المالية السيبرانية في العالم الافتراضي نتيجة إعتمادها على إخفاء الهوية التي بدأت تأخذ مسار كرة الثلج، و نتيجة القيمة الباهضة للبيتكوين و ماشابهه نجم عنه ظهور أساليب إجرامية جديدة، مثل التعدين الخفي Cryptojacking ، وتفاقم عمليات الاحتيال الهرمية القائمة على الأصول المشفرة.

لكن الواقع الذي يثبت إنتشار هذه الجرائم المالية السيبرانية الجديدة في العالم، لا يعني غياب المتابعات الجزائية في بلدنا خلوها منها، بل نكون أمام إحدى الإفتراضين إما أن الجرائم ترتكب و لاتكتشف أو أن النظام القانوني الوطني المطبق على الأصول المشفرة لم ينضج بعد بالرغم من التنصيص عليه في قانون الوقاية من تبيض الأموال و تمويل الإرهاب. بينما بفرنسا التكييف القانوني للأصول المشفرة يتم بموجب القانون رقم 486-2019 المؤرخ 22 مايو 2019 المتعلق بنمو وتحويل المؤسسات المعروف باسم قانون "الميثاق"و بموجب أحكام المادة L. 54-10-1 من قانون النقد والمالية[11].

كما تم عام 2014 تسليط الضوء على مخاطر الجرائم المالية المرتبطة بالأصول المشفرة من قبل مجموعة العمل المالي FATF، أين بينت بأنه يمكن لوسطاء العملات المشفرة الذين يوافقون على تبادل هذه الأصول، في معاملة

وجهًا لوجه، مقابل النقود الورقية، أن يلعبوا دورًا مهمًا في عمليات تبييض الأموال و إعتبرت منظمة التعاون الاقتصادي والتنمية،عام 2019 بأن الأصول المشفرة هي أصول افتراضية غالبًا ما تكون أقل تنظيمًا وأقل وضوحًا للسلطات من العملات الورقية يمكن أن تعزز إخفاء هوية المعاملات وإخفاء التدفقات المالية، وهذا ما يجعلها أدوات جذابة للمتهربين من الضرائب وغيرهم من المجرمين.

إن إخفاء هوية المعاملات وإخفاء التدفقات المالية والتنظيم الأقل صرامة للعملات المشفرة يجعل من هذه الأصول الافتراضية أداة مفضلة للمجرمين والمحتالين من خلال الموافقة على تبادل الأصول مقابل النقد في معاملة وجاهية.

ومن بين الطرق الإحتيالية المعروفة في هذا المجال، إما عن طريق إنشاء مواقع مزيفة تعرض شراء الأصول المشفرة بعروض فوائد جذابة للغاية و إما أن يكون الموقع جزءًا من عملية احتيال خالصة ويعرض الاستثمار في الأصول المشفرة الموجودة دون إعادة قيمة الاستثمارات إلى الضحايا على الإطلاق أو أن تكون عملية الاحتيال جزءًا من مخطط بونزي[12] وتعتمد على أصول مشفرة وهمية ومكافآت تعمل على أساس هرمي .هذه المواقع هي موضوع استنكار من قبل منظمات حماية الاستثمار و المستهلكين وهي مدرجة في القائمة السوداء إلى جانب مواقع تداول الخيارات الثنائية sites de trading aux options binaires التي تعتبر شكلاً من أشكال التداول المضاربي وينطوي على مخاطر عالية.

وجدير بالتنويه أن الأصول المشفرة هي وسيلة الدفع المفضلة لمشغلي الشبكة المظلمة Darknet لأنها تسمح لهم باستغلال وظائف إخفاء الهوية القوية وتسهيل المعاملات التي تتجاوز ضمانات النظام المالي التقليدي المنظم، بحيث يمكن لمشغلي منصات السوق السوداء على الإنترنت المظلم أن يعملوا كوسطاء ضرائب لتسهيل هذا التهرب الضريبي، وتمويل الأنشطة غير القانونية[13] .

