(ISSN: 2356 - 9492)

استخدام العملات الرقمية المشفرة
(المخاطر – الحلول)

استاذ دكتور / حسام نبيل الشنراقي
استاذ علوم البحث والتحقيق الجنائي المشارك
رئيس قسم ادارة الشرطة
اكاديمية شرطة دبي

الملخص باللغة العربية:

تكمن أهمية هذه الدراسة في أن العملات الرقمية هي أحد الأشكال الحديثة للنقود، والتي يتم تنفيذها من خلال أنظمة إلكترونية مع تشفير ويتم تداولها كأحد تطبيقات سلاسل الكتل ، مما يتيح إمكانيات عالية لحرية التداول دون تقييد حسب الحدود الاقتصادية والجغرافية ، ثم تقلل مصاريف التحويلات النقدية التي تمثل على مستوى واسع ملايين الدولارات وتوفر للمؤسسات التي تتعامل بمبالغ ضخمة من المصاريف الإدارية ، لذلك بدأت تفرض نفسها في المعاملات الحكومية ، الأمر الذي تطلب إنتاج عملة مشفرة لتعزيزها ، بالإضافة إلى زيادة جرائم اختراق الأنظمة الإلكترونية لأشهر العملات المشفرة ، مما أثر على اقتصاديات بعض الدول والمؤسسات ، لذلك بدت أهمية هذه الدراسة لتسليط الضوء على جميع جوانب العملات المشفرة.في المعاملات والمخاطر الأمنية المحتملة وكيفية التعامل معها في ظل التعاون الدولي، وتوضح الدراسة جرائم العملة المشفرة وما يعنيه ذلك من ظهور أنماط إجرامية جديدة وتطور أنماط إجرامية قائمة ، باعتباره اختراقًا لتأمين العملات المشفرة ، ما يهدد الأمن الشامل، فعندما تعتمد السلطات عليها في معاملاتها الحكومية وغير الحكومية .فهذا يتطلب إعداد نظام إستراتيجي للشرطة لمواجهة الأنماط الإجرامية

أولاً ، تم بوضع عدة أهداف لنفسي أريد الوصول إليها ، وهي توضيح ماهية العملات المشفرة ، وكيف تعمل ، والمخاطر التي ستنجم عن التعامل معها ، لفهم كيفية التعامل مع تلك المخاطر وإيجاد أفضل الطرق لمواجهتهم.

كما أظهرت أيضًا أنماط الجرائم التي يمكن أن تستهدف النظام الإلكتروني للعملات المشفرة .وتم تحليلها للوصول إلى الآلية المناسبة لمواجهتها وحمايتها وفهم الأساليب

التي تستخدم بها العملات المشفرة لارتكاب الجريمة ، وخاصة بعض الأنماط الشائعة مثل تمويل الإرهاب وغسيل الأموال وغيرها ، للوصول إلى آلية شرطية مناسبة لمكافحة كلا النوعين .سواء كانت الجرائم التي تهدف إلى اختراق نظام العملات المشفرة أو التي تستخدمه لارتكاب جرائم.وتناولت الدراسة الجرائم المرتكبة باستخدام العملات المشفرة، والجرائم المرتكبة ضد العملات بتهمة التزوير واختراق نظام التشفير والسرقة، والاساليب الإجرامية بالإضافة إلى منابع الجريمة سواء ارتكبت ضدها او باستخدامها ، وتم

التعريف بالعملات الرقمية من خلال شرح مفهوم العملات الرقمية وخصائصها وأسباب جاذبية التعامل مع العملات الرقمية وتطورها ومخاطرها ، ثم دراسة مخاطر استخدام العملات المشفرة في الجريمة من خلال توضيح ميزات العملات الرقمية لمرتكبيها و دورهم في إخفاء الأنشطة الإجرامية ثم الجرائم التي ترتكبها العملات الرقمية وهي جرائم الاحتيال والاستيلاء على العملات المشفرة وغسيل الأموال وتمويل الإرهاب ، ثم الجرائم التي تستهدف نظام العملات المشفرة مثل هجوم الإنفاق المزدوج وهجمات البنية التحتية وكسر –SHA دمج ٢٥٦ خوارزمية ، ثم مناقشة مستقبل العملات الرقمية من خلال اقتراح استراتيجية أمنية في مجال العملات الرقمية من خلال محورين

اختتمت الدراسة بأن العملات المشفرة هي أداة من المفترض أن تكون مفيدة للبشرية من جميع النواحي ، وبالتالي فهي تتمتع بالعديد من المزايا التي أبرزتها هذه الدراسة ، ولكن كما أن كل ابتكار جديد له جوانب مفيدة ، فإن له أيضًا استخدامًا ضارًا ، مما يؤدي إلى إلحاق الأذى بالآخرين ، وتتمثل هذه الأضرار في أنها أصبحت أداة لمرتكبي الجرائم ليتمكنوا من إخفاء أنشطتهم الإجرامية ، مستغلين ميزة إخفاء الهوية التي تميز هذه العملات وصعوبة تعقبها أو المحافظ الإلكترونية التي تحتوي عليها .والتداول من خلاله مما ساعدهم إلى حد ما .ما الخطأ في غسل أموالهم غير المشروعة وارتكاب جرائم مثل تمويل الإرهاب ، لكن الدراسة تظهر أن العملات الرقمية يمكن أن تخفي الأنشطة التي تستخدم فيها إذا لم يتم استخدامها لإيذاء شخص معين ، أي أنه لا يوجد ضحية لجريمة التي ارتكبوا فيها .المحور الثاني يتمثل في الجرائم التي تهدف إلى اختراق العملات الشخصية لخرق الثقة بها ، بحيث لا يتم التعامل معها ، أو يتضرر

(ISSN: 2356 - 9492)

المتعاملون فيها ويفقدون رؤوس أموالهم التي يستثمرون فيها .من خلال مبادرات إقليمية أو دولية .وخلصت الدراسة إلى توصيتين تفصيليتين:

- يعد استخدام العملات الشخصية أمرًا ضروريًا بالنظر إلى التحول الرقمي الكامل المتوقع ، فمن الضروري الشروع في تطوير استراتيجية للشرطة بعدة محاور ، بما في ذلك المحور التقني المتمثل في إنشاء بلوك تشين ، والذي يتم من خلاله إنتاج عملات رقمية مشفرة ، وسلسلة البلوكشين التي يتم تبادلها من خلال خوادمها، المحور الثاني يتعلق بالأمن الجنائي من حيث متابعة الأنشطة الإجرامية التي تتم من خلال الانترنت المظلم وتنسيق الجهود مع الجهات المعنية لتتبع وضبط عمليات تمويل الجماعات الإرهابية وتبادل وغسيل الأموال لصالح جماعات الجريمة المنظمة للحد من السلبيات .التأثيرات الأمنية للعملات المشفرة، المحور الثالث هو المحور التشريعي حيث تقنن العملات المشفرة ومواصفاتها المحددة والجهات المسؤولة عن إنتاجها وكافة تفاصيل إنتاجها وتداولها والعقوبات المقررة لمهاجمة نظامها الإلكتروني في إطار تقنين خاص أو ملحق بقانون مكافحة الجرائم الإلكترونية

بينما تضمن الثاني اقتراحًا بتضمين برامج تدريبية حول فهم نظام العملات المشفرة وبلوك تشين ضمن برامج تدريب الضباط وتخصصهم ضمن ضباط الجرائم المالية.

Abstract:

The importance of this study lies in the fact that digital currencies are one of the modern forms of money, which are implemented through electronic systems with encryption and are traded as one of the applications of block chains, which allows high possibilities for freedom of circulation without restriction according to economic and geographical borders, and then reduces the expenses of cash transfers that represent On a large scale, millions of dollars are provided to institutions that deal with huge amounts of administrative expenses, so they began to impose themselves in government transactions, which required the production of a cryptocurrency to strengthen it, in addition to the increase in crimes of hacking electronic systems of the most famous cryptocurrencies, which affected the economies of some countries

and institutions, Therefore, the importance of this study seemed to shed light on all aspects of cryptocurrencies in transactions, potential security risks, and how to deal with them in light of international cooperation. What threatens the overall security, when the authorities depend on them in their governmental and non-governmental transactions. This requires preparing a strategic police system to confront criminal patterns Firstly, I set several goals for myself that I want to reach, which is to clarify what cryptocurrencies are, how they work, and the risks that will result from dealing with them, to understand how to deal with those risks and to find the best ways to confront them. It also showed patterns of crimes that could target the cryptocurrency electronic system. And it was analyzed in order to reach the appropriate mechanism to confront and protect it, and to understand the methods by which cryptocurrencies are used to commit crime, especially some common patterns such as financing terrorism, money laundering, and others, in order to reach an appropriate police mechanism to combat both types. Whether it is crimes that aim to penetrate the encrypted currency system or that use it to commit crimes. The study deals with crimes committed using encrypted currencies, crimes committed against currencies on charges of counterfeiting, hacking the encryption system and theft, and criminal methods in addition to the sources of crime whether committed against or using them. Introducing digital currencies by explaining the concept of digital currencies, their characteristics, and the reasons for the attractiveness of dealing with digital currencies, their development and risks, then studying the risks of using cryptocurrencies in crime by explaining the advantages of digital currencies to their perpetrators and their role in concealing criminal activities, then the crimes committed by digital currencies, which are fraud and appropriation crimes On cryptocurrencies, money laundering, and terrorist financing, then crimes targeting the cryptocurrency system such as double spending attack, infrastructure attacks, and breaking SHA- integrating 256 algorithms, then discussing the future of digital currencies by proposing a security strategy in the field of digital currencies

(ISSN: 2356 - 9492)

through two axes The study concluded that cryptocurrencies are a tool that is supposed to be beneficial to humanity in all respects, and therefore they have many advantages highlighted by this study, but just as every new innovation has beneficial aspects, it also has a harmful use, which leads to harm to others. These damages are represented in the fact that they have become a tool for perpetrators of crimes to be able to hide their criminal activities, taking advantage of the anonymity feature that distinguishes these currencies and the difficulty of tracking them or the electronic wallets that contain them. And trading through it which helped them to some extent. What is wrong with laundering their illegal money and committing crimes such as financing terrorism, but the study shows that digital currencies can hide the activities in which they are used if they are not used to harm a specific person, that is, there is no victim of a crime in which they were committed. The second axis is the crimes that aim to penetrate personal currencies in order to breach confidence in them, so that they are not dealt with, or those who deal in them are harmed and lose their capital that they invest in. Through regional or international initiatives. The study concluded with two detailed recommendations: - The use of personal currencies is essential. Given the expected complete digital transformation, it is necessary to embark on the development of a police strategy with several axes, including the technical one of creating the Blockchain, through which cryptocurrencies are produced, and the Blockchain that is exchanged from Through its servers, the second axis is related to criminal security in terms of following up the criminal activities that take place through the dark web and coordinating efforts with the concerned authorities to track and control the financing of terrorist groups and the exchange and money laundering in favor of organized crime groups to reduce the negatives. The security effects of encrypted currencies, the third axis is the legislative axis, where encrypted currencies are legalized, their specific specifications, the parties responsible for their production, all details of their production and circulation, and the penalties prescribed for attacking their electronic system within the

framework of a special legalization or annex to the Anti-Cybercrime Law - While the second included a proposal to include training programs on understanding the cryptocurrency system and blockchain within the officer training programs and their specialization among financial crime officers.

مقدمة :

مع إدخال العملات الرقمية وتزايد الحديث عنها، ازداد الاهتمام بالعملات الرقمية بدرجة هائلة ويختلف الاهتمام مع اختلاف أصحاب الاعمال ورأس المال إلى متخصصي الأمن الإلكتروني إلى الاقتصاديين وقد تم اعتماد العملات الرقمية لأغراض شرعيّة وغير شرعيّة وحقق ذلك درجات متباينة. من النجاح وتبقى الاستفادة من الاستخدامات المتنوّعة للعملات الرقمية محل جدل.

تتطلّب العملات الافتراضية، اسسا ماديّة أقل بكثير من العملات الرسمية، والعملات الرقمية تتطلّب شبكات الكترونية قادرة على تنفيذ مثل تلك العمليّات اليوميّة، لذلك فإنّ النشر السريع للعملة الرقمية على نطاق واسع قد يكون أقلّ تعقيداً من نشر عملات تقليديّة لإمكانية صيرورة حجم المال والاساس الرقمي اللازم لنشر عملة افتراضيه أقل بكثير. ففي البلدان غير المستقرة داخليا قد تكون الإقتصادات غير كافية أو ضعيفة، وقد يكون نشر العملة الرقمية بديلاً مناسبا للمنظمات الاجرامية والارهابية التي تسعى إلى زعزعة السيادة وزيادة قوّتها السياسيّة والاقتصاديّة الخاصّة بسبب ضعف قدرات سلطات الشرطة.

وتتحدد أهمية العملات الرقمية بحسب عدد مستخدميها وقدرة شبكات تبادلها على القيام بمهامها.

والعملات الرقمية هي عملات إلكترونية لامركزية، تستخدم شبكة p2p والتشفير والتوقيع الإلكتروني لإثبات لكي يتمكن مستخدميها من نقل وتداول تلك العملات عبر شبكة الانترنت دون الحاجة لوجود وسيط أو جهة خارجية كالبنوك وذلك لكونها الية تيسر على المستخدمين التعامل بالعملات الرقمية عبر الانترنت، ويتركز اساس انتاج هذه العملات على اللامركزية فلا تعتمد على الوساطة المالية ولا تحتاج لهيئة مالية

(ISSN: 2356 - 9492)

مركزية تنظم التعامل بها كالبنوك، كما انها لا تنظم التعامل بها قواعد قانونية ولا تلتزم بضوابط البنك المركزي، ويتم تبادلها مع العملات الرسمية مثل الدولار أو اليورو وغيرها، كما تلبي رغبات الشركات والمستهلكين على تسريع ايصال الخدمة عبر الانترنت بمعنى أنها غير محسوسة وليس لها وجود مادي

وشهدت الفترة الاخيرة اهتماما عالميا بالعملات الرقمية لقبولها كوسيلة دفع وقبض في التجارة الإلكترونية والتي تعد وسيلة لتوصيل المعلومات والخدمات والمنتجات عبر شبكات الحاسوب و الوسائل الالكترونية الأخرى.[١]

أهمية الدراسة:

تعد العملات الرقمية احدى الاشكال الحديثة للنقود والتي تتم من خلال منظومة الكترونية ذات تشفير عالي يتم تداولها كأحد تطبيقات سلسلة الكتل (بلوك تشين) والتي تتيح إمكانيات عالية من حرية التداول دون التقيد بالحدود الاقتصادية والجغرافية ومن ثم تخفض نفقات التحويلات النقدية والتي تمثل في المستوى الواسع ملايين الدولارات وتوفر للمؤسسات المتعاملة بها مبالغ طائلة من المصروفات الإدارية لذا فقد بدأت تفرض نفسها في المعاملات الحكومية مما دعا دولة الامارات لإنتاج عملة رقمية بالاشتراك مع المملكة العربية السعودية لتعزيز عمليات التبادل التجاري والاقتصادي بينها وكذلك انتجت امارة دبي عملة الرقمية وسوف يتزايد الاعتماد عليها في الفترة القادمة بشكل كبير في ظل الرقمنةالكامل الوشيك في الدولة وهو ما ابرز المخاطر الاجرامية لهذه العملات بالإضافة لتزايد جرائم اختراق النظم المعلوماتية لأشهر العملات الرقمية في العالم مما اثر بشكل كبير على اقتصاديات بعض الدول والمؤسسات الكبيرة لذا ظهرت أهمية هذه الدراسة لإلقاء الضوء على كافة جوانب تطبيق تلك العملات في المعاملات في الدولة والمخاطر الأمنية المحتملة وكيفية التعامل معها في ضوء التجارب الدولية في هذا الصدد

مشكلة الدراسة

(1) Vittorio Aronica & others, digital transformation Leading our customers towards a new economy of digital ecosystems, pp:5-6, 2018, www.eng.it

تتمثل مشكلة الدراسة في فهم واستشراف المخاطر الأمنية المترتبة على استخدام العملات الرقمية في ظل الرقمنةالشامل للدولة وبخاصة امارة دبي سواء من ناحية الاثار الأمنية لاستخدامها وما يتضمنه ذلك من ظهور أنماط إجرامية جديدة او تطور لأنماط إجرامية موجودة فعليا وكذا اختراق المنظومة التأمينية لتلك العملات وهو ما يترتب عليه تهديد الامن بمفهومة الشامل عند اعتماد السلطات الحكومية عليها في تعاملاتها الحكومية وغير الحكومية وهو ما يستوجب اعداد منظومة امنية لمواجهه تلك الأنماط الاجرامية

تساؤلات الدراسة:

سوف نقوم بدراسة المشكلة من خلال الإجابة على مجموعة من التساؤلات كالتالي:

١- ما هو المقصود بالرقمنة؟

٢- ما هو المقصود بالعملات الرقمية؟

٣- ما هي الأنماط الاجرامية التي تستخدم فيها العملات الرقمية؟

٤- هل تعد العملات الرقمية امنه وما هي الاثار المترتبة على اختراق عناصر تأمينها؟

٥- ما هي المخاطر الأمنية المتوقعة في ظل استخدام العملات الرقمية في المعاملات؟

٦- ما هي الاليات الأمنية المتصورة لمواجهه هذه الأنماط الاجرامية؟

أهداف الدراسة:

تعد الدراسة من الموضوعات الهامة التي تحتاج للمزيد من البحث والدراسة وخاصة في ظل التحول نحو الرقمنة الكاملة فكان من الضروري العمل على استشراف الظواهر الاجرامية المتوقعة في ظل الرقمنة ووضع الحلول لمواجهتها في ظل رؤية شاملة للوضع المستقبلي والمخاطر التي سوف تحدث

حدود الدراسة

سوف تكون حدود دراستنا في عدة اتجاهات على النحو التالي:

(ISSN: 2356 - 9492)

– الحدود الزمانية: الفترة منذ ظهور العملات الرقمية الى توقع ما هو قادم من اثار مترتبة على تطبيقها عقب اكتمال الرقمنةفي دولة الامارات

–الحدود المكانية: تتناول الدراسة استشراف الظواهر الاجرامية المترتبة على تداول العملات الرقمية المشفرة مع التمثيل بما هو متبع في الدول التي سبقت في هذا المجال دون التقيد بدولة محددة

الدراسات السابقة:

١– دراسة بعنوان "التنظيم القانوني للعملات الرقمية" اعداد /اثير صلاح ابراهيم ابراهيم تحت اشراف الدكتور / محمد على الشباطات – للحصول على درجة الماجيستير في القانون العام – جامعة الشرق الاوسط – حزيران ٢٠٢٠ – متاحة على الموقع الالكتروني:

https://meu.edu.jo/libraryTheses/%D8%A7%D9%84%D8%AA%D9%86%D8%B8%D9%8A%D9%85%20%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86%D9%8A%20%D9%84%D9%84%D8%B9%D9%85%D9%84%D8%A7%D8%AA%20%D8%A7%D9%84%D8%B1%D9%82%D9%85%D9%8A%D8%A9.pdf

تضمنت الدراسة تحديد ماهية العملات الرقمية وخصائصها وتحديد الطبيعة القانونية لها ومشروعيه التعامل فيها وتداولها في التشريع الضريبي وتطبيقاتها، وهي تختلف عن دراستي في ان دراستي تركز بشكل اساسي على الجرائم من المنظور التقني وكيفية قيام الجناة بارتكابها والاساليب الاجرامية بالاضافة لتأصيل الجريمة سواء التي تقع عليها او ترتكب باستخدامها

٢– دراسة بحثية بعنوان " جريمة التعامل في العملات المشفرة او النقود الرقمية " دراسة مقارنه– د/ محمد جبريل ابراهيم– منشور في مجلة البحوث الجنائية والاقتصادية – عدد مارس ٢٠٢٢ – العدد رقم ٧٩ – الركن الشرعي في التعامل بالعملات الرقميةوالركن المادي والمعنوي في التعامل بالعملات الرقمية والعقوبات المقررة لها وهي تختلف عن دراستي في انني قد ركزت في تناولي لهذة الجرائم على الاساليب الاجرامية

وهي تفيد المحققين بشكل اكبر من رجال الشرطة كما انها تعزز الفهم الخاص باساليب ارتكاب الجريمة وطرق التحقيق فيها سواء التي تقع على العملات ذاتها او التي ترتكب باستخدامها

٣- دراسة بعنوان "**الحاجةُ لمظلَّةٍ تشريعيَّةٍ لمارِد الدفع الرقمي الحاضر والمستقبل**" للباحثة هايدي عيسى – كلية الحقوق – جامعة القاهرة – القاهرة – مصر – منشور في مجلة جامعة الشارقة للعلوم القانونية – المجلد ١٧ العدد ٢ ديسمبر ٢٠٢٠ – وتناولت الدراسة ماهية العملات الرقمية وطبيعتها القانونية والتمييز بينها وبين العملات الأخرى ومميزاتها وعيوبها وتختلف هذه الدراسة عن دراستي في انها تتناول التعريف بالعملات الرقمية ومدى الحاجة لايجاد معالجة تشريعية لها بينما ركزت دراستي على الجوانب الفنية والاساليب التقنية الاجرامية المستخدمة في ارتكاب الاعتداء على العملات الرقمية المشفرة او استخدامها في ارتكاب الجرائم

مصطلحات الدراسة:

العملات الرقمية (Crypto Currencies):

هي تعبير الكتروني عن قيمة مالية لا تصدر عن السلطات المالية الرسمية للدول، ولا تتعلق بالعملات الورقية كالدولار او اليورو

المحفظة الرقمية (Digital Wallet):

وهي جهاز رقمي يتيح للمستخدم القيام بمعاملات رقمية كالشراء عبر الانترنت باستخدام حاسوب أو هاتف ذكي لاتمام عمليات الشراء والبيع.

وتتيح تلك المحافظ ربط الحساب المصرفي للمستخدم بمحفظتة الرقمية. ويمكن استخدامها كذلك في تمرير وثائق التفويض إلى محفظة الشخص الذي يتم التعامل معه عبر الاتصال باستخدام الخواص التقنية بالبلوتوث، كما يتم استخدام المحفظه الرقمية لمصادقة وثائق اعتماد مالكها.

٣- التعدين (Mining) :

يستخدم مصطلح التعدين في مجال العملات الرقمية لتوضيح اسلوب البحث عن العملات المشفرة عبر الانترنت باستخدام برامج مجانية تقوم بعمليات حسابية موثوقة،

(ISSN: 2356 - 9492)

تتطلب من المستخدم القيام بعمليات حسابية باستخدام خوارزميات معقدة لكشف سلسلة طويلة من العمليات تزداد تعقيدا كلما زاد انتاج العملات الرقمية، ليتمكن من اصدارها وتحويلها الى عملة في محفظة رقمية، يمكن استخدامها عبر الانترنت، وغالبا ما تكون تلك العملات باسماء غير حقيقية، وليس لها خصائص النقود التقليدية ، بالإضافة لعدم وجود غطاء قانوني لها، فيستطيع أي شخص لديه تجهيزات خاصة انتاجها._[٢]

خطة الدراسة:

مطلب تمهيدي: العملات الرقمية واستراتيجية دبي للتحول الرقمي

الفرع الأول: مفهوم الرقمنة والعملات الرقمية والمفاهيم ذات الصلة

الفرع الثاني: التعريف بالعملات الرقمية وتطورها

المبحث الأول: مخاطر استخدام العملات الرقمية في الجريمة

المطلب الأول: مميزات العملات الرقمية للجناة ودورها في إخفاء الأنشطة الاجرامية

الفرع الأول: مميزات العملات الرقمية للجناة

الفرع الثاني: دور العملات الرقمية في إخفاء الأنشطة الاجرامية

المطلب الثاني: جرائم الاحتيال والتعدين الخفي Crypto jacking

الفرع الأول: مخططات بونزي الاحتيالية

الفرع الثاني: جرائم التعدين الخفي Cryptojacking

المبحث الثاني: الجرائم التي تقع على العملات الرقمية

المطلب الأول: هجوم الدفع المضاعف Double-spend

المطلب الثاني: هجمات البنية التحتية وكسر خوارزمية الدمج SHA-256

الفرع الأول: هجمات البنية التحتية

الفرع الثاني : كسر خوارزمية الدمج SHA-256

المبحث الثالث: مستقبل العملات الرقمية بين الواقع والمأمول

(٢) أيمن عز الدين ابو صلاح – العملات الرقمية وعلاقتها بالتجارة الالكترونية" دراسة حالة: دولة الامارات العربية المتحدة –دبي"- رسالة ماجيستير – جامعة الشرق الأوسط – كلية الاعمال – قسم المحاسبة – ٢٠١٨م – ص٥ص١٦

المطلب الأول: المبادرة الإماراتية السعودية في العملات الرقمية

المطلب الثاني: نحو استراتيجية امنية في مجال المعاملات الرقمية

الفرع الأول: التحديات التقنية للتعاملات بالعملات الرقمية

الفرع الثاني: محاور مواجهة مخاطر استخدام العملات الرقمية

مطلب تمهيدي

العملات الرقمية واستراتيجية دبي للتحول الرقمي

تمهيد وتقسيم:

تظهر أهمية العملات الرقمية في ظل الرقمنة الذي تتطور الية كافة المعاملات والتعاملات سواء المالية او الإدارية وهو ما سوف يترتب علية اثارا عديدة تمس العديد من القطاعات منها القطاع الأمني باعتباره مرآة لأي تغيرات اقتصادية او غير ذلك حيث تنعكس تلك التحولات على الظواهر الاجرامية بلا شك وهو ما يستتبع دراسة هذه التغيرات وما يترتب عليها من اثار امنية وانماط جديدة من الجريمة والجناة وعلى ذلك سوف نقوم بدراسة العملات الرقمية واستراتيجية دبي للتحول الرقمي من خلال عدة أفرع على النحو التالي:

الفرع الأول: مفهوم الرقمنة والعملات الرقمية والمفاهيم ذات الصلة

الفرع الثاني: محاور استراتيجية دبي للتعاملات الرقمية

الفرع الثالث: التعريف بالعملات الرقمية وتطورها

الفرع الأول: مفهوم الرقمنة والعملات الرقمية والمفاهيم ذات الصلة

أولا: تعريف الرقمنة

هو عملية انتقال إلى نموذج عمل يعتمد على التقنيات الرقمية في تنفيذ الاعمال وتقديم الخدمات، وتوفير قنوات جديدة من العائدات، وقد بينت العديد من الأبحاث العلمية الجديدة أن الشركات سوف تستثمر مبالغ هائلة في المرحلة المقبلة في تحديث وسائل الرقمنةالتقنية. وهذه الاستثمارات تتطلبها التعقيدات الكبيرة والمتطورة في نظم المعلومات بخاصة في الأجهزة وتطبيقات نظم المعلومات والرغبة في مضاعفة القدرة الإنتاجية للموظفين المعتمدين بشكل كبير على موثوقية نظم المعلومات. ولعل السبيل

(ISSN: 2356 - 9492)

الى الحفاظ على الميزة التنافسية لنظم المعلومات يجب الاعتماد على نظم المعلومات فتكون القدرة على العمل ذات الانتاجية الأعلى هي محور العملية الإنتاجية

ثانيا: أهمية الرقمنة:

١ – الرقمنة وانترنت الأشياء

تشهد أعداد الأجهزة المتصلة بإنترنت الأشياء تزايدا هائلا حيث تبلغ الان ما يقارب تسعه مليار جهاز، ويتصور وصول الرقم الى مئات المليارات .ووفقا لمؤشر سيسكو للتواصل الشبكي، يتوقع اتصال ما يزيد عن ٥٠٠ مليار جهاز وشيء بالإنترنت عام 2030، لذا تعتبر مرحلة الرقمنةالحالية الاهم على الاطلاق، وسوف يحقق الاضطراب الرقمي في قطاع الأعمال حالياً تغيرات جذرية في الاقتصاد وجوانب الحياة المختلفة. لذا فان الرقمنةيوجب على الشركات والهيئات المختلفة ضرورة الاستفادة من إنترنت الأشياء لتصبح أكثر فهما وامكانية على التوقع والمرونة في العمل وهو ما سيساعدها على الابتكار بشكل أكثر سرعة وايجابية للوصول للنتائج الايجابية لأعمالها، من خلال تطبيق الإطار الرقمي باستخدام تكنولوجيا المعلومات .وسيحتاج العدد الهائل من الأجهزة المتحركة وإمكانات الاتصال بالإنترنت والخدمات الرقمية في كافة القطاعات لشبكات تقنية متطورة وضخمة للقيام بتلك المهام .ومن خلال التواصل الرقمي بين الفاعلين والبيانات والأشياء، فإن إنترنت الأشياء يمكنه تسريع التغيير [٣]

٢ – الرقمنة ضرورة في تعزيز كفاءة الأداء المؤسسي:

أصبح الرقمنة من الضروريات بالنسبة لكافة المؤسسات والهيئات التي تسعى إلى التطوير وتعزيز خدماتها وتسهيل وصولها للمستفيدين، والرقمنةلا يعني فقط تنفيذ العمليات داخل المؤسسة بشكل رقمي بل هو برنامج متكامل لإدارة المؤسسة يعمل على تطوير وتغيير إدارة العاملين والاعمال وكذا تسريع وتيسير أداء تلك الخدمات ، وينصب الرقمنةعلى سبل استخدام الوسائل التقنية داخل المؤسسات العامة او الخاصة ، فهو يساعد على تعزيز الكفاءة التشغيلية وتعزيز الخدمات التي تقدمها للعملاء والجمهور

(3) Vittorio Aronica & others, digital transformation Leading our customers towards a new economy of digital ecosystems, pp:11-15, 2018, www.eng.it

، فيعمل على تحقيق الاستخدام الأفضل للتقنية لتحقيق الجودة في العمل وكذا في الخدمة التي يحصل عليها الجمهور فيوفر الوقت والجهد ، وقد صار الرقمنةضرورة حتمية في ظل التطور الكبير في استخدام التقنية الرقمية المعلوماتية في جوانب الحياة المختلفة سواء المؤسسية او على مستوى الافراد.

٣-<u>الجوانب الايجابية لرقمنة الصناعة:</u>

أ- ابتكار نهج صناعي مُطور يتماشى مع تكنولوجيات الصناعة الحديثة

ب- استخدام التقنيات الحديثة في كل التخصصات والمجالات والاقتصادات والصناعات

ت- استخدام تقنية المعلومات في الصناعة يوفر الوقت والنفقات ويحقق زيادة في الانتاج

ث- ظهور المؤسسات الصناعية التي تستخدم تقنية المعلومات في الانتاج والتي تتنبأ بالأعطال

ج- إنجاز مراحل الإنتاج بما يقلل الهدر في مدخلات الإنتاج مما يعظم الإيرادات ويخفض تكاليف الإنتاج

ح- تحقيق التواصل بين الصناعة والمدارس والجامعات ومراكز البحث العلمي لتقديم حلول ابداعية لتعظيم الناتج الصناعي

<u>ثالثا: جوانب الرقمنة:</u>

١-المدن الذكية: هي تلك المدن التي تدار فيها المرافق باستخدام التكنولوجيا الرقمية الذكية ويتم اتخاذ القرارات وبناء السياسات الخاصة بادارتها ومواجهه المشكلات فيها باستخدام علوم البيانات وتحليلها لتعزيز رفاهية الحياة فيها ورفع قدرات الخدمات والتنافسية.

٢-السياحة الذكية: تعتمد على تكنولوجيا الاتصالات اولمعلومات لدعم السياحة بتعزيز تجارب السائحين.

٣-رعاية جيل المستقبل: تستفيد من إجراءات الوقاية المناسبة للافراد اعتمادا على تكنولوجيا المعلومات والاتصالات لتوفير تجربة متميزة للمرضى.

(ISSN: 2356 - 9492)

٤-**المؤسسات التعليمية في المستقبل:** تقدم المؤسسات التعليمية في المستقبل نموذجاً لرقمنة نظم التعليم وتوفر فرصة الحصول على تجربةمتميزة وفريدة في التعلم.

٥-**الحكومة الذكية:** وتشير للاعتماد على تكنولوجيا الاتصالات والمعلومات عند تحديد السياسات وتقديم الخدمات واتخاذ القرارات.

٦-**مستقبل الانتقالات** :يوضح مستقبل الانتقالات شكل البنية التحتية الفيزيائية والرقمية والخدمات التي ستعزز قدرات تحرك الأفراد ونقل البضائع بشكل أمن وسريع ومريح واقل تكلفة ويعتمد على التكنولوجيا المتطورة في تسهيل التنقل وحل المشكلات المتعلقة به.(٤)

كما سيرتبط التنقل بسرعة البت والبايت ولن يرتبط بشكل او باخر بالبنية التحتية المادية وستساهم التكنولوجيات الجديدة في تعزيز مستوي السلامة و الكفاءة والحد من الازدحام المروري وسيصبح التنقل مرتبطا بالاتي:

أ- التنقل العصري الرقمي :مثل سيارات النقل الجماعي والسيارات ذاتية القيادة وإدارة حركة وسائل النقل وخدمات النقل عبر الإنترنت كالمواقف الذكية ورسوم الطرق الذكية وإشارات المرور الذكية واللافتات الذكية على الطرق)

ب- الابتكار في التكلفة والتمويل واساليب الدفع: ستوجد نماذج للتسعير الالي القائم على بيانات المستشعرات وبطاقات السفر ونماذج النقل

ت-ظهور وسائل النقل البديلة :مثل السيارات ذاتية القيادة وصديقة البيئة والدراجات الكهربائية

ث- إحداث نقلة نوعية في المطار:ات وتتمثل في ابتكار طائرات ذاتية القيادة ومطارات قائمة على تكنولوجيا الواقع المعزز والخدمات الذاتية وتطبيقات السفر عبر الهاتف الذكي

رابعا: فوائد الرقمنة:

(٤)) إيمانويل دورو واخرين – ديلويت" الرقمنة في الشرق الأوسط "رحلة رقمية" – ص٤١ص٤٤– متاح على شبكة الانترنت على الرابط:
e.huawei.com/ae/edm/global/NationalTransformationInTheMiddleEast

١-له فوائد كبيرة للعملاء والجمهور والمؤسسات والشركات

٢-يوفر الرقمنةالنفقات والجهد بشكل كبير

٣- يُحسن القدرة التشغيلية ويعيد تنظيمها بما يعظم الاستفادة

٤-يعمل على تعزيز الجودة وتبسيط الإجراءات للحصول على الخدمات المقدمة للمستفيدين

٥- يخلق فرص لتوفير خدمات ابداعية متميزة تحقق رضاء الجمهور المستهدف

٦-يساعد الرقمنةالمؤسسات والشركات على التوسع والانتشار في نطاق أوسع والوصول إلى شريحة أكبر من العملاء والجمهور

خامسا: حوكمة الرقمنة:

ترتب على التطور التقني وتعاظم استخدام المعلومات لتطور القدرة على السيطرة والاستفادة من تطبيقات التكنولوجيا التي انتشرت في شتى مجالات العمل وعلى جميع المستويات بصورة أصبحت ضرورية للتقدم والأداء الفعال للعمل بالرغم من المخاطر ومع انتشار التقنية تعاظمت اهمية الترابط بين التكنولوجيا والحوكمة والأعمال وظهرت مفاهيم جديدة تسهم في تطوير بيئة الأعمال ، منها حوكمة الرقمنةوالحوكمة التقنية وإدارة المخاطر وهيكلة العمليات والتصميم التكنولوجي، ، وبرزت هذه المصطلحات بصورة هامة وحيوية مترافقة مع استراتيجيات تطوير المؤسسات ومحاربة الفساد، ويُعد الرقمنةإطارًا هاما لنجاح الأعمال حيث يُعيد تشكيل أساليب الحياة اعتماداً على التقنيات وتطوراتها مع التخطيط المستمر والسعي الدائم لإعادة صياغة الخبرات العملية .ولأن الوصول إلى الخبرات التراكمية للإنسان أصبحت أسهل فإن إعادة التشكيل اعتمادا عليها صارت أبسط وأكثر فعالية حتى تحول ما اعتدناه والخبرات العالمية يتم تقييمه من حيث الرقمنة واعيد صياغة الخبرات وتضاف التعزيزات وتغيرت الأولويات من خلال تحليل مختلف للمعلومات وتغذية عكسية من مؤشرات الأداء كما ان ردود أفعال المستخدمين تُساعد الحوكمة في ضبط منظومة التفاعل مع المتغيرات المحيطة بالرقمنةحيث تتداخل مكونات مختلفة كالشركات المساندة وأنظمة الأعمال والوسائط التفاعلية بشكل مباشر أو غير مباشر لاستكمال العمليات والإجراءات .وتتدخل حوكمة

(ISSN: 2356 - 9492)

الرقمنةفي ضبط وتحليل تأثير التغير في العناصر القابلة للتغيير والتعديل والتطوير . وبهذا تسهل الأعمال بما يواكب التطور ويضمن التوازن بين الاطراف والحفاظ على الأهداف وخلق فرص جديدة(٥)

سادسا: تطبيقات الرقمنة

يطبق الرقمنةمن خلال:

١ – التكنولوجيا

يتم تنفيذ الرقمنةبواسطة مجموعه من الأجهزة، وقواعد البيانات ووسائط تخرين المعلومات وتحليل البيانات والبرامج التي يمكنها تحقيق الاهداف بما يحقق استدامه في استغلال الأصول .كما يتطلب تحقيق جودة مناسبة في الخدمات المقدمة لأفراد المؤسسة وعملائها وموردیها عبر مجموعات متخصصة مسؤولة إدارة النظام المعلوماتي الرقمي

٢ – البيانات

تقوم المؤسسات بإدارة وتحليل البيانات بما يحقق إيجاد معلومات وبيانات ذات موثوقية وتكاملية مع القدرة على التحليل الاحصائي لتلك البيانات للتنبؤ بالمستقبل لوضع خطط استراتيجية قائمة على أسس عليمة يمكن من خلالها تقليل المخاطر وزيادة المنفعة المتحققة من الموارد المتاحة

٣ – العنصر البشري:

يعد العنصر البشري من العناصر اللازمة لتنفيذ الرقمنةحيث يحتاج الرقمنةالى العنصر البشري لتنفيذه ويلزم كذلك توافر سمات الكفاءة والمهارة في التعامل مع البيانات والمعلومات وتحليلها واستخلاص النتائج منها وذلك حتى يمكن اتخاذ القرارات الصحيحة التي تحقق النتائج المرجوة كما ان توضع الاستراتيجيات يتطلب العنصر البشري وكذا تنفيذ تلك الاستراتيجيات

٤ – العمليات

(٥)) المبادئ الأربعة للاستشارات الإدارية – النهج اللين في الرقمنة- ٢٠١٧م – ص٢ص١١- متاح على الموقع الالكتروني: www.fourprinciples.com

يجب على المؤسسات إرساء بناء تقني فعال يسمح بتطوير الأداء داخليا وخارجيا وذلك حتى يمكن تحقيق تطبيق فعلي للتحول الرقمي وفي سبيل ذلك يلزم اعداد بنية تحتية رقمية تتضمن في مكوناتها أنشطة المؤسسات وعملياتها التقنية وكذا التطبيقات الرقمية ومعالجة البيانات(٦)

سابعا: الرقمنة في المجال المالي:

أصبحت تقنيات البلوك تشين، وتقنية القياسات الحيوية، والذكاء الاصطناعي، وتقنيات الواقع المعزز من المتوقع لها أن تسود لسنوات قليلة حيث انه لم تكن الاعمال المصرفية تواجه تحديات رقمية في كل عناصر إيراداتها. في ظل التعاملات التقليدية بينما أدى استخدام تقنيات مثل الند للند للدفع المباشر، وسلاسل الكتل الذي يتم باستخدامها الوفاء باستخدام العملات المشفرة ، إلى حدوث تحول في طرق تخزين القيمة، وتداولها والتعامل فيها .وبرغم ذلك فقد لاقت رواجا كبيرا واقبالا على استخدامها ووضعت البنوك العديد من الوسائل التي يمكن بواسطتها تأمين التعامل بها.(٧)

ثامنا: معوقات الرقمنة

١- نقص الكفاءات القادرة على قيادة برامج الرقمنةوالتغيير

٢- عدم كفاية الميزانيات المخصصة لهذه البرامج

٣- التخوف من مخاطر استخدام الوسائل التكنولوجيا

تاسعا: الرقمنة والامن:

تعتبر إجراءات الأمن والحماية اساس المدن .وقد شغل قطاع تكنولوجيا المعلومات أهمية متزايدة لدورة الهام في تحقيق الأمن سواء الفعلي أو الرقمي .فمن الناحية الفعلية،

(٦) تقرير فيوتشر بيرفكت ١٠ - مشروع بحثي مقدم من قبل ذراع حلول المحتوى لمجلة" تكنولوجي ريفيو "الصادرة عن معهد" ماساشوستس للتكنولوجيا (MIT Technology Review "بالتعاون مع القمة العالمية للحكومات – ٢٠١٨ م – ص١٥ص١٧ متاح على الموقع الالكتروني:
https://www.iccia.com/sites/default/files/library/files/Future%20Perfect%2010%20Reports_Arb_Low%20res.pdf

(٧) الدكتور /عدنان مصطفى البار – تقنيات الرقمنة – دراسة منشورة على شبكة الانترنت على الموقع الالكتروني: (www.kau.edu.sa › GetFile)

(ISSN: 2356 - 9492)

يتم اللجوء إلى تقنيات مثل التحكم عن بعد والتعرف على الوجوه والتحليلات التنبؤية لحماية المدينة وقاطنيها من الأذى وتساهم تقنيات الحماية في حماية بيانات الشركات والأفراد في المدينة كمكافحة سرقة الهوية والسرقات المالية وتعد إجراءات الأمن أولوية كبرى في مبادرات الرقمنة التي اطلقت عدد من المبادرات الرقمية لتطوير حماية اذكى واقوى لمكافحة ومنع الجريمة، وتتمثل في أنظمة الإنارة الذكية التي تعزز الحماية الأمنية بزيادة نسبة الإنارة، كما أطلقت شرطة دبي مؤخراً جهاز التحكم الذكي الذي يقدم المساعدة للموظفين في أقسام المرور ويمكنهم من الحفاظ على سلامة الطرقات وتعزيز المراقبة الإلكترونية وتحديد المخالفات بالإضافة للتحول نحو مراكز الشرطة الذكية (SPS).[٨]

الفرع الثاني

التعريف بالعملات الرقمية

أولا: ماهية العملات الرقمية

يعرف البعض العملات الرقمية بأنها: «عملة رقمية لامركزية غير معتمدة تستخدم طريقة "beer to beer" والتوقيعات الإلكترونية والتشفير وذلك لإثبات وتمكين المستخدمين من نقلها وتداولها عن طريق الانترنت بغير وسيط أو جهة خارجية موثوقة مثل البنوك». ويرى البعض الآخر أنها " نقود رقمية تتداول عبر الإنترنت "P2P"، ويمكن للمستخدم تخزينها وتبادلها من خلال تطبيق مجاني".