على الصعيد العالمي، نجد الولايات المتحدة الأمريكية تنظم الأصول المشفرة من خلال عدة وكالات ولوائح في السياق المالي والقانوني، من أهمها هيئة الأوراق المالية والبورصات SEC التي تلعب دورًا هامًا في تنظيم الأصول المشفرة فيما يتعلق بعروض الأمان Security Tokens ومشاريع العملات الرقمية الأولية ICOs التي تعتبر أمانًا إذ يجب على المشاريع الامتثال لقوانين القيم الورقية، وهيئة الأمور المالية FinCEN التي تتعامل مع قضايا مكافحة تبييض الأموال ومكافحة تمويل الإرهاب أين تلتزم المؤسسات المالية وشركات تبادل العملات المشفرة بمتطلبات تقديم التقارير ومكافحة غسل الأموال و توجد هيئة تداول العقود الآجلة والسلع CFTC التي تعتبر الأصول المشفرة عقود آجلة و يجب على الشركات التي تقدم هذه الخدمات الامتثال للقوانين والتقديم للتراخيص، فضلا عن مهام البنك المركزي الأمريكي Federal Reserve والمصارف المحلية التي تخضع الشركات التي تتعامل بالأصول المشفرة لرقابة شديدة تخوفا من تبييض الأموال. أما على صعيد قوانين الولايات فتختلف من ولاية لأخرى، البعض منها وضعت قوانين خاصة مثل ولاية نيويورك التي تتمتع بنظام تنظيمي صارم لمشغلي العملات المشفرة ومنحت BitLicense، وهي ترخيص خاص لشركات العملات المشفرة وولاية كاليفورنيا تعتبر واحدة من الولايات الرائدة في مجال التكنولوجيا والابتكار، وقد اتخذت بعض الخطوات لتنظيم الأصول المشفرة والتكنولوجيا المالية، و ولاية تكساس التي تعتبر بيئة مرحبة بشكل عام بصناعة العملات المشفرة، ولكن لا توجد تشريعات دقيقة على مستوى الولاية حتى الآن. ما يُقال باختصار أن السلطات الرقابية في الولايات المتحدة تسعى جاهدة لتطوير إطار قانوني يلبي تحديات وفرص الأصول المشفرة، وتتغير هذه التشريعات بشكل منتظم لمواكبة التطورات في هذا المجال[14] و هذا ما ننصح به على مستوانا الوطني.

على المستوى الأوروبي، يجري حاليًا اتباع نهج نحو التنظيم المنسق للأصول المشفرة وبالتالي، فإن لائحة أسواق الأصول المشفرة " MiCA[15]،

الهادفة لأجل تنظيم الأصول المشفرة، هي موضوع " لائحة " أوروبية تُطبق اعتبارًا من 30 ديسمبر 2024، باستثناء الأحكام المتعلقة بالعملات المستقرة (العنوانان الثالث والرابع من اللائحة) والتي ستدخل حيز التنفيذ اعتبارًا من 30 يونيو 2024[16]. و يأتي هذا الإطار التنظيمي الأوروبي الأول بعد انهيار العملات المشفرة منذ مارس2022.

2.1. المخاطر المتعلقة بالأصول المشفرة:

إن الاستثمار في الأصول المشفرة يتزايد بشكل متسارع، ومع ذلك يجب على المستثمرين فهم المخاطر المرتبطة بهذا العالم المتقلب حيث يتميز سوق العملات الرقمية بتقلباته الكبيرة ويمكن أن تتأثر الأسعار بعوامل مثل الأخبار السلبية أو تداولات كبار المستثمرين، إلى جانب معاناة القطاع من نقص في التنظيم، مما يعني أن المستثمرين قد يكونون عرضة للاحتيال والتلاعب و كثرة الهجمات السيبرانية وسرقة الأصول الرقمية التي تمثل تحديات الأمن للمستثمرين والمنصات، إضافة إلى التغييرات في التشريعات واللوائح بشكل مستمر مما يؤثر على القدرة على التداول والاستثمار[17].

من الضروري توخي الحذر وإجراء البحث والتحليل قبل الاستثمار في الأصول المشفرة و من المفيد استشارة المختصين في المالية والالتزام بإجراءات أمان قوية لحماية الأصول، كما يجب أيضًا التفكير بعمق في مستوى المخاطر الذي سيتم تحمله وتحديد استراتيجية استثمارية ملائمة[18].

منذ بداية عام 2018، تحذر هيئة الأسواق المالية AMF و صندوق النقد العربي[19] الجمهور بانتظام من عمليات الاحتيال العديدة الموجودة على الويب، ففي الولايات المتحدة، أنشأت *لجنة تداول العقود الآجلة للسلع CTFC* نظامًا للإبلاغ عن عمليات الاحتيال المتعلقة بالأصول المشفرة *scams*، بما في ذلك عمليات الاحتيال *والتلاعب* المتعلقة بالعملات الافتراضية و يتم تقديم مكافآت مالية[20] والحماية للمبلغين من الأفراد والمستهلكين للتنديد بسلوك *الضخ pump*

and dump والتفريغ أو *التداول المغشوش* أو منصات التداول غير مصرح بها. وهذه الآلية، شبيهة بآلية المبلغين عن المخالفات في قضايا التهرب الضريبي بالجزائر.

2. التعدين الخفي و عروض العملات الأولية

في ظل تقدم التكنولوجيا، أصبحت حالات التعدين الخفي تشكل تحديًا متزايدًا و يتعلق الأمر بإجراء عمليات التعدين للعملات الرقمية دون علم أو موافقة من قبل أصحاب الأجهزة، و هذا ما يُؤدي إلى استهلاك غير قانوني لموارد الحواسيب وتكلفة طاقة عالية لذا يتطلب حل هذه المشكلة التحقق من أمن الشبكة وتعزيز الوعي حول الأمن الرقمي.

إلى جانب التعدين الخفي كأحد مظاهر الجرائم المالية السيبرانية، تعتبر عروض العملات الأولية ICO وسيلة مبتكرة لجمع التمويل للمشاريع اللامركزية، إذ يُمكن للشركات الناشئة جذب الاستثمارات فيها من خلال بيع عملتها الرقمية. ومع ذلك، يجب أن تتبع هذه العمليات معايير الشفافية والأمان لحماية حقوق المستثمرين لكن تطرح هذه العمليات تحديات تنظيمية، وتتطلب إطارًا قانونيًا لحماية المستثمرين وتعزيز استدامة هذه الأسواق الناشئة.

سنحاول أن نستعرض في المحور الثاني هاتين الظاهرتين بإستجلاء وصفي و مفاهيمي لهذين الأسلوبين الإحتياليين السيبيرانيين.

2.1. التعدين الخفي Cryptojacking:

الكريبتوجاكينغ هي تقنية يستخدمها مجرمو الإنترنت لتعدين العملات المشفرة باستخدام قوة المعالجة لأجهزة الكمبيوتر الخاصة بالضحايا دون موافقتهم و غالبًا ما يتم استخدام هذه التقنية من خلال دمج التعليمات البرمجية الضارة مع موقع ويب أو برنامج أو بريد إلكتروني و بمجرد أن ينقر الضحية على الرابط الخبيث، يتم تنشيط الكود ويبدأ في تسخير قوة الكمبيوتر لاستخراج العملات المشفرة[21].

إن ظاهرة التعدين الخفي، وهي الاستخدام السري لقوة المعالجة للكمبيوتر من أجل استخراج الأصول المشفرة نيابة عن الشخص الذي قام باختراقها، آخذة في الارتفاع منذ نهاية عام 2017. وبالتالي تقوم الجماعات الإجرامية بإنشاء "شبكات الروبوتات"، والشبكات من برامج الكمبيوتر الطفيلية، للاستفادة من قوة أجهزة كمبيوتر الغير (الطرف الثالث). وبالتالي، يتم تخصيص وحدات جديدة من الأصول المشفرة للمجرم الإلكتروني دون تحمل التكلفة الكهربائية والمادية للعملية التي تقع على عاتق مالك الكمبيوتر. علاوة على ذلك، فإن التعدين، الذي يستهلك موارد النظام بشكل مكثف، يؤثر بشكل كبير على الأداء ويسرع بشكل كبير من إهتلاك المكونات و إذا لم يتم إيقاف التعدين السري في الوقت المناسب، فإنه سيؤدي إلى الانهيار والاستبدال الحتمي للمكونات الإلكترونية للكمبيوتر، لأن هذه البرامج الضارة تعمل في الخلفية وتستفيد من قوة الحوسبة لشبكة كاملة من الأجهزة المصابة لتحقيق الربح وتتحمل الضحية وحدها التكلفة.

ولدت فكرة التعدين الخفي في منتصف سبتمبر عندما اقترحت CoinHive برنامجًا نصيًا لتعدين العملات المشفرة (المونيرو في هذه الحالة). ومن بين المواقع التي اعتمدته موقع The Pirate Bay، وهو موقع المشاركة P2P، والذي اعتمد على موارد مستخدميه كوسيلة بديلة للتمويل و تشمل القنوات الرئيسية الأخرى التي استخدمت التعدين الخفي قناة شوتايم التلفزيونية والموقع الرسمي لنجم ريال مدريد كريستيانو رونالدو، الذي نشر نص CoinHive دون إخطار مستخدميه. و تتخذ اليابان إجراءات صارمة ضد إساءة استخدام Coinhive ويُعد استخدام المكتبة أمرًا مثيرًا للجدل، خاصة إذا لم يطلب مالكو المواقع الإذن من المستخدمين، وأصبحت المكتبة مفضلة لدى مؤلفي البرامج الضارة الذين غالبًا ما ينشرونها على المواقع المخترقة[22].