وهي لا تحمل اي أرقام تسلسلية وليست مدعومة حكوميا كالعملة الورقية، ويتم تداولها عبر الانترنت بمعنى أنها غير محسوسة وليس لها وجود فيزيائي. وتقارن بالعملات الأخرى كالدولار واليورو ويمكن استخدامها للشراء عبر الإنترنت أو تحويلها إلى العملات التقليدية عن طريق المبادلة، وتسمح للمُستخدمين بإرسال مبالغ مالية لبعضهم على الإنترنت دون الحاجة لسلطة تراقب الدفع وتحويل الاموال، مع المحافظة

(٨) إيمانويل دورو واخرين – ديلويت" الرقمنة في الشرق الأوسط "رحلة رقمية" – ص١٦ص١٨– متاح على شبكة الانترنت على الرابط:
e.huawei.com/ae/edm/global/NationalTransformationInTheMiddleEast

على عدم إمكانية تتبعها. كما لا تتطلب العُملات الرقمية وجود حسابات، بل يكفي تحميل التطبيق الخاص بها وهو يقوم بتوليد "العناوين" المستخدمة لإجراء التحويلات. فالعملات الرقمية لا تظهر عند تنصيب التطبيق، ويمكن الحصول على العُملات الرقمية عبر عملية التنقيب، وهي عملية شاقة وطويلة غير مضمونه النتائج دون الاستثمار في مُعدات التنقيب الخاصة بذلك.(٩)

ثانياً: خصائص العملات الرقمية

لا تخضع العملات الرقمية للأطر القانونية، ولا تصدر ها البنوك الحكومية المركزية، ولا يمكن ان يتم السيطرة عليها من الحكومات، بسبب وجودها على الإنترنت واستخدامها من قبل مستخدمي الألعاب الالكترونية والشبكات الاجتماعية كوسيلة لتداول السلع الرقمية ، وقد أصبحت العملات الرقمية تستخدم في السداد الالكتروني الشراء من المتاجر الالكترونية ، وتعد العملات الرقمية وسيط للوفاء بالقيمة ووحدة للحساب على النحو التالي:

١- وسيط للتبادل : تستخدم العملات الرقمية كوسيط للتبادل من خلال اعتبارها آلية للدفع بدلاً عن العملة التقليدية.

٢- مخزن للقيمة (Store of Value)، تتميز العملات الرقمية بتقلب أسعارها، ولذا يشكك العديد من الاقتصاديين في قابلية العملات الرقمية مثلا لأن تكون مخزناً مستقراً للمحافظة على القيمة، لكن التغيير في قيمتها يرتبط بالنظام اللامركزي لها، حيث يصعب السيطرة على معاملاتها أو تثبيت قيمتها عندما يتغير مستوى العرض أو الطلب.

٣- وحدة حساب (Unit of count)،(١٠) ويقتصر ذلك على مستخدمي العملات الرقمية، ولا يحدث خارجه، حيث لا يمكن لكافة الأفراد الدفع به، فأسعاره ليست مقومة ،

(9) Dong He, Karl Haber Meier & others , Virtual Currencies and Beyond: Initial Considerations,2016,pp:7-8

(١٠) مثال ذلك ما قام به البنك المركزي الصيني في عام ٢٠١٣ بحظر التعاملات بعملة "بتكوين"؛ مما خفض من الطلب الكلي عليها وخفض أسعارها في ذلك الأسبوع بنسبة ٥%. وفي العام اللاحق تم الحظر أيضاً من قبل البنك المركزي الروسي؛ مما خفض الأسعار بـنسبة ١٠% أخرى

(ISSN: 2356 - 9492)

فلا يعد وحدة حساب، ويمكن القول إن نظام العملات الرقمية يختلف تماما عن أنظمة البنوك المركزية التي تؤثر على العرض والطلب للعملات، ويشكل الموقف السلبي لهذه البنوك من العملات الرقمية عائقا لانتشاره.(١١)

ثالثاً: أسباب جاذبية على العملات الرقمية

تتمتع العملات الرقمية بقبول واسع لدى ملايين الأشخاص في العالم على الرغم من بعض العيوب، وعدم توافق الاقتصاديين على توفر المعايير المستقرة لها مثل العملات التقليدية، **ومن أبرز أسباب ذلك: .**

١ . **الحفاظ على السرية:** يتضمن نظام العملات الرقمية درجة عالية من إخفاء هوية المستخدمين، فعلى دفتر الأستاذ الخاص بها يتم فحص الرموز الخاصة بالعمليات التي يتم اجراءها للتيقن من تفردها، ولا يقوم المتعاملين بالتعريف عن هوياتهم في عمليات الوفاء بالعملات الرقمية.

٢ . **استخدام العملات الرقمية خلال الأزمات الاقتصادية:** فخلال أوقات الأزمات الاقتصادية، فقد العملة الوطنية لقيمتها السوقية أو تراجعها، تحتفظ العملات الرقمية بقيمتها؛ ما يجعلها تستخدم كبديل عن العملة التقليدية. لذا استخدم بعض مواطني الأرجنتين العملات الرقمية للحفاظ على اموالهم في حالات التضخم كبديل للعملة الوطنية.

٣ . **قلة تكلفة المعاملات لعدم وجود وسيط:** تعتبر العملات الرقمية اهم ادوات التجارة الإلكترونية حيث لا تكلف المعاملات بها شيئا، فلا توجد حاجة للاعتماد على البنوك لتسهيل المعاملات المالية، وهو الأمر الذي يقدره أطراف المعاملة. وبينما يقوم مستخدمي بطاقات الائتمان بتحمل ٢% إلى ٣%من قيمة المعاملة، فإن استخدام العملات الرقمية يكاد الا يكلف المستخدمين أي نفقات ولذلك فإن نظام العملات الرقمية

(١١) ايمن عز الدين أبو صلاح – العملات الرقمية وعلاقتها بالتجارة الالكترونية "دراسة حالة " دولة الامارات العربية المتحدة (دبي) – رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجيستير في المحاسبة – جامعة الشرق الأوسط – عمان – الأردن – ٢٠١٨م- ص١٣ص١٤

أفضل من بطاقات الائتمان في تشجيع المعاملات الإلكترونية بسبب عدم وجود وسيط، واستفادة المستخدم بعدم تحمل أعباء اضافية.

وعلى مستوى النمو الاقتصادي، يلاحظ أن نظام العملات الرقمية يشجع، التجارة الإلكترونية، وتوليد اشكال جديدة من التجارة، فقد نشأت شركات تحقق فرصاً لمقايضة العملات الرقمية بعملات مالية والعكس، وكذلك تأسست شركات لتبادل العملات الرقمية بسلع وخدمات أو تحويلها من شخص لآخر.

٤-**الألعاب الالكترونية تستخدم العملات الرقمية.** واحدة من أشهر ألعاب الطاولة في العالم، وهيMonopoly ، التي نشرتها شركةParker Brothers ، وتستخدم عملتها الخاصة داخل اللعبة، والتي يطلق عليها ."Monopoly Money" وهي فعالة داخل اللعبة، ولكنها ليس لها قيمة في العالم الحقيقي ونظرًا لأن العملات الرقمية غير موجودة في شكل أوراق نقدية أو عملات معدنية، فلا يمكنك إخراجها من محفظتك واستخدامها لشراء فنجان قهوة. فهي أنها موجودة فقط كسلسلة من الأحرف الرقمية، ولكي تقوم بشرائها أو بيعها أو استخدامها، يجب أن يكون لديك "محفظة رقمية". أما ليندن دولار فلا تتداول إلا في عالم الألعاب الالكترونية ، كلعبة (Second Life)،[١٢] والتي طورها مختبر ليندن ، وتعد أكثر الألعاب الرقمية شيوعاً.

ويمكن للاعبين توليد مكاسب حقيقية من أرباح اللعبة في العالم الافتراضي؛ وذلك لإمكانية تحويل "ليندن دولار" لأي عملة حقيقية عبر استخدام شركة الصرافة (Exchange business)، والتعامل بها في الحقيقة.

(١٢) هي لعبة الكترونية تم اطلاقها بشكل ثلاثي الأبعاد علي الإنترنت في العام ٢٠٠٣ كحياة ثانية موازية للحياة الانسانية علي الأرض ، أطلقتها شركة ليندن لاب في امريكا ، ذكرت صحف امريكية أن مصممي أزياء حققوا مبالغ كبيرة من تصميم أزياء افتراضية لساكني هذا العالم الافتراضي ، افتتحت عدة شركات عالمية فروع لها هناك فضلاً عن دولة السويد التي قامت بافتتاح سفارتها في لعبة الحياة الثانية وقام بافتتاحه وزير خارجيتها كارل بيلت ولوكالة رويترز وبي بي سي مكاتب هناك ويوجد في برنامج الحياة الثانية الكثير من الجامعات الخاصة والعامة، وبعضها مرتبط بالجامعة فعلياً والبعض يقومون بعمل تطوعي ، وفي لعبة الحياة الثانية تم إنشاء أول جامعة عربية وإسلامية وهي جامعة الملك سعود الافتراضية وتقدم دروس تعليمية في عدة تخصصات ويشرف عليها خبراء واكاديميين متخصصين ، وقد تميزت جامعة الملك سعود بتصميم فريد ومبتكر ، واستغرق تصميمها أكثر من (الف) ساعة عمل.

(ISSN: 2356 - 9492)

وتكمن المشكلة في استخدام "ليندن دولار" خطورتها بسبب المعاملات التي تتيسر التهرب من الالتزامات القانونية، حيث تستخدم في الاعمال التجارية في بورصة رقمية تسمى (LindeX exchange) .

٥- وفي ظل وجود أجهزة كمبيوتر متخصصة والدوائر المتكاملة الخاصة بالتطبيقات ، أو "ASICs" التي تم تعزيزها لإجراء الحسابات الرياضية اللازمة لإنتاج العملات الرقمية في السنوات الأخيرة ، استخدم المجرمون "botnets" لإجراء عمليات التعدين.

واستخدمت تطبيقات البرامج للأجهزة المحمولة التي تستخدم معالج الجهاز المحمول، لاستخراج العملات الرقمية، ومع ظهور الآلات المتخصصة فإن أرباح التعدين ذهبت إلى المؤسسات التي استخدمت اجهزة تعدين للعملات الرقمية.

٦- لا يتم إصدار عملات العملات الرقمية من السلطات المركزية بل يتم شراؤها من الوسطاء ، حيث يقبل مبادلو العملات الرقمية العملات التقليدية ويقومون بتبادلها مقابل عملات رقمية وفقا لسعر صرف متغير.

٧-يتم تخزين عملات العملات الرقمية في محفظة رقمية مرتبطة بـ "عنوان العملات الرقمية للمستخدم"، وهو مشابه لرقم الحساب المصرفي، والذي يحدد بسلسلة معقدة من الحروف والأرقام، وتأخذ شكل البلوك تشين."[١٣]

(١٣) ايمن عز الدين أبو صلاح – العملات الرقمية وعلاقتها بالتجارة الالكترونية "دراسة حالة " دولة الامارات العربية المتحدة (دبي) – رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجيستير في المحاسبة – جامعة الشرق الأوسط – عمان – الأردن – ٢٠١٨م- ص١٦ص١٨

رابعا: تطور العملات الرقمية

العملة	الشرح
١- ظهور خوارزمية الـ آر إس إيه RSA عام ١٩٧٧	تعد خوارزمية تشفير تم ابتكارها عام ١٩٧٧، عند قيام رونالد ريفست واثنين من معهد ماساتشوستس للتقنية بنشرها، سميت بالأحرف الأولى لأسماء للثلاثة ، وتعد هذه الخوارزمية علامة فارقة في تاريخ العملات الرقمية، لأنها تمكن المستثمرين في العملات الرقمية من تلقي الإيرادات.
٢- ديفيد تشوم يخترع ecash (١٩٩٣)	Ecashهي عملة رقمية ابتكرها عالم الرياضيات ديفيد تشوم عام ١٩٩٣ وفقا لبروتوكولات التشفير، وتعد احد النماذج الاولى للعملات الرقمية ، وبحلول عام ١٩٩٧ قام بجمع أموال لتنفيذ فكرته ، وانشأ شركة "DigiCash" لإدارتها ، إلا أن الشركة أفلست، وعلل ذلك بصعوبة قبول هذه العملة من المتعاملين.
٣- دوجلاس جاكسون يطلق الذهب الإلكتروني (١٩٩٦)	عام ١٩٩٦م أطلق جاكسون الذهب الإلكتروني " E-Gold" ، والتي اعتبرت عملة دولية تتداول استقلالا عن رقابة السلطات، وذلك من خلال فتح حساب على موقع الشركة ، بحلول عام ٢٠٠٥م كان هناك ٣,٥ مليون حساب في ١٦٥ دولة، واستفاد المجرمين من هذا النظام في غسيل الأموال، حيث قامت أجهزة الامن بالقبض على جاكسون، وتم اتهامه بغسل الأموال، مما أعاق تداول تلك العملات.
٤- Hashcash (١٩٩٧)	ابتكر ادم باك عام ١٩٩٧م هذه العملة للسيطرة على رسائل البريد الإلكتروني المزعجة، وقد أصبحت

(ISSN: 2356 - 9492)

	تستخدم في البت كوين وغيرها من العملات الرقمية وكانت جزءا من خوارزمية تعدين عملات جديدة.
٥- b-money (١٩٩٨)	في عام ١٩٩٨ وضع خريج علوم الكمبيوتر " we day" الأساس للعملات الرقمية، من خلال نشره مخطط عمل للعملة الإلكترونية " b-money" على قائمة بريدية عبر الإنترنت، وكان داي يهدف إلى تمكين الاقتصادات الإلكترونية غير القابلة لفرض ضرائب عليها، وساعدت فكرة هذه العملة في ابتكار البت كوين.
٦- باي بال (١٩٩٩)	كان لموقع باي بال أهمية كبيرة في تمكن المستخدمين من نقل أموالهم عبر الإنترنت، وتميز بشعور مستخدميه بالراحة عند تحويل الأموال عبر الإنترنت، مما ابرز فكرة العملات الرقمية.
٧- برنامج تور (٢٠٠٣)	حيث يوفر البرنامج الخصوصية من خلال السماح للمستخدمين بالتمتع بالمجهولية ، وعدم امكانية تعقبهم حال اجراء المعاملات بالعملات الرقمية باستخدام عنوان " IP"
٨- هال فيني يكشف عن بروتوكول قابل لإعادة الاستخدام (٢٠٠٤)	وهو تدبير مادي لمنع هجمات انكار الخدمة والبريد المزعج على الشبكات، ويعد مقدمة لظهور العملات الرقمية.
٩- ساتوشي ناكاموتو ينشر ورقة العملات الرقمية٢٠٠٨	نشر ناكاموتو أكتوبر ٢٠٠٨ ورقة بشأن عملة البت كوين، وتضمنت شرح لطريقة تحويل الأموال خارج المؤسسات المالية والسلطات الحكومية.
١٠- ناكاموتو ينشئ بلوك	الـ"بلوك شين" هو سجل لتبادل العملات الرقمية، والذي

تشين (٢٠٠٨)	يتيح تبادلًا آمنا للمواد القيمة كالأموال أو الأسهم أو حق الوصول للمعلومات، دون وسيط أو نظام مركزي لحفظ المعلومات لمتابعة عملية التداول.
١١- التعدين الأول للبت كوين (٢٠٠٩)	في يناير ٢٠٠٩ قام ناكاموتو بتعدين ٥٠ عملة رقمية.
١٢- العملات الرقمية يتساوى مع الدولار (٢٠١١)	في ٩ فبراير ٢٠١١ قفزت العملات الرقمية وتساوت مع الدولار على بورصة " MTGOX" لتداول العملات الرقمية، وظلت قيمتها تتزايد.
١٣- إصدار عملة نيم كوين ونظام DNS اللامركزي (٢٠١١)	عقب نجاح العملات الرقمية إصدار بعض المبرمجين عملات رقمية أخرى ، منها نيم كوين التي أنشأها فنسنت دورهام، وأعلنت في ٢٠١١، حيث أضاف مطوروها ميزة تمثلت في منظومة "DNS "، التي اتاحت للمستخدمين حفظ المعلومات الشخصية بشكل امن.
١٤- إصدار عملة الريبل	طورها آرثر بريتو واثنين اخرين واطلقت عام ٢٠١٢، واستخدمت كعملة وشبكة رقمية للمعاملات المالية الالكترونية، وتميزت بقبول العملات التقليدية والرقمية.
١٥- إصدار بيركوين (٢٠١٢)	تميزت عن العملات الرقمية بأنها أول عملة استخدمت البروتوكول المشترك، مما ساعد على تعدين كميات كبيرة من العملات المشفرة دون باقل استهلاك من الكهرباء.
١٦- العملات الرقمية تتجاوز قيمتها مليار دولار (٢٠١٣)	عام ٢٠١٣ بلغ عدد العملات الرقمية المتداولة ١١ مليون عملة، وارتفعت قيمة الواحدة منها إلى ٩٢ دولارًا، مما أدى إلى تجاوز القيمة الكلية لها المليار

(ISSN: 2356 - 9492)

	دولار.
١٧- فتح أول ماكينة صرف العملات الرقمية (٢٠١٣)	تم فتح أول ماكينة صرف آلي للعملات الرقمية في مدينة فانكوفر في أكتوبر ٢٠١٣، والتي تتيح للمستخدمين تحويل العملات الرقمية إلى عملات تقليدية.
١٨- بورصة بي.تي.سي تشاينا توقف التداول باليوان (٢٠١٣)	صرحت بورصة بي.تي.سي تشاينا لتداول العملات الرقمية في الصين عام ٢٠١٣ بعدم قبولها ايداعات باليوان، مما أدى لانخفاض قيمة العملات الرقمية من ١٢٠٠ دولار إلى ٥٧٢ دولارًا على بورصة " MtGox"، الا انها عادت وسمحت في ٢٠١٤ بقبول اليوان ثانية.
١٩- كلية نيقوسيا تستخدم العملات الرقمية لسداد الرسوم الدراسية (٢٠١٣)	جامعة نيقوسيا القبرصية قبلت سداد رسوم الدراسة بها بالعملات الرقمية عام٢٠١٣ كأول جامعة تقوم بذلك في العالم، لتقليل مصاعب تحويل بعض الطلاب اليها.
٢٠- موقع " Overstock" يقبل التعامل بالعملات الرقمية (٢٠١٤)	أصبح موقع "Overstock " أوائل عام ٢٠١٤م أول موقع للتجارة الالكترونية يقبل السداد بالعملات الرقمية، وفي وقت لاحق قبل الموقع العملات الرقمية في كافة مواقعه.
٢١- اختراق بورصة " MtGox" (٢٠١٤)	تعرضت هذه البورصة للاختراق عدة مرات حيث تم اختراقه عام ٢٠١١، وتسبب ذلك في غلقه لأيام وخسارة ٨,٧٥ مليون دولار، ثم تم اختراقه مجددا في عام ٢٠١٤ مما أدى لخسارة ٨٥٠ ألف من العملات الرقمية أي نحو ٤٠٠ مليون دولار في ذلك الوقت، وقد

	أدى ذلك إلى إفلاس الشركة في النهاية.
٢٢- إطلاق الإثيريوم (٢٠١٥)	في عام ٢٠١٥ أطلق المبرمج الروسي عملة ومنصة الإثيريوم، وهي منصة لإنشاء العقود الذكية بشكل آمن، وقد أدى نجاحها الكبير لوصول قيمتها السوقية إلى ٢٨ مليار دولار.
٢٣- قيمة العملات الرقمية تتجاوز الذهب (٢٠١٧)	في منتصف سبتمبر الماضي وصل سعر أوقية الذهب إلى ١٣٣١,٦٠ دولار، في حين بلغت قيمة العملة الرقمية الواحدة ٣٣٦٣,٤٢ دولار.
٢٤- شركة LedgerX (٢٠١٧)	اصبحت شركة LedgerX LLC أول منصة لتداول العملات الرقمية تحصل على موافقة لجنة تداول السلع الآجلة الامريكية، ان تكون بورصة للعقود الذكية بالعملات الرقمية.
٢٥- روسيا تتجه لتقنين العملات الرقمية (٢٠١٧)	حظرت السلطات الروسية عام ٢٠١٦ التعامل بالعملات الرقمية ، واقترحت عقوبات للمخالفين تصل للسجن ٧ سنوات، ثم تغير موقفها عندما قررت تقنين استخدام العملات الرقمية.(١٤)

خامسا: مخاطر العملات الرقمية

تعتبر العملات الرقمية في طور النشأة كما أن استقرار العملات وثقة المستخدمين بها يتطلبان وقتا، وهو ما تم عند التحول من نظام المقايضة للنقود، وما تم عند بدء التعامل بالعملات الورقية بالإضافة للمعدنية ، ولهذا لايزال التعامل بالعملات الرقمية يحمل العديد من المخاطر كالتالي:

(١٤)) كاثرين ستيوارت – العملة الافتراضية "اجراء المعاملات وتبادل القيمة في العصر الرقمي"- لمحةٌ حول الندوة الاستشارية المعنية بالعملة الرقمية التي عُقِدَت كجزءٍ من برنامج معهد كورشام للقيادة الفكرية لعام ٢٠١٧م – ص١٣ص١٧ - www.rand.org/t/CF371

(ISSN: 2356 - 9492)

١ . **غياب الأطر التنظيمية للعملات الرقمية:** عدم وجود اطار تنظيمي حكومي للعملات الرقمية ، يغل يد السلطات الحكومية عن مراقبة عمليات تداول هذه العملات، لأن الاقتصادات والعملات الرقمية تتعدى في استخداماتها الحدود الجغرافية، وهو ما يعيق المنظمين عن تحديد الاختصاص القضائي عند حدوث الجرائم بالإضافة لعدم تسجيل المعاملات المالية بالعملات الرقمية؛ وهو ما يتيح للمستخدمين إمكانية التعامل بها دون رقابة مصرفية مركزية، بالإضافة لإخفاء هوياتهم وبياناتهم ؛ مما يضاعف مخاطر استخدامها الامنية.