وتُعتبرالابتكارات الرقمية بمثابة دعم لأشكال جديدة من الاحتيال التي تنظم بالإنطلاق من تحديث المخططات الكلاسيكية و تصل إلى"عمليات السطو" المذهلة والسرقات واسعة النطاق التي تنفذ في صمت و بدون جلبة أو ضوضاء

العالم المادي. وأخيرا، يجد المتورطون في تبييض الأموال حلفاء في مقدمي خدمات الدفع الجدد الذين يكتسب عملاؤهم حمايةً بالتستر عن هويتهم و إخفائها، وهو ما يضمن في كثير من الأحيان الإفلات من العقاب بالإضافة إلى تسهيل عمليات الاتجار غير المشروع من خلال ثلاث آليات: منتديات المناقشة، والشبكات المظلمة ، والعملات المشفرة[23].

وجدير بالتنويه أن عمليات قرصنة المعطيات، جعلت من هذه التقنية أكثر تعقيدًا، بحيث يستطيع المحتالون الوصول إلى المخططات التنظيمية التفصيلية و استغلال رؤوس(en-tête) الرسائل والمستندات المحاسبية والتفاصيل المصرفية للموردين ثم يستخدم المحتال بعد ذلك عذر تغيير التفاصيل المصرفية للمورد لطلب تحويل طارئ، والذي سينتهي بطبيعة الحال في حساباته الخاصة. كما يستخدم القراصنة تقنية إرسال رابط مرتبط ببرنامج تجسس يدعو فيه الضحايا للاتصال بمقعهم المصرفي، ثم تتم سرقم بياناتهم ورموز الوصول إلى الإنترنت، والتي سيستخدمها المحتالون لإنشاء أوامر الدفع لمصلحتهم الخاصة[24].

2.2 عروض العملات الأولية ICOs :

ظهرت عمليات الطرح الأولي للعملات ICOs في عام 2016 وتطورت في بيئة ذات سيولة وفيرة، فهي تجمع بين ابتكارين رئيسيين: في إجراءات الدعوة إلى الادخار خارج أي إجراء تنظيمي على أساس معلومات ذات جودة متغيرة؛ ومن ناحية أخرى في الحقوق الممنوحة التي تكون شديدة التنوع (من حيث الملكية ، الإستعمال والمزايا المختلفة) ولكنها غالبًا ما تكون غامضة للغاية.

و تعد عروض العملات الأولية ICO، أو جمع الأموال في العملات المشفرة، وسيلة للتمويل التشاركي (التمويل الجماعي) لشركات تكنولوجيا Blockchain. فهي تقنية تخزين ونقل المعلومات، وتعتبر شفافة وآمنة وتعمل بدون هيئة تحكم مركزية[25].

حاليًا، لا يوفر وضع الإصدار هذا أي ضمان حقيقي للمشتركين وبالتالي فإن عمليات الطرح الأولي للعملات هي منتجات محفوفة بالمخاطر، ولكنها مع ذلك يتم "إدراجها "في كثير من الأحيان عند إصدارها على منصات البورصة وتشكل خاصية الأمان للبلوكشين أحد التحديات الرئيسية التي تواجهها إلى حد الوهم بالثقة العمياء في هذه التكنولوجيا ومنه يمكن أن تكون الثغرات الأمنية والقرصنة من أسباب فشلها. و يجب التوضيح أنه يمكن لأي حامل بيتكوين أن يفقده إذا فقد مفتاحه ولذلك فمن الضروري الاستعانة بمزود خدمة مسؤول عن أمنه الرقمي[26].

ولقد أدى التطور السريع لعمليات الطرح الأولي للعملات ICOعلى المستوى الدولي إلى خلق جاذبية للمحتالين الذين يقدمون مشاريع وهمية. في نفس الوقت تبين أن العديد من عمليات الطرح الأولي للعملات ICO كانت عبارة عن عمليات احتيال. و خير مثال ما وقع لبورصة *Coincheck* باليابان، حيث خسرت الكثير من عملات البيتكوين إثر إختراق عملة NEM المشفرة على منصة *Coincheck* ، أين تمت سرقة 523 مليون "رمز" بقيمة إجمالية تبلغ حوالي 530 مليون دولار على أساس الأسعار "المعروضة "في وقت "الكسر " ويُعتقد أن حوالي 260 ألف مستخدم قد تأثروا . من جراء هذه العملية. وقد تم تخزين الوحدات المسروقة "ساخنة"، بدلا من وضعها في محافظ "باردة " *offline* كي تكون أكثر أمانا باعتبارها تكون مفصولة عن الإنترنت. من هذه الحادثة يُمكن الإتعاض و إبداء النصيحة للهيئات التنظيمية من أجل السعي لإجبار منصات التبادل على استخدام التخزين دون اتصال بالإنترنت و استخدام التوقيع المتعدد، لأنه لم تكن العملات المعدنية التي سرقها القراصنة محمية بنظام التوقيع المتعدد[27].ذ

الخاتمة:

تتسارع التطورات الرقمية الحديثة بشكل كبير، ومعها يزداد استخدام بعض الأفراد والجماعات لتلك التكنولوجيا في أغراض إجرامية و التحايل

المالي و السيبيراني و تبييض الأموال باستغلال تخفي الهوية و الانترنت المظلم و غيرها من الأساليب التي عرجنا عليها بالتلميح و مع ذلك، يمكن أن تكون أهم **النتائج المتوصل** إليها في مقالناهذا ما يلي:

- تنبه الدراسات إلى الزيادة المضطردة في حالات الاحتيال المرتبطة بالعملات المشفرة التي يمكن أن تشمل هذه الاحتيالات سرقة المحافظ الرقمية، واحتيال الاستثمار، وأنشطة تزوير العملات المشفرة.

- يُمكن أن يؤدي زعزعة السوق المالية و الإئتمان لتجاري إلى تقلبات في الأسعار وانخفاض ثقة المستثمرين.

- قصور في التشريعات والتنظيمات والرقابة على استخدام الأصول المشفرة في حالات النصب والاحتيال و تبييض الأموال و تمويل الارهاب، مما يتعين تداركه.

الإقتراحات و التوصيات:

يُمكن أن نقدم بعض التوصيات بشأن الحلول والتدابير الوقائية للوقاية من الاحتيال باستخدام الأصول المشفرة و التصدي لها من خلال :

- تعزيز الأمن السيبراني وتطوير تقنيات جديدة للكشف عن الهجمات السيبيرانية و تعزيز سُبل الحماية ضد التهديدات السيبرانية و تطوير وتحسين إجراءات الأمن على منصات تداول العملات المشفرة للوقاية من هجمات القرصنة المعلوماتية.
- إعادة النظر في التشريعات لتكون أكثر فعالية في مواجهة التحديات الرقمية وتطويرها و تحديثها.
- تطويرالتشريعات و المراسيم و اللوائح التنظيمية المتعلقة بالأصول المشفرة لمكافحة جرائم النصب وتعزيز الشفافية.
- تعزيز التحقق من الهوية الرقمية و فرض إجراءات التحقق بصرامة كبيرة عند التسجيل على منصات التداول، للحد من إمكانية استخدام حسابات مزيفة و تجريم الهوية الرقمية المزيفة.

- توعية المستثمرين بشكل أفضل حول المخاطر المحتملة والإجراءات الواجب اتخاذها عند التعامل مع الأصول المشفرة.
- تعزيز الإجراءات للتحقق من شرعية المشاريع والمنصات التي تطلب تمويلًا عبر عروض العملات الأولية ICO .
- دعم البحث لتطوير حلول تقنية متقدمة لمكافحة الاحتيال السيبراني في مجال العملات المشفرة.
- تشجيع البحث في التكنولوجيا الأمنية للبلوكشين، قصد تقوية أمن العملات المشفرة.
- تشجيع التعاون الدولي بين الحكومات والهيئات التنظيمية لمواجهة الاحتيال السيبراني على مستوى عالمي.

التهميش و الإحالات :

[1] LEGEAIS D, Blockchain et actifs numériques, LexisNexis, 2019 .

[2] Cryptojacking : هو مصطلح يشير إلى عملية استخدام موارد حاسوب الضحية دون موافقتها لتعدين العملات المشفرة. يتم ذلك عادةً عن طريق زرع برمجيات خبيثة (malware) في الأنظمة أو عبر الإصابة ببرامج ضارة عبر مواقع الويب أو رسائل البريد الإلكتروني. عندما يتم تشغيل جهاز الكمبيوتر المستهدف، يتم استخدام معالجه وقدرته الحوسبية لحل معادلات رياضية معقدة ضرورية لعمليات التعدين. العملات المشفرة الرئيسية المستهدفة هي Monero ومماثلة، حيث توفر هذه العملات ميزات خصوصية تجعل من الصعب تتبع مصدر وجهات النقود. تحمل عمليات Cryptojacking عدة تحديات ومخاطر: تباطؤ الأداء، استهلاك الطاقة، مخاطر أمان المعلومات، فقدان الخصوصية. أنظر : أكاديمية البيتكوين العربية
https://btcacademy.online/كريبتوجاكينغ- هو- ما– cryptojacking؟/