٢ . **عدم ثباتها كوسيلة وفاء:** على الرغم من وصول الإنتاج من هذه العملات ل ١٣ مليون عملة في ٢٠١٤، الا انها لم يتم الاعتراف بها رسمياً كعملة للان فقد قضت محكمة في ولاية تكساس الأمريكية في الأمر وفصلت بأن العملات الرقمية هي نقود، فيما صرح بنك الصين أنها ليست نقود، واعتبرتها سلطات فنلندا سلعة، وحكمت محكمة ألمانية بأنها وحدة حساب.

٣ . **العملات الرقمية تستخدمها الجماعات الإرهابية والإجرامية:**

تتوافر أدلّة كثيرة على كون المنظمات الاجرامية والارهابية، وخاصّة مجرمي الإنترنت، تستخدم العملات الرقمية .مع ذلك لم يظهر ما يؤكد استخدام الجماعات الإرهابية لها في عمليّات تجاريّة. ومن اليقيني ان العملات الرقمية تستخدم كوسيلة لنقل الاموال بشكل آمن ومشفر، للحصول على منفعة معينه. فلا يوجد ما يؤيد قيام تلك الجماعات بتطوير ونشر عملات رقمية، مع توافر أدلة على أنها استخدمت عملات رقمية في تمويل الارهاب.

أحد الاستخدامات الجنائيّة للعملات الرقمية، في هجمات الفدية، حيث يقوم الجناة بتشفير بيانات الضحية وعدم فك تشفيرها إلاّ بعد دفع فدية بالعملة الرقمية، كذلك تستخدم في الاتجار غير المشروع بالمخدرات والأسلحة وغيرها، كما إنّ الأدلّة على أن الإرهابيين يستخدمون عملات رقمية على مستوى مؤثر إعلانان الكترونيّان لداعش لجمع التبرعات بالعملات الرقمية ، كما ظهرت حالات نشر للعملة الرقمية ذات اغراض سياسيّة لتحلّ مكان العملة التقليدية المركزية مثل ما حدث في ايسلندا من نشر عملة

"اوروار كوين" من خلال مصدر مجهول في ٢٠١٤ للحصول على عملات أقل عرضة للتضخم خارج اطار التنظيم المركزي الحكومي، وقامت الإكوادور بإطلاق عملة "سكوت كوين" كبديل للعملات التقليدية. ولم تعاقب حكومة ايسلندا واسكتلندا الشرعيّة على نشر العملة الرقمية، بينما في الإكوادور دعمت الحكومة الجهد المبذول لنشر تلك العملة. ويلاحظ ان نشر أيّ عملة رقمية بديلة لم يعتمد على نطاق واسع وثمة العديد من التحديات التي تمكن الجماعات الإرهابية من استخدام العملات الرقمية لتجنب كل الأنظمة المعروفة لمكافحة الإرهاب وغسل الأموال، في ظل إمكانية استخدام العملات الرقمية في تحويل الاموال واخفاء هوية المستخدمين مع عدم إمكانية مراقبه تداولها ، بما في ذلك المجموعات الإرهابيّة، حيث يمكنها استغلال العملة الرقمية من أجل مكاسبها السياسيّة والاقتصاديّة وعلى مستوى العمليات المالية.

كما تبين أن "العملات الرقمية هي الافضل للجناة والارهابيين لاستخدامها في سرقة العملات الرقمية وكذلك المضاربة وتكوين عملات رقمية احتياليا لا قيمة لها"، فكلما انتشرت العملات المشفرة تزايد إساءة استعمالها لإمكانية إخفاء الهوية عند استخدامها.(١٥)

وتجدر الإشارة إلى أن شبكات الجريمة المنظمة تسعى لإيجاد طرق لإخفاء مصدر وهدف التمويل غير الشرعي للأنشطة الإجرامية، ومن المسلم به صعوبة كشف غسل الأموال في الاقتصاد الحقيقي، وهو ما يؤكد صعوبة ذلك في مجال الجريمة الالكترونية. لذا فمستخدمي لعبة "الحياة الثانية" ينشؤون حسابات بأسماء وهمية او بسرقة هوية اخرين، ويستخدمونها في ارتكاب الجرائم، ثم يحولونها الى عملات حقيقية ويودعونها في البنوك.

(١٥) جوشوا بارون واخرين – تداعيات العملة الافتراضية على الامن القومي "البحث في إمكانية النشر من جهة فاعلة غير حكومية"- مؤسسة راند – كاليفورنيا- الولايات المتحدة الامريكية – ٢٠١٥م – ص٣٧ص٤٠ - www.rand.org/t/rr1231

(ISSN: 2356 - 9492)

وينطبق الأمر نفسه على العملات الرقمية، فقد يروج احد المتعاملين في المخدرات مثلاً عبر الانترنت، ويأخذ هذه الأموال الرقمية ويستخدمها في العاب عبر الانترنت، ويسحب المحفظة ويحولها من خلال الكازينو إلى الدولار، ثم يودعها في البنك.

ويستخدمها الإرهابيين في لعبة عبر الانترنت ك "الحياة الثانية" ويستخدمون الأرباح في تمويل العمليات الإرهابية، وقد يشترى ارهابي ليندن دولار، ويتواصل مع الاخرين في الجماعة الارهابية من خلال اللعبة، لشراء سلع رقمية، ثم يقوم بتحويلها لعملات مركزية لشراء ما يلزم للقيام بجريمة إرهابية، وقد تتم العملية نفسها بواسطة العملات الرقمية وهنا يكون تعقب هذه المعاملات المالية صعبا.

٤ . **تذبذب قيمة العملات الرقمية:** يؤدى ارتفاع أسعار العملات الرقمية لجذب الاستثمارات، الا ان الانخفاض المفاجئ لسعرها قد يؤثر على استقرار حجم وقيمة الاستثمارات عند اصدار اخرى أكثر قبولاً منها.

٥ . **احتمال التعرض للاحتيال الافتراضي:** يتم إغراء المستخدمين بالشراء عبر الانترنت لسلع غير حقيقية، وعقب السداد بالعملات الرقمية، يكتشف الاحتيال الذي وقع ضحية له. كما أن استخدام العملات الرقمية في الشراء لا يحميه قانون معين عند حدوث مخالفات لشروط التعامل.

وقد أوضحت الهيئة المصرفية الأوروبية لمخاطر استخدام العملات المالية الرقمية تزايد حجم المخاطر بسبب الهيكل غير المراقب للعملات الرقمية. وأنه من المخاطر المرصودة التعرض لخسارة الأموال من خلال استخدام منصات التداول، فعند شراء العملات الرقمية من خلال تلك المنصات لا ضمان للحفاظ على أموال المستهلك لاحتمال عدم قدرة المنصة أو إفلاسها، حيث ان عدم توافر الحماية للإيداعات من العملة الرقمية كالبنوك، فأي خسارة في الإيداعات لن يتم تعويضها وقد أشارت دراسة[١٦] أن ٤٥ % من المبادلات الرقمية تفشل، وعلى ذلك فالعملات الرقمية تحتاج لبحث ودراية وخبرة تكنولوجية ومالية، وبالنسبة للدول المتحكمة في المعايير الاقتصادية

(١٦) أعدها الباحثان تايلر ممور من جامعة "ساوثرن ميثودسيت"، ونيكولاس كريستسن من جامعة "كارنيجي ميلون"،

والتجارية تحد من استخدام التعاملات الرقمية ، ويشكك الاقتصاديين والمؤسسات الأوروبية المصرفية الكبرى فيها بسبب مخاطرها العالية، وافتقادها لمعايير وشروط انطباق تعريف العملة عليها.(١٧)

المبحث الأول

مخاطر استخدام العملات الرقمية في الجريمة

تمهيد وتقسيم:

من المؤكد ان لكل ابتكار انساني جانبان يتم استخدامه فيهما أولهما جانب يفيد الإنسانية وثانيهما جانب ضار بالإنسانية ولما كنا معنيين برصد ومنع والوقاية من الاضرار المترتبة على الاستخدام الاجرامي للابتكارات الإنسانية فسوف نتطرق في دراستنا الى الاستخدامات الاجرامية للعملات الرقمية على النحو التالي:

المطلب الأول: مميزات العملات الرقمية للجناة ودورها في إخفاء الأنشطة الاجرامية

المطلب الثاني: جرائم الاحتيال والتعدين الخفي Crypto jacking

المطلب الأول

مميزات العملات الرقمية للجناة ودورها في إخفاء الأنشطة الاجرامية

تقسيم:

الفرع الأول: مميزات العملات الرقمية للجناة

الفرع الثاني: دور العملات الرقمية في إخفاء الأنشطة الاجرامية

الفرع الأول

مميزات العملات الرقمية للجناة

أولا: عدم إمكانية كشف هوية المتعامل:

(17) Alan Lloyd Paris& Srinivasa Manikant Upadhyayula, Bitcoin: Currency of the future or money laundering vehicle?, June 2017,global research &Analytics ,p2

(ISSN: 2356 - 9492)

من المؤكد أن مرتكبي الجرائم يرغبون في نظام لا يطلب ما يفيد الكشف عن هوية المستخدم على الاطلاق، أو تقديم أي معلومات عنه، الا أن عدم الكشف عن الهوية، ليس في حد ذاته إشارة إلى السلوك الإجرامي فقد أثبتت بعض الحوادث كتلك التي حدثت في أوكرانيا من لجوء مؤيدي الحكومة والمساندة لعدم الكشف عن هويتهم على الإنترنت لحماية أنفسهم من التحديد والانتقام المحتمل بسبب وجهات نظرهم، يضاف لذلك أن هناك العديد من الحالات التي يكون فيها إخفاء الهوية عبر الإنترنت مهمًا.

ثانيا: الوصول العالمي: يجب أن يسمح نظام العملات الرقمية بتحويل الأموال من مكان لآخر وبأي قيمة، لذا فهي تتيح للمستخدم القدرة على تنفيذ معاملات عبر بلدان ثالثة ليس له اتصال بها ولا تربطه بها صلة فلا يمكن تحديد هويته أو البلد الذي يستخدم منه الشبكة.

ثالثا: السرعة: ينبغي للنظام إجراء عمليات التحويل بسرعة، وغالبا ما يكون في غضون ثوان. فكلما كانت المعاملة أسرع، قلت فرصة اعتراضها وحظرها.

رابعا: عدم التنصل: يجب أن تكون المعاملات نهائية على الفور فلا يجب ألا يكون هناك أي تحقق إضافي لتنفيذ أي معاملة. فلا ينبغي أن يكون الشخص المرسل للأموال قادرًا على "إلغاء إرسالها" أو عكس عملية النقل.

خامسا: تكلفة منخفضة للاستخدام: في حين أن هذا الأمر أقل أهمية بالنسبة لمستخدم العملات الرقمية بهدف اجرامي، سيكون من المرغوب تشغيل النظام بأقل قدر من النفقات العامة مما يسمح بإبرام المعاملات الكبيرة والصغيرة دون تناول قيمة المعاملات الصغيرة في الرسوم. ويمكن للوسطاء الذين يدعمون الاستخدامات غير القانونية للعملات الرقمية فرض رسوم على خدماتهم فعندما تفشل الخدمة المقدمة عن عمد في تقديم التقارير المطلوبة عن المعاملات المتضمنة جرائم كتمويل الإرهاب او غسل الأموال او نقل أموال الاتجار بالمخدرات او الأسلحة او الاتجار بالبشر او تهريبهم قد تتوقع رسوما أكبر مقابل الصمت.

سادسا: سهولة الاستخدام النسبية: بغض النظر عن النظام الذي تستخدمه، يجب أن يكون من السهل على الأشخاص غير التقنيين استخدامه، يجب أن يحتوي على

واجهة حاسوبية تجعل إعداد المعاملة سريعًا وسهلاً ويجب استخدامه بواسطة حاسوب أو هاتف ذكي متصل بالإنترنت.(١٨)

سابعا: توفير الأمان واخفاء الهوية: استخدام طبقات إضافية من إخفاء الهوية من شأنه جعل مهمة سلطات إنفاذ القانون ومكافحة الإرهاب أصعب بكثير، وهناك مستوى آخر من التعقيد سيواجه سلطات إنفاذ القانون ومحللي تمويل الإرهاب الناتج عن الحركة المتكررة لهذه الشبكات من الخوادم من مكان إلى آخر بمرور الوقت.

إن المراجعة الأولية تشير إلى أن العملات الرقمية تلبي احتياجات الإرهابيين وغاسلي الأموال وغيرهم من المجرمين الذين يعتمدون على القدرة على نقل الأموال على الصعيد العالمي. كما أن الخصائص المميزة للعملات الرقمية المذكورة أعلاه والتي تجعلها جذابة للإرهابيين وغسل الأموال والمجرمين تشكل تحديات أمام السطات . كما تشكل العملات الرقمية تهديدا لنقل القيمة النقدية خارج الخدمات المصرفية التقليدية وتحويل الأموال الرقمية.

ويعتبر الانترنت العميق جزءًا من الإنترنت الذي اكتسب سمعة ومكانة أسطورية على مر السنين، ومعظم المواقع الإلكترونية في الشبكة العميقة تتعامل بالعملات الرقمية. والشبكة العميقة مخصصه للأنشطة الاجرامية فيمكن مشاهدة صفقات تجارة المخدرات والأسلحة وحتى بيع الحيوانات المهددة بالانقراض وصولًا للإتجار بالأعضاء البشرية، وقد أصبحت العملات الرقمية هي الوسيلة المفضلة للدفع مقابل هذا النوع من الخدمات والصفقات المجرمة حيث توفّر الأمان والموثوقية للمتداولين والمشترين مقارنةً بالأموال التقليدية.

وقد استحوذت العملات الرقمية على اهتمام الناس من كل جانب، وعلى الرغم من أنها تُدعَى عملات رقمية مشفّرة إلّا أنها ليست آمنة وموثوقة تمامًا، فقد تم

(18) Geo_ Goodell& Tomaso Aste, Can Cryptocurrencies Preserve Privacy and Comply with Regulations?, arXiv:1811.12240v3 [cs.CY] 7 May 2019,pp:3-6

(ISSN: 2356 - 9492)

التوصل لبعض الثغرات فيها، فطبيعة عمليات النقل المجهلة لها اوجدت آلية جديدة للمخترقين لارتكاب الجريمة دون إمكانية ملاحقتهم وضبطهم.

وتتميّز العملات الرقمية بدرجة عالية من الأمان والخصوصية ولكنّها تتّسم ببعض الغموض أيضًا، فحتى لو كان بإمكانك مشاهدة المحفظة التي ذهبت إليها العملات الرقمية فلن تتمكن أبدًا من معرفة صاحب المحفظة، ونقل العملات الرقمية عبر التبادلات التي نقوم بها يعني أن تختفي العملات داخل الشبكة وبسبب غموض العمليات التي نقوم بها فقد اكتسبت العملات الرقمية سمعة سيئة ونفورًا من قبل الحكومات في جميع أنحاء العالم.

كما تساهم العملات الرقمية في زيادة مستوى الجريمة الرقميّة، فعلى سبيل المثال تقدّم عملات رقمية مثل Monero وVerge عروضًا مثيرة جدًا لمحبي الخصوصية، وأصبحت هذه العملات هي العملات المفضلة بالنسبة للمخترقين ومن الجرائم الإلكترونية التي ازدادت بسبب العملات الرقمية فايروسRansomware وهو نوع من أنواع البرمجيات الخبيثة التي تشفر ملفات الضحية، ويكون بحاجة لمفتاح معين لفك التشفير بعد دفع مبلغ معيّن للمهاجم، ويتم دفع هذه الفدية باستخدام العملات الرقمية ، والتي يصعب معها ملاحقة الجناة.

وقد كان انتشار الفايروس مزعجًا للغاية حينها للكثير من الناس، فقد كان عام ٢٠١٧ عامًا حافلًا بالهجمات الإلكترونية، ولم تستطع المؤسسات القيام بأي شيء حيال حماية البيانات، فوصلت الهجمات لمستوى خطير جدًّا، حيث استهدفوا المستشفيات وقام المهاجمين بتشفير السجلّات الطبية للمرضى مما تسبّب بفوضى كبيرة حينها[١٩].

(19) (19) Alan Brill, Lonnie Keene, Cryptocurrencies: The Next Generation of Terrorist Financing?, Defense Against Terrorism Review, Vol. 6, No. 1, Spring &Fall 2014, pp. 7- 30

الفرع الثاني

دور العملات الرقمية في إخفاء الأنشطة الاجرامية

إن سِجلَّ العملات الرقمية ثابت ومتاح عالميا، ويحتوي هذا السجل على كل التحويلات ما دام العملات الرقمية مستمر بالعمل. لهذا [٢٠]، يمكن القول أن مستخدمي العملات الرقمية ذوي هويات مُستعارة. لذا يمكن الربط بين هويات الاشخاص وعناوين محافظ العملات الرقمية، وتعقب تحويلات تلك العملات من خلال عنوان المحفظة الرقمية الخاصة بالمستخدم لها عند التحقق من هويتة الحقيقية.

كما ان البلوك تشين الخاصة بالعملات الرقمية تجعل من الصعوبة بمكان إخفاء الهوية على الشبكة، فقد يكون من السهل التخلص من حاسوب، أو عنوان صندون للبريد الالكتروني، أو رقم تعريفي "IP"، إلا أنه يصعب مسح مسار العملات الرقمية عند خروجها من محفظة او دخولها اليها لأن طبيعة بنية البلوك تشين الخاصة بالعملات الرقمية لا تمنحها الخصوصية المتصورة. لذا فانه يصعب على المجرمين استخدام العملات الرقمية في ارتكاب جرائمهم، وذلك لان الهويات المزيفة يمكن من خلالها ربط العناوين بالهويات الحقيقيه حتى بعد مرور فترة طويلة على وقوع الجريمة، فيمكن لاجهزة انفاذ القانون أو الضحايا الذين يتم توظيفهم أن يربطوا بين تلك المحافظ والجناة من اجل تحديد هوية المجرمين، لذا، يمكن من خلال تعقب خط سير المدفوعات من العملات الرقمية تحديد الهوية الحقيقية للعديد من المتاجرين بالمخدرات بشكل غير مشروع على الانترنت وضبطهم لكونهم ظنوا ان العملات الرقمية مجهولة الهوية بالكامل.

إن العملات الرقمية تكنولوجيا هي تكنولوجيا نقدية، والنقد يستخدم من مرتكبي الجريمة في العديد من الاحوال لهذا، يمكن استخدام النقد بواسطة المجرمين او لتسهيل ارتكاب الجرائم، لكن الا انه نظرا لوجود سجل لتحركات وانشاء العملات الرقمية فان

(20) John Collins, Crypto, crime and control" Cryptocurrencies as an enabler of organized crime", June 2022, pp:16-19, https://globalinitiative.net/wp-content/uploads/2022/06/GITOC-Crypto-crime-and-control-Cryptocurrencies-as-an-enabler-of-organized-crime.pdf

(ISSN: 2356 - 9492)

ذلك يجعلها غير فعالة بالنسبة لمرتكبي الجرائم مع وجود ضحايا يمكنهم التقدم بشكوى لاقتضاء حقوقهم.

فالعملات الرقمية يمكن استغلالها في ارتكاب"الجرائم التي ليس لها ضحايا"، لأن عدم وجود ضحية يعني عدم محاولة تحديد هوية "الجاني". ولانه ليس هناك ما يُدعى بالجريمة التي لا تحتوي على ضحية، لأنه إن لم يحتوِ الفعل على ضحية، فهو ليس جريمة فيمكن للعملات الرقمية أن يكون مفيدا في تلك الأعمال غير الشرعية، لأنه لا يوجد هناك ضحايا يحاولون الإمساك بالمجرم. فتلك النشاطات التي تم ارتكابها ستَظهر على البلوك تشين كتحويل فردي قد تتعدد أسبابه.

لذا، فجرائم المقامرة على الشبكة والتهرب من ضوابط رأس المال، من الممكن للمرء أن يتوقع استخدام العملات الرقمية فيها، ولكن لن يتوقع استخدام العملات الرقمية لجرائم القتل والإرهاب. لهذا، يمكن ان يتم استخدام البلوك تشين للعملات الرقمية في الاتجار غير المشروع بالمخدرات او في غسل الاموال او تمويل الارهاب.

كما تعزز العملات الرقمية حرية الأفراد الا انها لا تسهِّل عليهم ارتكاب الجرائم، فهي أداة يمكن الاستفادة منها في المستقبل.

إنَّ "المطالبة بفدية" هي واحدة من اخطر الجرائم الحاسوبية التي استخدمت فيها العملات الرقمية كما انها طريقة للدخول غير المصرح به لحواسيب الضحايا وتشفير المعلومات الخاصة بالضحايا، لحين دفع الفدية باستخدام العملات الرقمية. وبالرغم من سابقة وجود تلك الأنواع من الجرائم قبل العملات الرقمية، إلا أن تنفيذها أصبح أكثر سهولة منذ ظهورها، ومع هذا يمكن الفهم ان جرائم طلب الفدية تلك تستغل الحواسيب التي تفتقر للأمن والحماية.

فالشركات التي يتم تشفير بياناتها الحاسوبية من المخترقين الذين يهدفون للحصول على المال في شكل عملات رقمية لديها مخاطر أكبر من عملية الاختراق ودفع الفدية. فقد يكون دافع المخترقين هو مبلغ الفدية، لكن دافع المنافِسين أو العملاء والممولين في جمع بيانات الشركات اخطر بكثير. وعلى ذلك فقد سمحت جرائم المطالبة بالفدية عن طريق العملات الرقمية بتحديد وكشف العيوب في حماية أمن الحواسيب، وأدت

بالشركات لتعزيز اساليب التأمين للنظم الحاسوبية وإلى زيادةٍ في نمو برمجيات واساليب التأمين وحماية الحواسيب. وتسمح العملات الرقمية بتسييل سوق حماية الحواسيب. وبينما يمكن للمخترقين حاليا الاستفادة من ذلك، يمكن للشركات منتجة تلك البرمجيات تحديد افضل سبل التأمين.(٢١)

المطلب الثاني

جرائم الاحتيال والتعدين الخفي Crypto jacking

تقسيم:

الفرع الأول: مخططات بونزي الاحتيالية

الفرع الثاني: جرائم التعدين الخفي Cryptojacking

الفرع الأول

مخططات بونزي الاحتيالية

مع انتشار العملات الرقمية واعتبارها وسيلة سهلة لكثير من المستثمرين من أجل كسب المال السريع والحصول على عوائد ضخمة من استثماراتهم، كانت مخططات بونزي تزداد انتشارًا أيضًا. حيث تعتمد هذه المخطّطات على كسب ثقة الناس وجذبهم للاستثمار في محافظهم الرقمية من خلال تقديم ارباح خيالية وهمية، فمثلاً استثمر ١٠٠٠ دولار أمريكي في إحدى المحافظ الرقمية واحصل على عوائد مالية بقيمة ١٠ آلاف دولار أمريكي شهريًا، أحد الأمثلة الأكثر شهرة على مخطّطات بونزي الاحتيالية، ويمكن أن يقع فريستها الكثير من المستثمرين المبتدئين ويفقدون أموالهم بسبب هذا النوع من العروض الاحتيالية.

ومخطط بونزي هو عملية احتيال استثمارية تتضمن دفع عوائد مزعومة للمستثمرين من أموال ساهم بها مستثمرون جدد. غالبًا ما يطلب منظمو مخطط بونزي مستثمرين جدد من خلال الوعد باستثمار الأموال في الفرص التي تدعي أنها تحقق عوائد ضخمة دون مخاطر. في العديد من مخططات بونزي ، بدلاً من الانخراط في أي نشاط

(21) Geo_ Goodell& Tomaso Aste, Can Cryptocurrencies Preserve Privacy and Comply with Regulations? arXiv:1811.12240v3 [cs.CY] 7 May 2019, pp:1-4

(ISSN: 2356 - 9492)

استثماري مشروع ، حيث يقوم المحتالون بجذب أموال جديدة لتسديد ارباح وعدت بها مستثمرين سابقين وكذلك لتحويل بعض هذه الأموال "المستثمرة" للاستخدام الشخصي ، غالبًا ما يستخدم منظمو مخططات Ponzi أحدث ابتكارات أو تكنولوجيا أو منتجات أو صناعة نمو لجذب المستثمرين ومنح مخططهم وعدًا بعوائد عالية. غالبًا ما يكون المستثمرون المحتملون أقل تشككا في وجود فرصة استثمارية عند تقييم شيء جديد أو جديد أو "متطور."

لذا أصبحت العملات الرقمية ، مؤخرًا شعبية وتهدف إلى أن تكون بمثابة نوع من المال. قد يتم تداولها في البورصات عبر الإنترنت للعملات التقليدية ، أو تستخدم لشراء السلع أو الخدمات ، وعادة ما تكون عبر الإنترنت.

وفي ظل الاستخدام المتزايد للعملات الرقمية في السوق العالمية قد يغري المحتالين لجذب المستثمرين إلى Ponzi وغيرها من المخططات التي تستخدم فيها هذه العملات لتسهيل الاستثمارات أو المعاملات الاحتيالية و قد ينطوي الاحتيال أيضًا على عرض أو منصة تداول غير مسجلة. غالبًا ما تعد هذه المخططات بعوائد عالية للحصول على ظاهرة إنترنت متنامية وقد يستخدم المحتالون العملات الرقمية لارتكاب عمليات احتيالية ، حيث يفترض أن يكون للمعاملات في العملات الرقمية فوائد خصوصية أكبر وإشراف تنظيمي أقل من المعاملات التي تتم في العملات التقليدية[٢٢]

وتشترك مخططات بونزي في بعض الخصائص مثل:

١- الوعد بعوائد استثمار عالية مع مخاطر ضئيلة أو معدومة.

٢- يحمل كل استثمار درجة من المخاطرة: عادة ما تنطوي الاستثمارات ذات العوائد المرتفعة على مخاطر أكبر. يجب أن تكون عوائد الاستثمار "المضمونة" أو الوعود بعوائد عالية مقابل القليل من المخاطرة ينظر بالشك.

(22)Edward V. Murphy &others - Bitcoin: Questions, Answers, and Analysis of Legal Issues - Congressional Research Service - Congressional Research Service – 2015 – pp:15-26

٣- عوائد متسقة للغاية: تميل الاستثمارات إلى الارتفاع والنزول بمرور الوقت، وخاصة تلك التي تسعى إلى تحقيق عوائد عالية. تشك في وجود استثمار يولد عائدات ثابتة بغض النظر عن ظروف السوق.

٤- استثمارات غير مسجلة. تتضمن مخططات بونزي عادة استثمارات لم يتم تسجيلها لدى المؤسسة أو مع هيئات تنظيم الأوراق المالية الحكومية.

٥- الباعة غير المرخصة. تتطلب قوانين الأوراق المالية الفيدرالية وقوانين الولايات ترخيصًا أو تسجيل بعض المهنيين في مجال الاستثمار وشركاتهم. العديد من مخططات بونزي تشمل الأفراد غير المرخص لهم أو الشركات غير المقيدة.

٦- الاستراتيجيات السرية أو المعقدة وهياكل الرسوم. من الجيد أن تتجنب الاستثمارات التي لا تفهمها أو التي لا يمكنك الحصول على معلومات كاملة بشأنها.

٧- لا يوجد حد أدنى لمؤهلات المستثمر تتطلب معظم فرص الاستثمار الخاصة المشروعة أن تكون مستثمرًا معتمدًا. يجب أن تكون متشككا للغاية في فرص الاستثمار التي لا تسأل عن راتبك أو ثروتك الصافية.

٨- مشاكل مع الأوراق. كن متشككا من الأعذار فيما يتعلق لماذا لا يمكنك مراجعة المعلومات حول الاستثمار في الكتابة. اقرأ دائمًا ونظر بعناية في نشرة أو بيان الإفصاح قبل الاستثمار. احترس من الأخطاء في كشوف الحساب والتي قد تكون علامة على نشاط احتيالي.

٩- صعوبة في تلقي المدفوعات. كن واعيا إذا لم تتلقى دفعة أو كنت تواجه صعوبة في صرف استثمارك. يشجع منظمو مخطط بونزي في بعض الأحيان المشاركين على "ترحيل" المدفوعات الموعودة من خلال تقديم عوائد استثمار أعلى.

١٠- إنه يأتي من خلال شخص لديه تقارب مشترك. غالبًا ما يستغل المحتالون الثقة المستمدة من كونهم أعضاء في مجموعة تشترك في تقارب، مثل الانتماء

(ISSN: 2356 - 9492)

القومي أو العرقي أو الديني. في بعض الأحيان ، يمكن تجنيد القادة المحترمين أو الأعضاء البارزين ، عن قصد أو بغير علم ، لنشر كلمة "الاستثمار."[٢٣]

الفرع الثاني

جرائم التعدين الخفي Cryptojacking

هو نوع جديد من الجرائم المرتبطة بالعملات الرقمية التي انتشرت بكثرة في الفترة الماضية عقب ارتفاع أسعار العملات الرقمية بشكل كبير. وترتكب من خلال استخدام لغة جافا للبرمجة من اجل التلاعب في المواقع التي يتم تصفحها، حيث عقب فتح المستخدم موقع الويب يبدأ حاسوبة في تعدين العملات الرقمية واستخدام وحدة المعالجة المركزية الخاصة بحواسيب الزوّار دون علمهم بذلك. وقد بلغت هذه الهجمات ذروتها في عام ٢٠١٧ واستهدفت العديد من مواقع الويب الرئيسية مثل الصحف والمجلّات العالمية المشهورة. فعندما ظهرت العملات الرقمية كأحد تطبيقات سلسلة الكتل وبدأت في الانتشار في النظم المختلفة والموزعة على العديد من الإمكان في العالم لتخزين العملات الرقمية حظيت بثقة كبيرة من المتعاملين فعززت الشفافية في المعاملات مما ترتب علية تعزيز ثقة العملاء فيها ويتم تعدين العملات من خلال عمليات التجزئة واسعة النطاق والتي يتم التحقق منها بعد ذلك بواسطة نقاط التعدين الموزعة في شبكة نظير إلى نظير .(P2P) ومع ذلك، فقد لجأ البعض من القائمين بالتعدين الى ارتكاب جرائم الاختراق للمواقع والأجهزة الطرفية المرتبطة بشبكات الند للند لكي يستغلوا تلك الأجهزة في تعدين العملات لما لذلك من عائد مادي ضخم يحققونه وذلك باستغلال أجهزة المستخدمين ومساحاتهم التخزينية لإنتاج العملات الرقمية وتحقيق أرباح طائلة من ذلك دون ان يتكلف شئيا

تسمى هذه الجريمة التي ظهرت مؤخرًا باسمcrypto jacking ، ويتمثل السلوك الاجرامي في تثبيت برنامج على الجهاز المستهدف سرا ونقل العملات التي يتم تعدينها

(23) SEC "office of investor –education –advocacy", Investor Alert Ponzi schemes Using virtual Currencies, SEC Pub. No. 153 (7/13),pp:2-5,available online: www.investor.gov

باستخدامه إلى خادم بعيد، وتتطلب هذه الجريمة ان يحصل الجناة على إذن المستخدم لتنزيل البرنامج واتصال دائم بالإنترنت ويتم إبلاغ نتيجة التعدين بالاختراق للخصم أو خادم dropzone يسيطر عليه. ومع ذلك ثبت ان ارتكاب الجريمة بشكل مطلق غير ممكن لعدة أسباب. أولاً، ليس لجميع الأجهزة اتصال دائم بالإنترنت عند الحاجة لإرسال المعادلات الرقمية التي تمثل العملة الرقمية التي تم تعدينها للخادم الخاص بالجاني وكانت حساسة للوقت، وإذا لم يتم إرسالها فور حلها، فإنها تصبح قديمة. ثانياً ، يمكن لشركات مكافحة الفيروسات التعرف بسهولة على الثنائيات المستخدمة لإعداد الشفرة الخاصة بالعملة المراد انتاجها والكشف عنها بالإضافة لتطلب هذا النوع من الهجوم ناقلًا للعدوى ، حيث يمكّن المستخدمون من الهجوم عن طريق تثبيت برمجيات اختراق التشفير عن طريق الخطأ على أجهزتهم.(٢٤)

وقد ظهر شكل حديث من برمجيات التشفير في المتصفح والتي لا تعاني من هذه المشكلات. وهنا لا يتطلب تثبيت برمجيات التشفير في المتصفح تثبيت برمجيات أو تفويض من المستخدمين لتشغيل النظام. حيث تستخدم مثيلات تشفير التشفير في المتصفح Java Script لحساب PoW في متصفح الويب ونقل PoW إلى خادم drop zoneعن بعد. على هذا النحو، وبما أنها محمية في عملية المتصفح، فهي غير مكتشفة بواسطة ماسحات مكافحة الفيروسات. علاوة على ذلك ، يضمن التنقيب أثناء تصفح الويب النقل المتواصل لـ PoW عبر اتصال إنترنت ثابت في المكان. تم تصميم crypto jacking داخل المستعرض بسهولة من خلال الاستخدام الجيد كمصدر بديل للدخل للإعلان عبر الإنترنت ، وذلك بفضل الخدمات عبر الإنترنت مثل Coinhive، والتي وفرت قوالب JavaScript لـ .cryptojacking تقدم Coi hive برامج نصية لتعدين"Monero" ، وهي عملة رقمية يصعب تتبعها، ومكافأة القائم بالتعدين استنادًا إلى التجزئة المجمعة التي يساهمون بها. وتوضح تقارير بحث

(24) Igor Makarov, Antoinette Schoar, Cryptocurrencies and Decentralized Finance (DeFi), BPEA Conference Drafts, March 24-25, 2022, pp:5-9, https://www.brookings.edu/wp-content/uploads/2022/03/SP22_BPEA_MakarovSchoar_conf-draft.pdf

(ISSN: 2356 - 9492)

Googleعن Crypto jacking و "Monero" و "Coin hive" من مايو ٢٠١٧ إلى مارس ٢٠١٨ الاهتمام المتزايد بإنتاج العملات الرقمية كظاهرة عالمية ، وتزامن هذا الارتفاع مع الزيادة في اختراق تلك الشفرات في المتصفح حيث تم الإبلاغ عن أكثر من ٣٢٠٠٠ موقعًا يشغل سكريبتات "Coin hive "، والعديد منها ناتج عن التسوية والحقن ، و تعد أداة التعدين في المتصفح بمثابة وسيلة هجوم للمتسللين الذين يضخون كود JavaScriptفي مواقع الويب الشهيرة دون علم مالكي مواقع الويب ويعرف باسم هجوم الاصطدام التشفير ، والذي أصبح يشكل مشكلة كبيرة في الآونة الأخيرة.[٢٥] وفقًا لتقرير سيمانتيك الأخير حول تهديد أمن الإنترنت (ISTR) ، حيث ارتفعت عدد هجمات التشفير على المواقع الإلكترونية بنسبة ٨٥٠٠ ٪ خلال عام ٢٠١٧ ، وفي (فبراير) ٢٠١٨ ، أصاب هجوم كبير بالتشفير أكثر من ٤٠٠٠ موقع إلكتروني حول العالم ، وشمل الهجوم مواقع الويب الخاصة بالقضاء الفيدرالي الأمريكي وخدمة الصحة الوطنية في المملكة المتحدة. أيضًا في فبراير ٢٠١٨، أصبحت Tesla ضحية هجوم تشفير للاصطياد حيث قام المهاجمون باختطاف سحابة Tesla ونشروا رمز تشفير التشفير الخاص بهم.

المطلب الثالث

استخدام العملات الرقمية في غسل الاموال وتمويل الارهاب

تقسيم:

الفرع الأول: غسل الأموال باستخدام العملات الرقمية

الفرع الثاني: استخدام العملات الرقمية في تمويل الإرهاب

الفرع الأول

غسل الأموال باستخدام العملات الرقمية

أولا: ماهية ماهية غسل الأموال باستخدام العملات الرقمية

(25) Muhammad Saad, Amanullah Khormali, Aziz Muheisen, End-to-End Analysis of In-Browser Crypto jacking, pp:3-5,2018,available online: https://arxiv.org/pdf/1809.02152.pdf

بدأ ظهور مفهوم العملة الرقمية بعد ٤٦ يومًا من إفلاس بنك ليمان براذرز، وهو الحدث الذي يمثل بداية ثاني أكبر أزمة مالية في تاريخ البشرية وخلال الوقت الذي كان العديد من المديرين التنفيذيين وصانعي القوانين والمديرين يحاولون تحديد التدابير أو الممارسات الفعالة والوقائية لإعادة الاقتصاد إلى حالته المستقرة، قررت مجموعة صغيرة من المهندسين متابعة فكرة العملة الرقمية. وفي ذات الوقت ، ظهرت مجموعة قررت استخدام العملة الرقمية الجديدة لتحقيق الثراء لهم والاستفادة منها في الأنشطة الاجرامية مما افرز انماطا جديدة من الجريمة وتزايد استخدام العملات الرقمية في الجريمة ، وارتفعت أسعارها إلى مستويات مرتفعة.

وقد أدت خصائص العملات الرقمية مثل اللامركزية ، طابعها العالمي الوراثي ، الطبيعة المجهولة المصدر ، والافتقار الأولي للوائح عملياتهم لتمتعها بجاذبية خاصة لعصابات الجريمة المنظمة وغاسلي الأموال وممولي الإرهاب لذا حددت السلطات الحكومية تحديد الإجراءات اللازمة للحد من الاستخدام غير المشروع لها وقدمت بعض المبادئ التوجيهية لتحقيق الاستدامة والشرعية لها ، فوفقًا لتقرير اليوروبول الصادر في عام ٢٠١٥، استُخدمت العملات الرقمية في أكثر من ٤٠٪ من الجرائم في الاتحاد الأوروبي؛ حيث أدركت العصابات العالمية مزاياها فنجحت في جذب المواقع المتخصصة في الأنشطة الاجرامية ، كما انتشرت استخدام العملات الرقمية بين مرتكبي الجريمة الإلكترونية التي تتعامل مع معدات القرصنة، والوثائق المزورة، والمخدرات، والأسلحة، في أسواق الشبكة المظلمة.[٢٦]

وبالرغم من أنها أتاحت فرصة لإنشاء وسيط قادر على خدمة الاقتصاد الرقمي، مع تفاعل المستخدمين على أساس الند للند، فقد تم استخدامها في ارتكاب الكثير من أنماط الجريمة بوسائل مستحدثة للغاية وحققت تلك الأنماط نتائج جذابة للجناة ، حيث أدركوا

(26) ciupa katarzyna, cryptocurrencies: opportunities, risks and challenges for anti-corruption compliance systems, OECD global anti-corruption& integrity forum , 20-21 march 2019 ,Paris, OECD conference ,p:3

(ISSN: 2356 - 9492)

أن ارتكاب الجريمة أصبح أسهل كثيرًا منذ استخدام العملات الرقمية خاصة في غسل الأموال.

كما تتواصل المجموعات عبر مواقع التواصل الاجتماعي المختلفة مثل تلي جرام والتي يتم من خلالها الاتفاقات بشأن تبادل الأموال او تحويلها من مكان لآخر باستخدام العملات الرقمية دون الخضوع للقيود المفروضة من الحكومات على تبادل الأموال التي تستهدف غسلها

كما اشتهرت بين المتسللين الذين استخدموها كشكل جديد من أشكال الرشوة في حالة وقوع هجمات الفدية.(٢٧)

ومع ظهور التجارة الإلكترونية كان لا بد من إيجاد وسيلة دفع جديده تتناسب معها ، ومن ثم كانت العملات الرقمية هي الخيار الأمثل الا ان استخدامها افرز استعمالها لغرض ارتكاب الجرائم ومنها جريمة غسل الأموال(٢٨)

وغاسل الأموال يبحث عن اساليب جديدة لا تعلمها سلطات مكافحة غسل الاموال لكي يرتكب جريمته ويفلت من العقاب لذا فقد سارع مرتكبوا تلك النوعية من الجريمة الى استغلال العملات الرقمية في ارتكاب جرائمة ، مستفيداً من حداثة هذا الشكل من اشكال النقود وعدم فهم بعض سلطات انفاذ القانون المختصة لكيفية التعامل معه في البداية.(٢٩)

وتكمن العلاقة بين العملات الرقمية وجريمة غسل الأموال باستغلال المجرم لهذه العملة الرقمية كوسيلة لارتكاب جريمته وهي من أهم الأدوات الإلكترونية لغاسلي الأموال

---

(٢٧) وفقًا لإحصاءات مكتب التحقيقات الفدرالي في عام ٢٠١٧، سُرق أكثر من ثمانية وخمسون مليون وثلاثمائة ألف دولار أمريكي في حالات الفدية الإلكترونية، عندما طلب المهاجمون الدفع بعد حجب الوصول إلى الملفات بالعملات الرقمية، معظمها في Bitcoin أو Ethereum أو Bitcoin Cash (Cipher Trace

(28) The Telegraph. Britain's first Bitcoin heist as trader forced at gunpoint to transfer cyber currency. 28 January 2018.
http://www.telegraph.co.uk/news/2018/01/28/britains-first-bitcoin-heist-trader-forced-gunpoint-transfer/ accessed 2 February 2018.

(٢٩) ساسكيا كالباكيس واخرين – الدليل الدراسي لامتحان شهادة اختصاصي معتمد في مكافحة غسيل الأموال – ط٤ – ميامي – الولايات المتحدة الامريكية – ٢٠٠٧م – ص٧٦ص٨٠

وذلك لاستحالة تعقبها وسريتها وسرعتها ذلك لإمكانية نقل أي مبلغ من خلالها في مدة صغيرة دون مشاكل تذكر ، وحتى بدون حاجة للوسيط المالي حيث توجد إمكانية كبيرة لغسل الأموال باستخدام العملة الرقمية من خلال مرحلتي الإيداع والدمج ففي المرحلة الأولى يبدأ حائز المال المراد غسله بتدوير هذا المال في العالم المادي والافتراضي بالإيداع الرقمي، لتجنب الضوابط المحاسبية التقليدية.(٣٠)

ثانيا: أثار وإجراءات غسل الأموال بالعملات الرقمية

١ – <u>أثار غسل الأموال بالعملات الرقمية:</u>

تتجلى العلاقة السلبية بين العملات الرقمية وجريمة غسل الأموال باستغلال غاسل الأموال لهذه

الأموال كطريقة لارتكاب الجريمة لأن العملات الرقمية وسيلة مناسبة لاختزان القيم المالية غير المشروعة لغسلها وهنا نتبين سلبياتها، بحيث تتحول إلى وسيلة لارتكاب جريمة غسل الأموال على لأن متابعتها مسألة صعبة للغاية، كما تخفي هوية المستخدمين لذا يسهل على غاسلي الأموال إخفاء جرائمهم.

وتعد العملات الإلكترونية أحد طرق غسل الأموال لأنها أسهل استخداما وأيسر تعاملا من البنوك، حيث يقوم المتعامل بإدخال شفرة سرية في الحاسوب ثم تحويل ما يرغب من أموال، مما ييسر لغاسلي الأموال نقل أو تحويل أموال بسهولة وسرعة وأمان وتوجد إمكانية كبيرة لغسل الأموال باستخدام العملات المشفرة من خلال مراحل الإيداع والدمج، ففي الأولى يقوم الجناة بتدويره بإيداعه في المؤسسة المالية، بطريقة الإيداع الرقمي، وبذلك يتفادى الرقابة المفروضة على نقل الأموال من الحكومات المركزية وفي المرحلة الثانية يحول الجناة العملات الرقمية لدول يمكن فيها تحويل تلك الأموال لاماكن أخرى وإعادة إدخالها في عمليات تجارية واقتصادية.