[3] احتيال ICO أو (عروض العملات الأولية): هو إطلاق عملات رقمية جديدة من خلال ICO والاحتيال في عملية جمع التمويل عبر الحصول على أموال من المستثمرين دون توفير المشروع المعترف به.
و يعتبر احتيال ICO نوعًا خطيرًا من الاحتيال حيث يتم استغلال حماس المستثمرين لتمويل مشاريع عملات رقمية جديدة. في هذه العمليات، يقوم المحتالون بإصدار عملات رقمية جديدة باسم مشروع واعد، يتم تسويقها كاستثمار مستقبلي مربح. ومع ذلك، يكمن الاحتيال في عدم تحقيق المشروع للوعود التي قدمها للمستثمرين.
تتبنى عمليات احتيال ICO العديد من الطرق المكشوفة للحصول على الأموال بشكل غير قانوني، مثل:
استخدام تكتيكات التسويق المضللة لإيهام المستثمرين بأن المشروع يحمل إمكانيات نمو كبيرة دون توفير معلومات دقيقة ونشر نشر معلومات كاذبة أو غير دقيقة أو قد يتم استخدام صور غير حقيقية لأعضاء الفريق أو الشركاء بهدف الإخفاء هوية المحتالين الحقيقية.و أخيرا بمجرد جمع الأموال، قد يقوم المحتالون بالاختفاء دون تحقيق المشروع أو توفير المنافع المعتادة للمستثمرين.أنظر المرجع أعلاه أكاديمية البيتكوين العربية.

[4] كلمة «فوركس» تشير إلى سوق العملات الأجنبية أو البورصة العالمية للعملات الأجنبية، وهي اختصار للمصطلح الاقتصادي من اللغة الأجنبية "Foreign Exchange Market" أي «سوق تداول العملات الأجنبية»، وهو سوق يمتد في جميع أنحاء العالم حيث تصرف العملات من قبل عدة مشاركين، مثل البنوك العالمية والمؤسسات الدولية والأسواق المالية والمتداولون الأفراد.
أنظر:
https://ar.wikipedia.org/wiki/سوق_صرف_ العملات

[5] أمر رقم 12-02 ممضي في 13 فبراير 2012، الجريدة الرسمية عدد 8 المؤرخة في 15 فبراير 2012، الصفحة 6، يعدل ويتمم القانون رقم 05-01 المؤرخ في 27 ذي الحجة عام 1425 الموافق 6 فبراير سنة 2005 والمتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما.

[6] أنظر المادة 04 من القانون رقم 23-01 المؤرخ في 07 فبراير سنة 2023 النعدل و المتمم للقانون 05-06 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما. (ج.ر عدد08 مؤرخة في 08 فبراير2023، ص 6).

[7] "يُعرف أيضًا باسم جهاز التسجيل الإلكتروني المشترك".
G. MARRAUD des GROTTES Auditions au Sénat sur la blockchain : les incompréhensions demeurent… RLDA N°135 1er mars 2018.

[8] Mathis B, Quel régime juridique pour les cryptoactifs, RLDA 2018/143, Suppl., nº 6613.
بالنسبة للبنك المركزي الأوروبي (ECB) وبنك فرنسا، فإن "البيتكوين ليست عملة، لأنها لا تجمع بين الخصائص الثلاث: وسيلة الدفع، ووحدة الحساب، واحتياط ذو قيمة."

[9] الطرح الأولي للعملة (ICO) هو نموذج لجمع التمويل يتيح للشركات أو المشروعات الناشئة جمع الأموال من خلال بيع عملتها الرقمية المستقبلية (عادة ما تكون عملة رقمية أو رمز مميز) للمستثمرين. يتم ذلك من خلال توزيع هذه العملة الرقمية للمستثمرين مقابل العملات التقليدية أو العملات الرقمية الأخرى مثل البيتكوين أو الإيثيريوم. ويمر بالخطوات الرئيسية:وضوح الفكرة، إعداد الوثيقة البيضاء (Whitepaper)، تحديد الهدف المالي، تحديد فترة الICO، التسويق وجذب المستثمرين، إطلاق العملة الرقمية، الحفاظ على التواصل.
تعد ICO طريقة شائعة لتمويل المشروعات اللامركزية والتكنولوجيا الجديدة، ولكنها تأتي مع مخاطر، بما في ذلك عدم وجود تنظيم قوي، واحتمال حدوث احتيال، وتقلبات كبيرة في قيمة العملة الرقمية.
انظربالتفصيل:
https://www.rain.com/ar/learn/ico-initial-coin-offering-explained-beginners-guide

[10] ALUMASEANU S., Le traitement pénal du Bitcoin et des autres monnaies virtuelles, Gaz. Pal 2014, no 242.