(٣٠) د/ شامي يسين – تبييض الأموال عن طريق العملات الرقمية كجريمة مستحدثة - ورقة عمل مقدمة للمؤتمر الدولي الخامس عشر لكلية الشريعة والدراسات الإسلامية بجامعة الشارقة "العملات الافتراضية في الميزان"- المنعقد بجامعة الشارقة ١٦، ١٧ ابريل ٢٠١٩م – ص٧٢٩ص٧٣١

(ISSN: 2356 - 9492)

وتعد احدى أفضل الوسائل التي أفرزتها التكنولوجيا الحديثة لتسوية المعاملات وتتمتع بميزات تمكن أصحاب الاموال المتحصلة من الجرائم من استخدامها لغسل أموالهم ويتم التعامل بالعملات الرقمية دون الحاجة لإبراز هوية المتعاملين، ما يعد فرصة لدى غاسل الأموال لاستخدامها في ارتكاب جرائمه، فلن تتحدد هويته ، كما أن العملات الرقمية لها طابع من السرية مما يصعب معه على سلطات مراقبة جرائم غسل الأموال مراقبة السجلات والعمليات المالية والتحويلات المصرفية المستخدمة فيها، كما ان استخدام النقود المشفرة يعتمد اساسا على استخدام الحواسيب ونظم المعلومات التي يمكن ان تتعطل ، فيتعذر مراقبة استخدام العملات الرقمية ومن ثم فيشجع الجناة على ارتكاب جريمة غسل الأموال ، بالإضافة لإمكانية استعمال الشبكة في الدخول إلى مواقع التجارة الالكترونية والتسوق عبرها ودفع قيمة المشتريات ودون أية قيود في هذا المجال العالمية وعندئذ يمكن لغاسلي الأموال توظيفها والتعامل مع البنوك عبر الانترنت.

كما أن البنوك تقوم بمهمه حيوية للحيلولة دون غسل الأموال، وذلك من خلال مراقبتها للأسواق المالية، فيظهر خطر تزايد استخدام العملات الرقمية التي تؤثر في ميزانية البنوك المركزية، ومن ثم تقلل القدرة المالية لانخفاض الرصيد، مما يجعل تلك البنوك غير قادرة على متابعة أسواق المال.

كما تجدر الإشارة بأن عمليات غسل الأموال عبر الانترنت تتميز بالسرعة والمجهولية وتتجاوز الحدود الجغرافية، بحيث أن الجودة ذاتها التي تجعل من شبكة الانترنت محل ترحيب من المستخدمين ، تجذب الجناة للتعامل بها في غسل أموالهم ، خاصة في ظل شيوع العملات الرقمية التي يسهل نقلها من مكان لأخر بمجرد استخدام الحاسوب.(٣١)

ولما كانت تلك الأموال متحصلة من جرائم فإن العملات الرقمية ستؤمن هذه الأموال فمثلا يؤدي استخدامها إلى زيادة حالات التهرب الضريبي حيث يصعب على مؤسسات جمع الضرائب متابعة العمليات الالكترونية باستخدامها فيتعذر تحديد القيمة

(٣١) بسام أحمد الزلمي - دور النقود الإلكترونية في عمليات غسل الأموال - مجلة جامعة دمشق للعلوم الاقتصادية والقانونية –المجلد - 26 العدد الأول- 2010 - ص٥٥٧ص٥٦٠

الضريبية المستحقة على المتعامل بها كما أن الأموال الناتجة عن جرائم التهرب الضريبي تحتاج للغسل بالإضافة لطبيعة العملات الرقمية الخاصة التي يتعذر التحقق من صحتها ، ومن ثم فان الأموال الناتجة عنها قد تحتاج إلى الغسل لكونها متحصلة من جريمة ، كما توجد إمكانية لاستخراج نسخ مزيفة من العملات الرقمية من خلال معرفة تفاصيل العملات الرقمية الأصلية فتكون النقود المزيفة أموالا غير مشروعة.[٣٢]

٢- إجراءات غسل الأموال باستخدام العملات الرقمية:

تؤدي العملات الرقمية مهمه حيوية في تحفيز اقتصاد الدول لتمكينها للمستخدمين من القيام بإبرام معاملاتهم الكترونيا دون الحاجة للتوجه للمصارف التقليدية، وتوفر النفقات على المتعاملين الا ان لها آثارا خطيرة تتمثل في علاقتها بجريمة غسل الاموال حيث تسهل الجريمة وتقلل القدرة على الحد منها.

أ- مراحل غسل الاموال الكترونيا

تطور سلوك الجناة في جرائم غسل الاموال حيث استعانوا بالوسائط الإلكترونية في غسل الأموال، في مراحل الجريمة المختلفة على النحو التالي:

أ- مرحلة الاموال النظيفة:

التعرف على الثروات المتواجدة في مصادرها الأصلية، عن طريق استعمال الوسائل الإلكترونية والدخول إلى نظم المعلومات والمصارف الالكترونية، أو أي مصدر للأموال المشروعة ومحاولة فك شفراتها السرية والتخطيط للاستيلاء عليها.

ب-مرحلة جمع المبالغ القذرة: -

سحب الأموال بأساليب غير مشروعة وباستخدام الشفرات السرية لأرقام حسابات المصارف

والمؤسسات الأخرى وعملائهم، وباستخدام أجهزة ATM والحواسيب.

ت-مرحلة ادارة الاموال القذرة: -

(32) Malte Möser& others,An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem, Pre-publication copy. To appear in the proceedings of the 2013 e-Crime Researchers Summit (e-Crime) published by IEEE, pp:3-9 , available on: https://maltemoeser.de/paper/money-laundering.pdf

(ISSN: 2356 - 9492)

تستخدم نظم وبرامجيات الحاسوب لتعزيز القدرات الاجرامية للجناة عند التخطيط للجريمة والقيام بعمليات تنظيم ومراقبة تلك الاموال غير المشروعة والمحافظة عليها.

مرحلة التوظيف: –

يتم توظيف الأموال القذرة من خلال:

- التحويل الالكتروني لها لحسابات مصرفية خارجية
- تحويل الاموال القذرة الى الكترونية
- الدخول الالكتروني الى الاسواق المالية لشراء الاسهم والسندات

ج – مرحلة التغطية: –

يتم تخبئه الرابطة بين الثروات القذرة ومصادرها الأصلية بطريقة على الفور بدون وسيط فيتم:

- إبرام العمليات التجارية المشبوهة عبر الإنترنت أو البريد الإلكتروني
- تأسيس المؤسسات الوهمية بأسماء غير حقيقية والتعامل بالدخول إلكترونيا لمواقع البيع والشراء لإصدار أسهم وسندات وهمية
- شراء أصول مادية ودفع قيمتها بالعملات الرقمية وهنا قد يتم الاحتيال في السداد.

خ- مرحلة الدمج: –

يتم دمج الأموال القذرة لتوليد الاحساس بمشروعيتها عن طريق:

- إيداع النقود التي تم الحصول عليها من صفقات وشركات مشبوهة ومن مصادر وهمية في البنوك الإلكترونية
- الدخول الالكتروني لأسواق المال الفرعية والاتجار في السندات
- عمليات التجارة الإلكترونية

ويقوم الحائز بإجراء تحويلات رقمية لدول ليست فيها رقابة مشددة على غسل الاموال ثم يقوم بتحويلها مرة اخرى الى دول اخرى ودمجها في عمليات تجارية دون كشف المصدر الحقيقي لها وما يدعم إمكانية مخاطر استخدام العملات الرقمية في غسل الأموال يمكن أن يعود الى أمرين اثنين:

أ. عدم إمكانية تتبعها: العملات الرقمية وسيلة دفع سرية تخفي هوية المستخدم ، كما تقلل من تدخل مؤسسات مركزية وسيطة في الصفقات.

ب. القابلية للتحرك والانتقال: تتداول عبر العالم لذلك تتيح نظم النقود الإلكترونية، إمكانية تقليل تداول الاموال عبر الانترنت، لعدم وجود تنظيم تشريعي لها.(٣٣)

وتتراوح تقديرات حجم الأموال التي يتم غسلها في جميع أنحاء العالم بين ٥٠٠ مليار دولار أمريكي إلى تريليون دولار أمريكي، ولا يمثل هذا الإجراء مشكلة سوى عدد قليل من الدول وقد تم تصنيف حوالي ٦٤ ٪ من البلدان بأنها تنطوي على خطر كبير من غسل المال مع ٤ ٪ فقط من البلدان ومنذ عام ٢٠٠٨، أصبح لدى المستخدمين غير الشرعيين أداة أخرى، وهي العملات الرقمية، والتي أصبحت آلية هامة للغاية للراغبين في غسل اموالهم، ويمكن أيضا أن تأتي من مصادر مختلفة. ويمكن جمعها كمدفوعات فدية مسروقة من عمليات تبادل العملة الرقمية، التي يتم جمعها من خلال عمليات الاحتيال.

وبعد جمع الأموال، تبدأ عملية الغسل بخطوة "التصفيف" التي يتم فيها خلط المدخلات من أجل كسر الرابط الأولي بأصولها القذرة وفي حالة العملات الرقمية، يمكن أن تتضمن العملية استخدام بنية تحتية مخصصة أو مواقع التشفير وكازينوهات المقامرة وهي لا تتطلب اتباع قواعد ولوائح معينه ، وبالتالي تسمح بإجراء غسيل فعال للغاية أو تتعلق بالعديد من عمليات التبادل المتكررة حتى لا توجد علامة على اتصالات غير قانونية، يجري استخدامها في كثير من الأحيان.

بمجرد الانتهاء من "التصفيف" ، تبدأ مرحلة "التكامل" ، حيث يتمثل هدفها في دمج الأدوات النظيفة في النظام المالي العادي. ومع ذلك، فإن هذه الممارسة ليست تافهة وإيداع مبالغ كبيرة من الأموال في حساب مصرفي دون أي تاريخ موثق جيدًا لأصولها ليس بالتأكيد مهمة سهلة. كما أن المستخدمين غير الشرعيين يستخدمون "غسل الأموال

(33) A n d r e w t a r p e y, The money laundering risk of cryptocurrencies, Southpac Group, New Zealand,2018,pp:1-3,available on: www.southpacgroup.com

(ISSN: 2356 - 9492)

الجزئي"، حيث يتم تبادل عدد بسيط من العملات الرقمية للحصول على أوراق مالية وتودع في وقت لاحق في حسابات منتظمة، مما يجعلهم أقل تشككا. وتم استخدام هذه الممارسة من قبل كارتل الكوكايين وسمح للتجار الأوروبيين بدفع ثمن الكوكايين الكولومبي

ووفقًا لإحصاءات اليوروبول ، يقوم حوالي ٣-٤٪ من مجرمي أوروبا بغسل حصيلة جرائم فيروسات الفدية وهو ما يقدر (حوالي ٤،٢-٥،٦ مليار دولار أمريكي) ، مقارنة بممارسات غسل الأموال الإجمالية التي تمثل ٢-٥ ٪ من الناتج المحلي الإجمالي (حوالي ٨٠٠ مليار – ٢ تريليون دولار أمريكي .[٣٤]

الفرع الثاني

استخدام العملات الرقمية في تمويل الإرهاب

لا يمكن الحديث عن الإرهاب دون الحديث عن التمويل، لأهميته بالنسبة للعمليات الإرهابية[٣٥]، حيث لأهمية المال في اعداد الكوادر الإرهابية وتدريبهم للقيام بجرائمهم ، وتوفير اللوجستيات كالمعدات المستخدمة في تصنيع المتفجرات او الأسلحة او المراقبة او أماكن الايواء او التسكين .

وقد قامت الجماعات الإرهابية في لإدراكها أهمية المال في استمرارية قدرتها على ارتكاب جرائمها،[٣٦]، بالاعتماد على مصادر مشروعة من خلال المشروعات الاقتصادية التي تقوم بها، بالإضافة للأموال التي تتحصل عليها من الجمعيات أو الجهات المساندة لها. والمصادر غير المشروعة، من أهمها متحصلات غسل الأموال، وتجارة المخدرات والأسلحة والتزوير والخطف ، والسرقة والسطو المسلح ، والإرهاب الذي يعتمد على تدفق الأموال للحصول على الاحتياجات والذخائر والأسلحة التي يمكنه بها تنفيذ العمليات الإرهابية ولعل من اكبر التحديات المعروفة في مجال الاعداد

(34) ciupa katarzyna, cryptocurrencies: opportunities, risks and challenges for anti-corruption compliance systems, OECD global anti-corruption &integrity forum, 20-21 march 2019, Paris, OECD conference, p:5

(٣٥)) ليندا بن طالب: غسل الأموال وعلاقته بمكافحة الإرهاب، دراسة مقارنه – دار الجامعة الجديدة - الإسكندرية – ٢٠١١م – ص١٥١

(٣٦)) عبد القادر شهيب، ممولو الإرهاب في مصر، دار الهلال، القاهرة، ط١ ١٩٩٤، ص٨٨.

وتنظيم الأنشطة الإرهابية الدولية هي تمويل الإرهاب ، حيث تغيرت اليات نقل الأموال حول العالم بشكل كبير فتم التحول لاستخدام الذهب الالكتروني والعملات الرقمية وهو ما أصبح يعتبر من الوسائل المعقدة والتي يصعب تتبعها والمستخدمة في تمويل الإرهاب والتي وفرت أموال غير محدودة مركزيا ولا تنتمي إلى دولة ولا تخضع لتنظيم حكومي أو قانوني يحد من قيمتها أو نقلها أو يمكن وضع قيود على نقلها من شخص لأخر أو بلد إلى بلد أخر وهو ما أصبح يشكل آلية ناجزه للإرهابيين تتيح لهم نقل الأموال لمنفذي العمليات الإرهابية حول العالم دون رقابة أو قيد على حركة تلك الأموال بالإضافة لإمكانية جمع التبرعات بطرق أكثر غموضا ولا يمكن إحكام الرقابة عليها سواء في مصادر تلك الأموال أو كيفية إنفاقها كما أنها تتيح التغلب على القواعد الخاصة بقوانين البنوك بشأن تداول الأموال ونقلها عبر الحدود .

وقد أولت مختلف الدول اهتماما بمسألة تمويل الإرهاب، وقامت بتجريم وسائل تمويل الإرهاب، وإدراجها في استراتيجية مكافحة الإرهاب. وانتقل الاهتمام بهذا الجانب إلى المستوى الدولي فصدرت اتفاقية قمع تمويل الإرهاب عن الجمعية العامة للأمم المتحدة في ١٩٩٩م ،إلا أن معالجة مسائل تجريم دعم الإرهاب قد تبلور الاهتمام بها عقب صدور القرار٣٧٣ عن مجلس الأمن والذي تضمن مجموعة من الالتزامات ذات الطابع التشريعي والهادفة إلى تجريم جميع أشكال الدعم وتمويل الإرهابيين[٣٧].

وقد انتشرت مؤخرا العملات الرقمية، بالرغم من ان مفهومها وطرق استخدامها والمخاطر المترتبة على التعامل بها لازالت غير واضحة وبخاصة تأثيراتها على امن الدول، وقد رصدت اجهزة الامن ان المنظمات الارهابية تستخدم العديد من الطرق لتمويل الانشطة الارهابية ومن الوسائل التقليدية في هذا الإطار تحويل الاموال من خلال البنوك الدولية بينما تتعاظم امكانية تمويل العمليات الارهابية وانشطة الجماعات

(٣٧)) صدر عن مجلس الأمن الدولي مجموعة قرارات للحد من تمويل الإرهاب منها: القرار ١٢٦٧ في ١٥ أكتوبر ١٩٩٩ بخصوص تجميد الأموال والموارد المالية الأخرى لحركة طالبان في سبتمبر ١٩٩٦. القرار ١٣٦٣ في ٣٠ يوليو ٢٠٠١ الخاص بإنشاء آليات متابعة تنفيذ التدابير الواردة في القرارين ١٢٦٧ و١٣٣٣. -القرار رقم ١٣٣٣ في ١٩ ديسمبر بخصوص تجميد أموال وموارد أسامة بن لادن زعيم تنظيم القاعدة.

(ISSN: 2356 - 9492)

المتطرفة من خلال استخدام العملات الرقمية. كما رصدت العديد من تلك التمويلات للجماعات الارهابية باستخدام العملات الرقمية والذي يتعذر تتبع عمليات التحويلات التي تتم باستخدامه.(٣٨)

ومستخدم الانترنت لابد ان يترك بصمته الرقمية فعند استخدام الحاسوب يتم انشاء سجل يعطي انطباعا عن الافكار والعادات الخاصة للفرد فكل حاسوب متصل بالإنترنت له بصمة الكترونية تسمي عنوان بروتوكول الانترنت والذي يحدد من ناحية اخري المكان الفعلي لمستخدم الانترنت ويعرفه بانه مستخدم هذا الحاسوب والعنوان ، وعندما ظهرت شبكة تور وهي اشهر محرك بحث يمكن استخدام الانترنت الخفي من خلاله والتي تتسم بالقدرة على اخفاء العلاقة بين الحاسوب وعنوان بروتوكول الانترنت الخاص به كما توفر آلية للحفاظ على الخصوصية لمستخدميه وقد تم تطوير هذه الشبكة في معامل الابحاث بالبحرية الامريكية كأحد التكتيكات العسكرية للتخفي عبر الانترنت فيتتبعون الاهداف دون ان تتمكن من رصدهم حيث تتسم الشبكة بقدرتها على جمع المعلومات الاستخباراتية الخاصة بالدول الأخرى دون ان تستشعر اجهزة الامن في تلك الدول بهذه المراقبة كما انها تتيح لرجال الجيش القدرة على استخدام الموارد الالكترونية والتي تتم ادارتها ومراقبتها من قبل المتمردين دون كشفهم كما ان جهات انفاذ القانون تستخدم تقنيات مماثلة لتعزيز حماية الخصوصية عند اجراء عمليات التخفي عبر الانترنت لحماية الهوية الشخصية لرجال انفاذ القانون .(٣٩)وسوف نتناول الحديث عن ماهية الشبكة العميقة وآلية عملها ومميزاتها لمرتكبي الجرائم وعلاقة العملات الرقمية بالشبكة العميقة ومدي استخدام العملات الرقمية في تمويل الإرهاب.

أولا: ماهية شبكات التخفي

(٣٨)) تشيلسي اية لويس – التخفي "نظرة متعمقة في شبكة تور (شبكة تخفي) وآثارها على امن الحاسوب وحرية الرأي والتعبير في العصر الرقمي" – مقال منشور في مجلة معهد دبي القضائي – السنة الثالثة – العدد الخامس – فبراير ٢٠١٥م

(39) Vandervort, David, Dale Gaucas, and Robert St. Jacques, “Issues in Designing a Bitcoin-Like Community Currency,” paper presented at the Second Workshop on Bitcoin Research, San Juan, Puerto Rico, January 30, 2015

توفر شبكات التخفي(Deep Web) الامن والسرية للمستخدمين عند تداول المستندات التجارية وحماية المصادر المجهولة وتزويد الناشطين بوسائل فعالة للحماية فتوفر للمعارضين ملاذا أمنا وكذا المجرمين ، وعلى ذلك فان الشبكة تحقق الخصوصية لمستخدميها الا ان استخدام الشبكة من جانب القطاع الخاص يؤدي الى ظهور حواجز متعلقة بالتحقيقات في المسائل العسكرية والجنائية ومثال ذلك الدور الذي لعبته تلك الشبكات في تسريبات وثائق ويكيليكس حيث سمحت للمسربين بتحميل العديد من الوثائق التي تم تسريبها دون تمكن الاجهزة الامنية من كشف هويتهم وهو ما شكل تهديدا كبيرا لأمن العمليات العسكرية الامريكية في شتى بقاع العالم الا انه من ناحية اخري يحمي المبلغين عن الفساد والاعمال الاجرامية واسعة النطاق كجرائم العصابات المنظمة ، ولعل ما يثور هنا هو مدى امكانية المفاضلة بين اعتبارات الخصوصية والامن وهنا تثور اشكالية مدى اعتبار الشبكة اداة تساعد على نشر الفكر الارهابي والاجرامي فالحقيقة ان هذه الشبكة قد تعتبر منبرا لحماية الخصوصية في الاتصالات القانونية الا ان الحقيقة انها اصبحت تستخدم في الاغراض غير القانونية كتبادل الاتصالات والتكليفات فيما يتعلق بالأنشطة الارهابية والجنائية والتي ترتكب بعيد عن الرقابة الامنية ومن ثم فقد اصبحت الشبكة احد وسائل الدعم الفعلي للإرهاب ومن ذلك نقل الاموال الافتراضية كالعملات الرقمية والذي يتم من خلالها حتي لا يمكن تتبع مصادر تلك الاموال ولا متلقيها(٤٠)

كما تستخدمها الشركات لحماية سرية بياناتها والصحفيين لحماية المصادر المجهولة والابحاث الحساسة وعلى ذلك فان شبكة تور تعد من اكبر شبكات التخفي والتي تسهل عمليات التواصل الخفية من خلال مجموعة من الحواسيب حول العالم وتعمل شبكات التخفي من خلال الانترنت وتتطلب مزايا معينة وتوفر مفاضلة بين

(40) Shubhdeep Kaur, Sukhchandan Randhawa, Dark Web: A Web of Crimes, Springer Science+Business Media, LLC, part of Springer Nature 2020, pp:3-7, https://www.researchgate.net/publication/338878596_Dark_Web_A_Web_of_Crimes/link/5f1600a84585151299ab503b/download

(ISSN: 2356 - 9492)

التخفي وقابلية الاستخدام والكفاءة وقد تم اتاحة مزاياها للجمهور في ٢٠٠٤م وتوفر حاليا العديد من المشروعات مفتوحة المصدر ويمكن للمستخدمين استخدام البرنامج بتحميلة من شبكة الانترنت كما يمكن اخفاء مكان المستخدم للشبكة حيث تقوم شبكة التشفير المعقد بعزل الاتصالات عبر الانترنت عن عنوان بروتوكول الانترنت المصدري له لإخفاء الموقع الحقيقي للمستخدم بشكل فعال ويقوم البرنامج بالربط بين ثلاثة خدمات وكيلة كل منها مزود بمفتاح تشفيري فردي خاص بها ويقوم عقب ذلك البرنامج بإنشاء سلسلة جديدة من الاجهزة الخادمة ومفاتيح التشفير لكل مستخدم على فترات متقاربة ومن خلال عملية تسمي التسيير البصلي ترتد كافة الاتصالات الموجهة من خلال الشبكة الى عقد مختلفة او خوادم وكيلة في كل انحاء العالم قبل وصولها لوجهتها النهائية وبعد ذلك يدخل حاسوب المستخدم الى الشبكة يتم توجيه معلومات المستخدم من خلال سلسلة عشوائية من عقد المرحل قبل التوجيه الى عقدة الخروج التي ترسل المعلومات الخاصة بالمستخدم الى الانترنت الفعلي كما ان كل عقدة تتصل فقط بالعقد التي تسبقها وتليها مباشرة ومن ثم يكون حاسوب المستخدم متصل بالعقدة الاولى في السلسلة ويتصل الانترنت فقط بالعقدة الاخيرة في السلسلة وعلى ذلك تكون الحركة من الشبكة يمكن تعقبها فقط عند عقد الخروج بشكل يختلف عن المصدر الحقيقي للبيانات .[٤١]

وتمكنت الجماعات الارهابية من التواصل بسرية تامة، ولكن ليس باستخدام مواقع "تويتر" و"فيسبوك"، حيث يسهل اختراقها والتوصل لمواقع المستخدمين، فاستخدموا الـ"Deep Web"، حيث يمكنهم العمل بسرية، ولا تستعمل "الشبكة العميقة" المتصفحات التي تعرض المحتوى السطحي للانترنت، بل تسخر أنظمة معقدة تسمح لمستخدمها باستخدام الشبكة دون رقابة وتتيح له المجهولية، من خلال البرامج والمتصفحات الخاصة مثل"Onion Tor" .

(٤١)) دومينيك هيرمان ، رولف ويندولسكي وهانز فيدراث ، التسلل الى المواقع الالكترونية : تقنيات تحسين التسلل الى الخصوصيات العامة مع مصنف متعدد الحدود مبني على خوارزمية (Naïve Bayes) ، (٢٠٠٩):http://dl.acm.org/citation.cfm?doid=1655008.1655013/

ويمكن لأي شخص الولوج إلى الشبكة العميقة، التي لها جوانب إيجابية دون شك، حيث تتيح التواصل السري للمستخدمين، سواء لتبادل المعلومات او لأهداف أخرى ذات نفع للمستخدم ولا تشكل نشاطا اجراميا، كما تستخدم أيضا لارتكاب أنشطة غير قانونية، وتعتبر متطورة بشكل كبير عن مثيلتها العادية وهي الانترنت العادي ومن مظاهر هذا التطور التقني امتلاكها لعملة خاصة تشترى وتتبادل العملات الرقمية. (٤٢)

وتتم التعاملات المالية المرتبطة بالحسابات البنكية للمستخدمين بصورة سرية، وبالرغم من السعي الدائم من الأجهزة الأمنية لتحديد أماكن الخوادم الرئيسية وإغلاق مواقع الأنشطة الاجرامية وتحديد هوية مديريها وضبطهم، فإن الجانب الأخطر لها هو ارتباطها بالتنظيمات الإرهابية والمتطرفة، التي تستخدمه للتواصل فيما بين عناصرها وتمويل عملياتها نظرا لتمتع مستخدميها بعدم إمكانية تتبع مواقع اجهزتهم او تحديد هوياتهم.وهناك العديد من الحسابات الوهمية على موقعي "فيسبوك" و"تويتر" لإرهابيين وتنظيمات ارهابية، ومنتديات تحرض على الارهاب وتسعى لاستقطاب العناصر التي يمكنها الانضمام للجماعات الارهابية، الا ان التنسيق وتظيم العمل الارهابي بين المنظمات الارهابية المختلفة لا يتم باستخدامها، بل تلجأ إلى استخدام شبكات خاصة تنشئها لهذا الغرض او تقوم بالاستيلاء عليها واستخدامها ضمانا لعدم قدرة الأجهزة الأمنية على رصدهم وتحديد هوياتهم.

ويوجد لدى تنظيم "داعش"، إدارة مختصة بالتواصل واستخدام الشبكة العميقة لحمايته من الملاحقة والاختراق وتأمين تبادل المعلومات والتمويل، وهذا ما تحاول الاستخبارات الأميركية مواجهته، نظرا لوجود ملفات نصية تشرح طرق التبرع للتنظيم ، وتبين أهمية بذل المال للجهاد ويشرح كيفية التبرع بالأموال عبر الشبكة العميقة."(٤٣)

(42) Gebin George & others, Hands-On Dark Web Analysis, 2018 Packt Publishing, pp:77-80, https://dl1.newoutlook.it/book/2020/08/Darkweb.pdf

(43))https://arabic.rt.com/news/808846-%D8%AA%D9%86%D8%B8%D9%8A%D9%85%D8%A7%D8%AA-%D8%A5%D8%B1%D9%87%D8%A7%D8%A8-%D8%AF%D8%A7%D8%B9%D8%B4

(ISSN: 2356 - 9492)

ويعيش في قاع الانترنت كذلك مواقع مرتبطة بكافة انماط الجريمة والافعال المشينة والشاذة التي تخرج عن نطاق الانسانية والسلوك البشري الموافق للفطرة الانسانية كجرائم القتل، وصولاً للأكثر اجراما، وهي مواقع الاستغلال الجنسي للأطفال.

تعتبر الشبكة العميقة متطورةً لدرجة أنها تمتلك عملة رقمية تُشترى وتتبادل وتتم التعاملات المرتبطة بحسابات البنوك للمستخدمين بصورة سريّة، وتعتبر آمنه إذا كان الموقع موثوقاً، وإلا قد يقع ضحية للاحتيال.(٤٤)

ثانيا: الشبكة العميقة والأعمال الإرهابيّة

بالرغم من المحاولات الدائمة من قبل أجهزة انفاذ القانون في العديد من الدول للوصول الى مواقع الخوادم وإغلاق مواقع الارهابيين والتنظيمات الارهابية وضبط مشغليها، فإن الجانب الأخطر للشبكة المظلمة مرتبط بالجماعات الإرهابية التي تستخدمه للتواصل ونشر جرائمها بهدف اثارة الرعب والفزع بين المتابعين لتلك المواقع.

ويوجد في فيسبوك وتويتر العديد من الحسابات الوهمية لإرهابيين وجهاديين وتنظيمات مسلحة، بالإضافة لمنتديات عديدة، لكن التواصل بين تلك الجماعات الإرهابية يتم من خلال مواقع خاصة بها.

خلال العقد الماضي، لم يقتصر النشاط الإرهابي في الشبكة العميقة على مواقع ومنتديات على الشبكة المظلمة والمواقع التي يتم استخدامها عند تعرض الموقع الرئيسي للقرصنة أو الغلق والتي يمكن تسميتها بالموقع البديل، فقد قام التقنيون في هذه المنظمات الارهابية باعداد برامج تشفير أشهرها "أسرار المجاهدين"، وصدر منه إصدار ثاني في ٢٠٠٨ ثم تم تطوير تطبيق للتراسل الفوري خاص بالهواتف الذكية.

%D8%A7%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%AF%D8%A7%D8%B1%D9%83-%D9%88%D9%8A%D8%A8/

(44) Cynthia Dion-Schwarz, David Manheim, Patrick B. Johnston, Terrorist Use of Cryptocurrencies: Barriers and Future Threats, Copyright 2019 RAND Corporation, pp:23-27, https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3026/RAND_RR3026.pdf

عام ٢٠١٣، صدر عن "لجنة الفجر التقنية" تطبيق جديث سمي "أمن المجاهدين" لتأمين اتصالات الارهابيين وتبادل تفاصيل العمليات بامان.

وتحاول العديد من الدول إحكام السيطرة على العمليات والتفاعلات على الشبكة المظلمة، لذا تأسست "القوات الخاصة لمكافحة الجرائم الرقمية" في الاتحاد الأوروبي، بدعم من مركز الجرائم الرقمية الأوروبيّة، بهدف مكافحة الجرائم والانشطة المشبوهة في أوروبا والولايات المتحدة بالتعاون مع مكتب التحقيقات الفيدرالية والأمن الوطني، ومن المؤكد انه لا يمكن التيقن من امكانية السيطرة على ما يحدث في الشبكة المظلمة، لصعوبة ذلك.(٤٥)

فالإنترنت يشمل ما نراه على الشبكة العادية وكذا تلك التي لا يمكن تداوله عبر الشبكة العادية للإنترنت يمكن باستخدام الشبكة المظلمة الوصول اليه بل ومناقشته في اطار كامل من المجهولية للأطراف وعدم إمكانية تحديد هوياتهم او مواقعهم.(٤٦)

وقد انتشرت في الآونة الأخيرة التنظيمات الإرهابية حول العالم، لزعزعة الأمن والاستقرار العالمي، وتم تمويل عناصر تلك التنظيمات باستخدام البت كوين، حيث استخدم لتمويل الأنشطة الإرهابية، وأثارت وثيقة لأحد تابعي تنظيم «داعش» الإرهابي بعنوان "العملات الرقمية وصدقة الجهاد"، حددت الأحكام الشرعية لاستعمال "البت كوين"، وضرورة استعمالها لتمويل الأنشطة الجهادية، اهتمام وسائل الإعلام العالمية ومواقع التواصل الاجتماعي.

وتصمنت الوثيقة أن العملات الرقمية تمثل حلا للمشكلات التي تواجه التنظيمات الارهابية بسبب القيود على تداول الاموال والتي تديرها وحدات مكافحة غسل الاموال بالبنوك وشركات نقل الاموال، وشرحت طرق استخدامها وإنشاء الحسابات على مواقع تلك العملات الرقمية، ونقل الأموال خفية، ودفع ذلك جهات انفاذ القانون ومكافحة

(45))http://www.huffpostarabi.com/2016/01/25/story_n_9059062.html
(46)) http://www.migliorisiabogados.com/que-es-la-deep-web-que-peligros-esconde/?lang=ar

(ISSN: 2356 - 9492)

الارهاب لدراسة التهديدات الأمنية المحتملة لهذه المعطياتللوصول لالية لتعقب تلك الاموال .

ومنذ أن تم ابتكار العملات الرقمية عام ٢٠٠٩، أصبحت العملات الافتراضية الاكثر انتشارا واستخداما بشكل كبير جدا في مجال الدفع في عمليات الاتجار بالمخدرات والاسلحة بل وايضا دفع مقابل عمليات الاغتيال والاستئجار على القتل، وتوصف العملات الرقمية بأنها وسيلة الدفع الافتراضية الاكثر غموضا وتأثيرا على كافة الحكومات، فقد تنوعت النقود الافتراضية منذ نشأتها الى أكثر من ٦٥٠ شكل مختلف. ولكن مؤخرا قامت الجماعات الارهابية كتنظيم الدولة الاسلامية بوضع العملة الافتراضية (البت كوين) موضع اهتمامها حيث اعتمدت عليها بشكل كامل في تمويل عملياتها الارهابية على المستوي الدولي.[٤٧]بينما قامت حكومة الولايات المتحدة الامريكية باتخاذ العديد من الاجراءات لتوضيح المخاطر الامنية مثل العروض التكنولوجية والمعالجات الغير مناسبة التي اتخذت بواسطة السلطات الفيدرالية والتي ترتب عليها مخاطر هائلة تعرضت لها الولايات المتحدة. وهذه المعالجات الغير مناسبة بالإضافة الى الطبيعة غير الملموسة والتقنية لهذه العملة الافتراضية شكلت عائقا كبيرا امام الحكومة الفيدرالية جعلت التشريعات التي تجرم تمويل الارهاب غير فعالة ويصعب تطبيقها، ومن الضروري فهم وسائل الدفع الافتراضية كشكل من اشكال العملات القانونية ووضع تصور للقوانين التي يحتاج اليها في هذا الإطار.

ثالثا: الصلة بين العملات الرقمية وتمويل الارهاب

تم ابتكار العملات الرقمية من خلال شخص او مجموعة من الاشخاص تحت اسم (ساتوشي ناكاموتو) اما البداية الحقيقية فقد تمت عندما قرر ناكاموتو بان العملات الرقمية قد تم اطلاقها بهدف التخلص مما يسمى الثقة المبنية على القوالب الجامدة والتي تأسست على الطرف الثالث في المعاملات وهي البنوك عندما بدأت في تفعيل التحويلات عبر الانترنت ونفس الوثيقة ناقشت مسائل التكاليف الكبيرة للتحويلات

(47))History of Bitcoin: the world's first decentralized currency , http://historyofbitcoin.org/(last visited Jan.23,2016).

ومحدودية حجمها ، وتلك المعوقات ليست فقط امكانية تنظيم تلك التحويلات الحديثة ولكن تطوير التكلفة الخارجية مع فقد القدرة على حفظ معلومات عمليات الدفع مقابل الحصول على خدمات غير قابلة للحفظ .[٤٨]

ان آلية عمل العملات الرقمية تعتمد على نظام اللامركزية في نقل الاموال الالكترونية وهو ما يعني عدم امكانية التحكم فيها سواء من أي بنك او حكومة فالعملات الرقمية قد احلت النظام المشفر (القدرة على الاداء) محل النظم المعتمدة على الثقة.

وبتتبع اول عملية تبادل للبت كوين والتي تمت في فبراير ٢٠١٠، قامت المنظمات الارهابية والحكومات على حد سواء بالوضع في الاعتبار ان العملات الرقمية توفر بيئة مناسبة لتمويل العمليات الارهابية دون القدرة على تتبع تلك العمليات، كما ان المنظمات الحكومية الدولية العاملة في مجال مكافحة غسل الاموال قد قامت بتعميم توضيح يتضمن معلومات حول مدي قدرة المنظمات الارهابية على اخفاء مصادر تمويل عملياتهم باستخدام العملات الرقمية، وفي اكتوبر ٢٠١٠م قامت اكبر مؤسسات تغيير العملات الافتراضية العملات الرقمية(MT.Gox) بتغيير الاسس التي تتبعها في تلقي مقابل الخدمات التي تقدمها الى اقتضاؤها بالعملات الرقمية وسميت بالعملة الحرة ، هذه العملة كانت غير قابلة للإلغاء في فبراير ٢٠١٤م والتي صاحبت اصدار بت كوين بمبلغ ٤٥٠ مليون دولار .[٤٩]

ان اللامركزية والغموض هما السمة التي تتسم بها عملة العملات الرقمية والعديد من المنظمات الارهابية قد لجأت لاستخدام تلك التكنولوجيا التي بدأت في العراق وسوريا في جمع العملات الرقمية كمصدر لتمويل عملياتها المحتملة في الولايات المتحدة الامريكية، كما ان جميع عمليات الاختراق التي تتم بمعرفة سلطات مكافحة الارهاب عبر الانترنت قد رصدت وجود محافظ مالية لتداول العملات الرقمية مملوكة لتنظيم الدولة الاسلامية (داعش) وتزيد قيمة العملات الرقمية الموجود بها عن ملايين

(48))Satoshi Nakamoto , bitcoin : A Peer – to – Peer Electronic Cash System , Bitcoin Project , https://bitcoin.org/bitcoin.pdf(last visited Jan.22,2016).
(49)) Paul Anning , Stuart Hoegner,& Jerry Brito , The Law of Bitcoin, 2015.

(ISSN: 2356 - 9492)

الدولارات ، وقد تبين ايضا ان هذه التمويلات قد رصدت لتمويل عمليات ارهابية في الولايات المتحدة الامريكية وتونس وقد وضعت السلطات في كلا البلدين ما تم رصدة موضع الاعتبار واتخذت اجراءات جادة في هذا الشأن وفي ضوء هجمات نوفمبر ٢٠١٥ م في باريس فقد تنبه العالم اجمع الى خطورة ما يسمى بالعملات الافتراضية في العالم المتحضر ، يضاف الى ذلك انه في العام ٢٠١٤ م تم ضبط على المدعو / على شوقي امين في الولايات المتحدة الأمريكية وذلك لتقديمه توجيهات بشأن كيفية استخدام العملات الرقمية لدعم تنظيم داعش الارهابي.(٥٠) كما بين الاتحاد الأوروبي وسائل للحد من استخدام العملات الرقمية في تمويل الارهاب.(٥١)

ويمكن للتعرف على كيفية تمويل المنظمات الإرهابية باستخدام العملات الرقمية هو فهم كيفية قيام العملة الافتراضية بوظيفتها في تمويل الإرهاب كعملة غير مركزية دون الحاجة إلى دعم من نظم التمويل المركزية، وتهتم معظم الحكومات بالعملات الورقية فقط وهو ما يعني أن الأموال لا يشترط ان تكون على شكل ذهب او فضة، وتاريخيا فان العملة الورقية للدولة تقوم غالبا بالذهب أو الفضة.

كما أن أحد أساليب تعامل وزارة الخزانة الأمريكية مع قيمة تداول الدولار هو التحكم في قيمة تداول العملة، والعبء لرفع القدرة على الاكتفاء الذاتي، وإيجاد مستويات توظيف عالية، استقرار الأسعار لدعم القوة الشرائية للعملة وإيجاد استثمارات طويلة المدى وتحقق أنظمة البنوك المركزية هذه الأهداف بدراسة الاقتصاد وتوقع التغيرات المستقبلية في السوق العالمي.(٥٢)

(50)) Deborah Hastings ,Va. Teen gets 11 years in prison for tweeting about ISIS , aiding the terrorist group ,N.Y. Daily News (Aug.28,2015),http://www.nydailynews.com/news/national/va-teen-11-years-rpison-aiding-isis-article-1.2340577.

(51)) Marry-Ann Russon, Paris attacks: EU to crack down on bit coin transfers in attempt to strange Isis funding, Int'1 Bus. Times (Nov.20, 2015, 11:50 AM),http://wwwibtimes.co.uk/paris-attacks-eu-crack-down-bitcoin-transfers-attempt-strangle-isis-funding-1529693 .

(52)) Mark Koba , The federal Reserve: CNBC Explains ,CNBC (Mar.18,2015, 9:21 am), http://www.cnbc.com/id/43752521.

كما تقوم هيئات طباعة الأوراق المالية بتطبيق آليات جديدة لتامين العملات التي تقوم بإصدارها لمنع تزويرها، أما العملات الرقمية فتعمل بنفس الطريقة التي يتم بها إنتاج العملات الحكومية الورقية مع استثناء أنها ليست تحت السيطرة من خلال أي نظام مركزي فهذه العملات الافتراضية ليست مدعومة من أي نظام تقويم سلعي.

ان القاعدة العامة في نظم البنوك المركزية في شأن العملات الرقمية قد استبدلت ببرامج مركزية مفتوحة المصدر، فمن بين الخدمات الأخرى فان هذه البرامج تنظم آليا طالما أن هذه العملات الافتراضية يتم إدارتها داخل منظومة ذات إطار زمني معين وفي دورة مدعومة من خلال المستخدمين لعملة البت كوين.[٥٣]

صارت غالبية العملات الافتراضية تتبع أسلوب الند للند في تبادل العملات، كما ان مستخدمي العملات الافتراضية أصبحوا يضعون عملاتهم الافتراضية في محافظ الكترونية حيث يمكنهم استخدامها في إرسال واستلام المقابل لها من البضائع أو غير ذلك مما يعادل قيمتها التي يتم إنتاجها.

كما ان إصدار واستلام الطلبات المشفرة لتلك المحافظ الالكترونية لاستبدالها بالبضائع تماثل تماما تلك العمليات التي يتم بها التنقيب عن العملات الافتراضية والتحقق والحصول على التحويلات والتي لا تتضمن فقط الاستخدام الشامل ولكن الذي يتسم بالغموض أيضا.[٥٤]

إن أي تهديدات أمنية يجب أن تحدد وان مجموعة تطوير العملات الرقمية يجب أن تعالج البرنامج الأساسي للبت كوين وكذا التطوير الذي يحتاجه المستخدمين له ، كما أن أوعية المنقبين عنه والبرامج الأساسية لهذه العملات الافتراضية لا يمكن أن يتم وضعها على حاسوب واحد أو بنوك الحواسيب وهؤلاء المنقبون يتلقون حظرا على تحويلات العملات الرقمية التي تم إعدادها باستخدام معادلات رياضية شديدة التعقيد

(53)) Kevin Drumm , Bitcoin is a fait Currency ,But That's not Its big Problem , Mother Jones (Feb.25,2014,11:54am) ,http://www.motherjones.com/Kevin-drum/2014/02/bitcoin-fait-currency-that’s-not-its-big-problem.

(54)) Edward Murphy , Federation of American Scientists , Cong .Research Serv.(Nov.12,2015) ,http://www.fas.org/sgp/crs/mist/R43339.pdf.

(ISSN: 2356 - 9492)

والتي تتطلب جهدا كبيرا من الحواسيب وشبكات المعلومات التي يتم من خلالها التعامل عليها لفك شفرتها.، وبحل ذلك الحظر على التحويل فان المنقبون لا يؤكدون فقط صلاحية العملة الافتراضية ويجيزون التعامل بها بل يتلقون مكافآت من واضعي البرامج نفسهم .