[11] في 25 يوليو 2017، تم القبض على ألكسندر فينيك في اليونان، بناءً على طلب من الولايات المتحدة للإشتباه في قيامه بتبييض الأموال من أنشطة غير قانونية عبر منصة تبادل الأصول المشفرة الخاصة به .BTC-e. التي كان يستخدمها حوالي 700 ألف زبون - هذه المنصة التي تم إنشاؤها في عام 2011-، وتمكن من نقل حوالي 9.4 مليون بيتكوين (أو حوالي 33 مليار يورو في عام 2018)2، لكن تم الإفراج عنه لنفي فينيك هذه الاتهامات ثم يتم تسليمه إلى فرنسا في 2020، حيث حوكم في ديسمبر 2020، ثم في يونيو 2021 وإدانته بالحبس لمدة 5سنوات وتم تأييده عند الاستئنافلثبوت جرم تبيض الأموال في إطار العصابة المنظمة .
أنظر بالتفصيل:

https://arabic.cnn.com/world/article/2022/08/05/russian-man-accused-of-money-laundering-running-4b-bitcoin-exchange-extradited

[12] مخطط بونزي، يتم تشكيل نموذج استثماري يعتمد على تحقيق عوائد للمستثمرين من خلال أموال الأفراد الجدد بدلاً من الأرباح الحقيقية أو الاستثمارات و يتم تحقيق النصب في مخطط بونزي: وعود أرباح غير واقعية وغالبًا تكون عالية جدًا، عندما يستثمر شخص مبلغًا من المال، يتم استخدام هذا المبلغ لدفع الأرباح للمستثمرين السابقين. بمجرد أن يتم الحصول على مزيد من المستثمرين، يتم استخدام أموالهم لدفع الأرباح للمستثمرين الأقدم وفي مخطط بونزي، لا يوجد استثمار حقيقي أو نشاط تجاري يولد الأرباح. بدلاً من ذلك، يتم استخدام الأموال الجديدة لدفع الأرباح للمستثمرين السابقين والإبقاء على التيار المستمر، مما يؤدي في نهاية المطاف إلى انهيار المخطط.

أنظر بالتفصيل:

https://www.cryptopolitan.com/ar/مخططات-بونزي-مقابل-الهرم-احذر-من-الخداع/ /

[13] وفي تقريرها لعام 2020، وجدت Tracfinأيضًا أن الأصول المشفرة التي تم الحصول عليها بهذه الطريقة يمكن تحويلها إلى ممتلكات من خلال مزودي خدمات الدفع الذين يقدمون هذا الاحتمال.

أنظر: https://www.economie.gouv.fr/tracfin/tracfin-2020-activite-et-analyse

[14] أديتيا نارين, مارينا موريتي، تنظيم العملات المشفّرة، مجلة صندوق النقد الدولي ، سبتمبر 2022.

أنظـــــر المقـــــال: https://www.imf.org/ar/Publications/fandd/issues/2022/09/Regulating-crypto-Narain-Moretti

[15] MiCA : *« markets in crypto-assets »*.

[16] Règlement (ue) 2023/1113 du parlement européen et du conseil du 31 mai 2023 sur les informations accompagnant les transferts de fonds et de certains crypto-actifs, et modifiant la directive (ue) 2015/849.journal officiel de l'union européenne. L 150/1.

[17] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.

[18] Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. John Wiley & Sons.

[19] مخاطر وتداعيات العملات المشفرة على القطاع المالي، أمانة مجلس محافظي المصارف المركزية ومؤسسات النقد العربية، رقم 2019/117، تاريخ النشر 12-04-2020 من طرف صندوق النقد العربي. أ،ظر بالتفصيل:

https://www.amf.org.ae/sites/default/files/publications/2022-01/the-risks-and-repercussions-of-cryptocurrencies-on-the-financial-sector.pdf

[20] للإشارة، إذا نتج عن التنديد عقوبة تزيد على مليون دولار، فستذهب مكافأة تتراوح بين 10 إلى 30% من العقوبة للشخص المبلغ.

[21] M. ROUSSILLE Crypto-actifs : le modèle de régulation en jeu Bull. Joly Bourse n°02 p. 73, 1er mars 2018.

[22] Stéphane le calme, La première condamnation pour usage malveillant de la bibliothèque Coinhive pour cryptojacking est tombée, Le 5 juillet 2018 à 18:09 L'accusé n'a pu se faire que 38 €.

[23] Cryptoactifs,lamyline
[24] https://www.avast.com/fr-fr/c-protect-yourself-from-cryptojacking?redirect=1
" Protégez-vous du cryptojacking"
[25] R. SOCHON La révolution technologique du Bitcoin et des ICO : un casse-tête pour les commissaires aux comptes Petites affiches 31 janv. 2018 n°023 p. 4 ID : LPA133m6
[26] Lamyline.fr
[27] Legeais D., JCl. Commercial, V° Blockchain, Fasc. 2160 .

قائمة المراجع:

a. ***Ouvrages***

1. Féral schuhl c., cyberdroit, coll. Praxis, dalloz, 11e éd. ;
2. Ghernouarti s., la cybercriminalité/ les nouvelles armes de pouvoir lausanne, les presses polytechniques et universitaires romandes, 2017, 2e éd. ;
3. Legeais d, blockchain et actifs numériques, lexisnexis, 2019 ;
4. Maison rouge (de o., les cyberrisques, la gestion juridique des risques à l'ère immatérielle, lexisnexis, 2018 ;
5. Quéméner m., Le droit face à la disruption numérique, Gualino, Lextenso, 2018 ; Criminalité économique et financière à l'ère numérique, Economica, 2015 ;

b. ***Articles et chroniques***

1. A. Touati m. Cabassu, *Le traitement des cryptomonnaies dans les bilans comptables* Les Nouvelles Fiscales, N°1217, 1er mars 2018.
2. Alumaseanu s., le traitement pénal du bitcoin et des autres monnaies virtuelles, gaz. Pal 2014, no 242.
3. Beaussonie g., cybercriminalité – la place du droit pénal dans la lutte contre la cybercriminalité, jcp g 2021, aperçu rapide .
4. Clément s., lelieur j., la conformité anti- blanchiment face aux crypto-actifs, rsc 2021, p. 15 .

5. Fernandez-bollo e., institutions financières et cybercriminalité, revue d'économie financière, 2015/4, n° 120, p. 181.
6. Cabon s.-m., l'influence du cyber espace sur la criminalité économique et financière, dr. Pén. 2018, étude 5 .
7. Chopin f., Cybercriminalité, Rép. pénal Dalloz, n° 198 et s. .
8. Francillon J., Le droit pénal face à la cyberdélinquance et à la cybercriminalité, RLDI 2012/81, n° 2728 .
9. F. Dempure *où en est la révolution blockchain ?* Jcp n. N°18-19, 04 mai 2018, 1182.
10. Maltis b, crypto-actifs : les régulateurs en quête d'une doctrine. Retour sur l'actualité de 2019, rldi 2020/166 .
11. P. Létienne la crypto-monnaie bitcoin (btc) s'apprecie, rldi, mai 2018.
12. S. Maouche *amf : vers un nouveau cadre légal pour les initial coin offerings* dossiers d'actualité, lexisnexis 10 avr. 2018
13. M. Roussille crypto-actifs : le modele de regulation en jeu bull. Joly bourse n°02 p. 73, 1er mars 2018.
14. V. Balta *quelle régulation pour les dérivés sur crypto-monnaies ?* Dictionnaire permanent epargne et produits financiers – instruments financiers 15 mars 2018.
15. V. Renoux s. Bernard *généralités – crypto-monnaies et initial coin offerings : voyage en terre inconnue* droit fiscal n°5, 1er févr. 2018, 150.

c *Rapports et sites web*

1. Amf, étude sur la cybercriminalité boursière : définition, cas et perspectives, 10 oct. 2019 .
2. Bernalicis u. Et maire j., rapp.an n° 4314 d'information sur la mise en œuvre des conclusions du rapport d'information n° 1822 du 28 mars 2019 sur l'évaluation de la lutte contre la délinquance financière.2021.
3. Club des juristes, le droit pénal à l'épreuve des cyberattaques, avr. 2021.
4. Colb, rapport analyse nationale des risques de blanchiment de capitaux et de financement du terrorisme en france, sept. 2019 .

5. Dgccrf, guide, les risques de blanchiment de capitaux de financement du terrorisme liés à la crise sanitaire et économique de la pandémie covid-19, 28 mai 2020 .
6. Dossier, Cybersécurité, Banque et stratégie 2019, n° 383 et 2018, n° 365 .
7. Gauvain r., rapport sur la protection des entreprises contre les sanctions américaines, rapport parlementaire, 26 juin 2019 .
8. Ocde, en finir avec les montages financiers abusifs : réprimer les intermédiaires qui favorisent les délits fiscaux et la criminalité en col blanc, févr. 2021 .
9. Rapp. Anssi 2022, www.sssi.gouv.fr.;
10. Rapp .Ctrf,www.ctrf.mf.gov.dz/
11. https://www.bank-of-algeria.dz/
12. https://www.joradp.dz/
13. https://www.legifrance.gouv.fr/