إن صعوبة حل سلاسل التحويلات تزيد وتنقص اعتمادا على المدة الزمنية التي يستغرقها المنقبون في شبكة العملات الافتراضية للوصول لحل العدد المحدد سلفا من التحويلات المحظورة ، كذلك فان منشئي العملات الرقمية يمنحون مكافآت لهؤلاء الذين يقومون بحل المشكلات الناجمة عن عمليات حظر التحويلات لتلك العملة المنقب عنها التي تتزايد بمضي الوقت ، هذه الملامح طبقت بتصميم لكي يتم تنظيم الكمية التي يتم إنتاجها من العملات الرقمية وطرحها في السوق دون أي تنظيم من البنوك المركزية(٥٥)

المبحث الثاني

الجرائم التي تقع على العملات الرقمية

تمهيد وتقسيم:

تستخدم العملات الرقمية في ارتكاب الجرائم وتمويل الأنشطة الإرهابية كما بينا وذلك لما تتسم به من خصائص وسمات تتيح لمرتكب الجريمة باستخدامها التخفي والمجهولية التي يسعى اليها الا ان هناك أيضا جانب اخر هام في الجرائم التي ترتكب ضد تلك العملات من اجل الحصول عليها او اتلافها او تقليدها وذلك لما تتمتع به من خواص بالإضافة لقيمتها الكبيرة وسوف نقوم بدراسة الجرائم التي تقع على العملات الرقمية الى عدة مطالب على النحو التالي:

المطلب الأول: هجوم الدفع المضاعف Double-spend

المطلب الثاني: هجمات البنية التحتية وكسر **خوارزمية الدمج SHA-256**

(55) Y N C T C , DHS, FBI, NCTC Identifying and Preventing Illicit Use of Cryptocurrency by Terrorists, 23 S E P T E M BER 2021, pp:3-5, https://www.odni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/119s - First Responders Toolbox - _Identifying_and_Preventing_Illicit_Use_of_Cryptocurrency_by_Terrorists.pdf

المطلب الأول

هجوم الدفع المضاعف Double-spend

إن هجوم الدفع المضاعف Double-spend أو ال % ٥١ هي اسلوب اجرامي يتم باستخدام كم كبير من الطاقة لاجراء تحويلات احتيالية ومُزوَّرة بالعملة الرقمية ذاتها مرتين، مما يترتب علية إلغاء أحد التحويلين، فإذا تمكن القائم بالتعدين، الذي يملك القدرة على التحكم بمعدل الهاش من حلّ مسائل إثبات العمل بسرعة، عندئذ يمكنه توجية عملة للعملات الرقمية على البلوك تشين العامة التي يتم عليها التأكيد، وفي ذات الوقت يعدن سلسلة منقسمة موازية من خلال تحويل آخر للعملات الرقمية نفسها الى عنوان آخر له، فيحصل متلقي التحويل الأول على التأكيد وهنا يقوم المهاجم باستخدام طاقة المعالجه الخاصة به لجعل السلسلة الأخرى أطول. وينجح الهجوم إذا امكن للجاني جعل السلسلة الأخرى أطول من الأولى، وعندها سيظهر لمُستلم التحويل الأول أن العملات التي تسلمها اولا قد اختفت.

وكلما زاد معدل الهاش الخاضع لسيطرة المهاجم، زادت قدرته على جعل السلسلة الاحتيالية أطول من السلسلة العامة، وبالتالي يمكنه إلغاء تحويله وتحقيق مكاسب مالية، وكلما زادت مدة انتظار المتلقي للتأكيد، تقلصت فرصة نجاح المهاجم، وإذا كان الملتقي يمكنه انتظار الحصول على ستة تأكيدات، فسيقل احتمال نجاح الهجوم اكثر، وتبدو هجمة ال ٥١ % ممكنة تقنيا، الا ان الدوافع الاقتصادية تعوقها بشكل كبير. فإذا نفَّذ معدِّن الهجمة بنجاح، سيقلل ذلك من الدافع الاقتصادي لاستخدام العملات الرقمية، وبذلك سيقل الطلب على العملات الرقمية. ومع تزايد تعدين العملات الرقمية ليصبح قطاعا قائما على كثافة رأس المال باستثمارات كبيرة مسخرة لإنتاج العملات، يزداد اهتمام المعدنين بالمحافظة على نزاهة الشبكة، حيث ترتبط قيمة مكافآتهم بذلك. ويشار الى أنه لم تسجل هجمة إنفاق مزدوج ناجحة على أي من تحويلات العملات الرقمية الحاصلة على توثيق واحد على الأقل.(٥٦)

(٥٦) وأقرب محاولة ناجحة للإنفاق المزدوج شهدتها العملات الرقمية كانت عام ٢٠١٣، حيث كان موقع مراهنة للعملات الرقمية يسمى " Bitcoin Dice للعملات الرقمية دايس" يحوي ما يُقدَّر

(ISSN: 2356 - 9492)

ويمكن تنفيذ هذه الهجمات نظريا إن لم ينتظر متلقي المدفوعات حتى يتم إنتاج بلوك تشين جديدة تؤكد مصداقية التحويل. ومن الناحية العملية فان الهدف المالي يعوق ملاك طاقة المعالجة لذا لم تنجح هذه النوعية من الهجمات على المحول لهم الذين انتظروا توثيقا واحداً على الاقل لذا فان هذه الهجمات لن تنجح إذا كانت تستهدف تحقيق الربح، اما اذا استهدفت هذه الهجمات القضاء على منظومة العملات الرقمية فالوضع عندئذ يختلف، فاذا ارادت جهة حكومية أو خاصة الحصول على سعة تعدين للاستيلاء على غالبية الشبكه، واستخدام طاقة المعالجة للقيام بهجمات إنفاق مزدوج لخداع المستخدمين والقضاء على أمان الشبكة، فان الطبيعة الاقتصادية للتعدين ستقف بشكل كبير ضد حصول ذلك الحدث.

وحيث ان طاقة المعالجة سوقٌ عالمية تنافسيةٌ، ويعتبر تعدين العملات الرقمية من اهم استخداماتها، وأكثرها ربحا فقد يبحث المهاجم عن ثمن الاستيلاء على ٥١ % من طاقة المعالجة المستخدمة لشراء المعدات اللازمة لذلك، الا انه إذا خصص قدرا كبيرا من موارده لشراء معدات تعدين العملات الرقمية، فسيؤدي ذلك لارتفاع سعرها، مما سيحفز المعدِّنين للاستثمار في شراء معدات التعدين ، بالاضافة لاستثمار رأس مال أكبر في إنتاج طاقة التعدين، مما سيقلل ثمن طاقة المعالجة وسيزيد من سرعة نمو معدل طاقة المعالجة للعملات الرقمية.(٥٧)

وسيبقى المهاجم دون أفضلية، حيث يؤدي شرائه لمعدات التعدين لنمو سريع في طاقة المعالجة المستخدمة في التعدين التي لا يمكنه التحكم بها. وعلى ذلك فكلما زادت الموارد المصروفة على إنتاج طاقة المعالجة للهجوم على نظام انتاج العملات الرقمية، زادت سرعة نمو طاقة المعالجة فيه وزادت صعوبة القيام بهجمات تستهف نظم معلومات العملات الرقمية المشفرة.

بمجموع ١٠٠٠ عملة للعملات الرقمية) تقدر قيمتها بحوالي ال ١٠٠,٠٠٠ $ في ذلك الوقت(، وتمت سرقة العملات منه في هجمة إنفاق مزدوج باستخدام مصادر تعدين هائلة. على كل حال، لم تنجح الهجمة إلا لأن موقع ال " للعملات الرقمية دايس " كان يقبل تحويلات بلا أي توثيق عليها، مما جعل تكلفة الهجمة زهيدا نسبياً.

(57) Andes: Bitcoin's kryptonite: The 51% attack. https://bitcointalk.org/index.php?topic=12435 ,(June 2011),pp:3-5

لذلك بينما يمكن تقنيا تنفيذ هذا النوع من الهجمات، إلا أن اقتصاد الشبكة سيجعل من نجاحه أمرا غير مرجح الحدوث، فيمكن الهجوم على العملات الرقمية عبر الاستيلاء على البنية التحتية الخاصة بالتعدين واستغلالها بهدف غير ربحي للتقليل من أمن وحماية الشبكة، لكن بما ان تعدين العملات الرقمية هي عملية موزعة جغرافيا فان هذا الاحتمال يصبح صعب التحقق ويحتاج لتعاون من عدة حكومات عبر العالم، ولهذا فان أفضل طريقة لتحقيقه ستكون بالاستيلاء عليها عبر الثغرات الموجودة بلأجهزة وليس بالاستيلاء على معدات التعدين ماديا.

ولما كان ثمة احتمالية للتشويش على شبكة العملات الرقمية أو تدميرها بإفساد الأجهزة المشغلة للنظام البرمجي الخاص بالعملات الرقمية لكي تصبح متاحة لأطراف خارجية، يمكن دس برمجيات خبيثة لا يمكن رصدها في عقد التعدين تسيطر بها الأطراف الخارجية على معدات التعدين، وبذلك يمكن تعطيل تلك المعدات و السيطرة عليها عن بعد في ذات وقت تنفيذ هجمة ال ٥١ % ويمكن ايضا التجسس تكنولوجيا بتنصيب الوسيلة التقنية على حاسوب يسمح بالدخول لحساب العملات الرقمية للمستخدم والوصول لمفاتيحه الخاصة. وهذة الهجمات تؤدي لتقليل الثقة في العملات الرقمية وكذا تقليل الطلب عليها.

ويمكن تنفيذ هذه الهجمات تقنيا ولا يشترط نجاحها بشكل كامل لتربك العملاء وتؤذي سُمعة العملات الرقمية، كما قد تنجح هذه الهجمات على اجهزة التعدين اذا كان المعدنين ومُصنِّعي معدات التعدين قليلين، وهو ما قد يؤدي لفشل العملات الرقمية. الا انه مع نمو التعدين، سينجذب صانعي الأجهزة لصناعة معدات التعدين، مما سيقلل الأثر السلبي على الشبكة حال اختراق معدات صانع أجهزة واحد.

وهذه الخطورة أقل تأثيرا على الشبكة مع وجود الحواسيب الشخصية وذلك لوجود عدد كبير من صانعي الأجهزة في دول العالم المختلفة لديهم معدات ولوج لشبكة العملات الرقمية. فإذا كان مُنتِجي الأجهزة مخترَقا وتم كشف ذلك، فسيؤدي ذلك لانتقال المستهلك لمُنتِج آخر. كما يمكن للمستخدمين توليد مفتاح خاص لعناوينهم على الحواسيب التي لن تتصل بالشبكة اما المتشككين فيستطيعون توليد عناوينهم ومفاتيحهم

(ISSN: 2356 - 9492)

الخاصة على حواسيب غير متصلة بالشبكة ثم تدميرها عقب ذلك، وستنجو العملات المخزنة في تلك المفاتيح الرقمية الخاصة من الهجمات على الشبكة.

كما أن ميول حَمَلَة العملات الرقمية مع تبنيهم لأفكار حركة Cypher punk تُعَدُّ من العوامل الحامية للعملات الرقمية من الهجمات، مما يعزز لديهم الميل الى التوثيق أكثر من الثقة. فمالكو العملات الرقمية مُتخصصون من الناحية التقنية، كما يتميزون بالدقة عند فحص الاجهزة الخاصة بهم وكذا التطبيقات التي يستخدمونها. كما أن ثقافة استعراض النظير مفتوح المصدر تعد وسيلة دفاعية هامة ضد هذة الهجمات. ولما كانت الشبكة ذات طبيعة موزعة، فيمكن أن تسبب هذه الهجمات تكاليف كبيرة للأفراد، كما قد تؤدي لتعطيل نظام الشبكة، الا انه سيكون من الصعب أن تسبب توقف الشبكة أو العزوف عن طلب العملات الرقمية لان الرغبة في الربح هي الدافع الاساسي لطلبها و هي ما تجعلها قيمه ولا يمكن للأجهزة المستخدمة القيام بذلك. فيمكن استبدال أي من المعدات بأخرى دون تأثر العملات الرقمية. برغم ذلك، فإنَّ استمرار وموثوقية العملات الرقمية ستتحسنان إذا تنوع مُصنِّعي الأجهزة المستخدمة فلا يتأثر النظام بأي منهم. (٥٨)

وتسهل هذه الطريقة للمجرم سرقة الأموال من خلال عكس العملات التجارية في البلوك تشين، وأحيانًا يشار لهذه الجريمة بهجوم ٥١%، حيث إذا أراد الجاني أن يقتحم البلوك تشين لعملة البت كوين، يجب عليه أن يسيطر على نسبة تفوق ٥١% من قوة تجزئة الشبكة الرقمية للعملة.

اي يقوم بدفع مبلغ كبير للحصول على تقنيات التعدين أو التعاون مع مجموعات تعدين، للحصول على قوة تجزئة تفوق المستخدمين الأخرين.

ومن المؤكد ان النجاح في هذا يسهل للمهاجم تعدين اجزاء من البلوك تشين دون اكتشافه من باقي المستخدمين، فيمكنه التعديل واختيار طريقة التبادل التجارية التي يتم

(58) Kang, Kee-Youn, Cryptocurrency and Double Spending History: Transactions with Zero Confirmation, 6 May 2019, pp:7-10, https://mpra.ub.uni-muenchen.de/96875/1/MPRA_paper_96875.pdf

إجراؤها في هذه الأجزاء من البلوك تشين، كما يستطيع الجاني صرف أمواله من البت كوين والحصول على عملة رقمية أخرى أو تبادل الأموال.(٥٩)

بعد أن يقوم الجاني بصرف البت كوين، يقوم الآن بعرض أجزاء البلوك تشين الخاصة به للمستخدمين، وعلى ذلك فان بروتوكول البت كوين يعتمد على أطول جزء من البلوك تشين على أنه الجزء الصحيح والآمن للتبادل، وحيث ان الجاني يمتلك قوة تجزئة أكثر من الاخرين، فسوف يضطر المستخدمين الشرعيين لقبولها على أنها السجل الصحيح من العمليات التجارية والتبادلية أو على أنها الجزء الأطول من البلوك تشين، ولكنها في الواقع تكون عملية خداع لجذب المتعاملين و اختراق العمله الرقمية.

وبالرغم من قدرة الجاني على اختيار العملية التبادلية أو التجارية الممكن إضافتها للبلوك تشين، الا انه يمكنه أن يضمن عمليات الدفع الحقيقية التي قام بها لعناوين أخرى، وهو ما يتيح له ايضا أن يصرف عملة بت كوين واحدة مرتين، والتي تعد وسيلة مكلفة ومعقدة بسبب النظام المغلق للبلوك تشين، كما انها غير ناجحة في البلوك تشين الضخمة والطويلة، لأن الجاني في هذه الحالة لن يستطيع الحفاظ على تفوقه الذي حققة في بناء أجزاء أطول من البلوك تشين الحقيقية لضخامتها.

وقد تفشل الطريقة السابقة مع عملات مثل بت كوين و ايثيريوم، إلا أن نسبة نجاحها ترتفع مع العملات الرقمية الضعيفة في قوة التجزئة، لذا قد يلجأ الجاني للهجوم على عملات أخرى تعاني من هذه المشكلة لكن قيمتها عالية، مثل ByteCoin وLiteCoin Cash و Bitcoin Gold، وتفلح هذه الطريقة عند الاعتماد على خدمات سحابية في عملية التعدين أو توظيف منصة خاصة تتميز بقوة التجزئة مثل NiceHash.

(59) Itay Eyal and Emin Gun Sirer, Majority is not Enough: Bitcoin Mining is Vulnerable, from book" Financial Cryptography and Data Security": 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers,pp:5-15

(ISSN: 2356 - 9492)

وقد لوحظ ان القائم بهجمة دفع مضاعف ٥١% على بت كوين لمدة ساعة كاملة يتكلف قرابة ٧٠٠ ألف دولار، بينما الهجمه على عملة رقمية أصغر مثل ByteCoin لا يكلفه الا ٥٣٩ دولار رغم ان قيمتها السوقيه ٦٠٠ مليون دولار.

المطلب الثاني

هجمات البنية التحتية وكسر خوارزمية الدمج SHA-256

الفرع الأول

هجمات البنية التحتية

من أكبر المشكلات التي تواجهها العملات الرقمية أن إيقاف وتعطيل البنية التحتية للاتصالات التي تعتمد عليها المنظومة يمكن ان يسبب وقف تلك العملات بتعطيل عمل الإنترنت. والمشكلة هنا هي عدم فهم العملات الرقمية على أنها شبكة بمعناها التقليدي حيث تضم أجهزة متخصصة وبُنى تحتية ذات نقاط ضعف حرجة يمكن مهاجمتها وتعطيلها. ومن ناحية اخرى فان العملات الرقمية عبارة عن بروتوكول برمجي؛ كونها عملية داخلية يمكن تشغيلها على أي حاسوب من الحواسيب الموزعة حول العالم. لذا، فالعملات الرقمية ليس لها نقطة فشل واحدة، ولا تعتمد على اجهزة أو بُنية تحتية لذا يمكن التخلي عنها. فيمكن لأي حاسوب يشغل برمجيات العملات الرقمية أن يتصل بالشبكة وأن يتم إجراء العمليات عليه.[٦٠]

(٦٠) سيف الدين عموص – معيار البت كوين "البديل اللامركزي للنظام المصرفي المركزي " – ترجمة احمد محمد حمدان – مؤسسة العبيكان للنشر- ط١ العربية ٢٠٢٢- ص٣٠٠ - https://books.google.ae/books?id=l1NlEAAAQBAJ&pg=PA300&lpg=PA300&dq=%D9%83%D8%B3%D8%B1+%D8%AE%D9%88%D8%A7%D8%B1%D8%B2%D9%85%D9%8A%D8%A9+%D8%A7%D9%84%D8%AF%D9%85%D8%AC+SHA-256&source=bl&ots=RzNAKTLrBz&sig=ACfU3U3pOzHPd9Q4EHYiT1rI2wFQ1fnk5g&hl=ar&sa=X&ved=2ahUKEwiI8oS4ncP6AhWvxYUKHXP6AEMQ6AF6BAgOEAM#v=onepage&q=%D9%83%D8%B3%D8%B1%20%D8%AE%D9%88%D8%A7%D8%B1%D8%B2%D9%85%D9%8A%D8%A9%20%D8%A7%D9%84%D8%AF%D9%85%D8%AC%20SHA-256&f=false

فالعملات الرقمية تشبه الإنترنت لأنها عبارة عن برتوكول يتيح للحواسيب الاتصال ببعضها؛ وليست البنية التحتية هي التي تصل هذه الحواسيب ببعضها. كما أن كمية البيانات المطلوبة لنقل المعلومات حول العملات الرقمية صغيرة جدا بالنسبة لكمية المعلومات المتدفقة في الإنترنت. فلا تحتاج العملات الرقمية لكم كبير من البنية التحتية التي يحتاجها الإنترنت، وذلك لأن البوك تشين الخاص بالعملات الرقمية تبث ١ ميجابايت من البيانات كل ١٠ دقائق ونظرا لوجود عدد غير نهائي من التقنيات المستخدمة لنقل البيانات، فالمستخدم يحتاج تقنية واحدة فقط للولوج إلى الشبكة. ولكي لا يتمكن المستخدم للعملات الرقمية من الاتصال مع الاخرين، يجب الاضرار بمعلومات العالم وبياناته والبنية التحتية للاتصالات وهذا غير متصور ، لذا فإن محاولة إيقاف أو تعطيل عمل البنية التحتية للإنترنت بشكل متزامن ستؤدي لضرر كبير ومع ذلك قد يفشل في إيقاف تدفق العملات الرقمية. حيث يمكن للأجهزة المتفرقة أن تتصل ببعضها باستخدام برتوكولات اتصال مشفرة فهناك العديد من الحواسيب والاتصالات الموزعة، فلا يمكن إيقافها بشكل متزامن، لذا فان هذا التهديد للعملات الرقمية هو اقلها احتمالا للحدوث وأقلها مصداقية ومعنى. كما ان التزايد في تكلفة العُقَد والتناقص في عددها بدلاً من تصور حالات تنطوي على المساس بالبنية التحتية للاتصالات لاستئصال برنامج ما، وذلك لان هناك تهديدات حقيقية للعملات الرقمية تأتي من مبادئ وأساسيات في تصميمها. فخواص العملات الرقمية كنقد لا يمكن التلاعب بها وكعملة رقمية لا يمكن إيقافها أو الاستيلاء عليها دون تدخل طرف ثالث، تعتمد على أن يكون تغيير القواعد المتفق عليها للشبكة أمرا صعبا خاصة في العرض النقدي.

وما يحقق الاستقرار الذي تحافظ عليه العملات الرقمية هو أنه من الخطورة بمكان ان يقوم احد بالعمل خارج الاطار الحالي والا يتبنَّى باقي الأفراد القواعد الخاصة بها. لكن السبب الذي يجعل تلك الخطوة خطيرة يتمثل في أن عدد العُقَد التي تشغل البرنامج كبير جدا ما يجعل عملية التنسيق بينها غير وارد، فاذا ارتفعت تكلفة إدارة العقد في العملات الرقمية، فستصبح إدارة العقد أصعب بالنسبة للأعضاء، مما سيُقلل عدد العُقَد في الشبكة، ومن ثم لن تكون العملات الرقمية شبكة غير مركزية فعالة فسيصبح من

(ISSN: 2356 - 9492)

السهل على العُقَد التي تدير الشبكة أن تتفق لتعيد صياغة القواعد في الشبكة بما يخدم مصالحها وهو ما سيؤدي لتخريبها.

وهذا الخطر هو الأخطر من الناحية التقنية لأنه يشكل تهديد للعملات الرقمية على المديين المتوسط والبعيد. ومن المؤكد ان الشيء الوحيد الذي يمكن ان يحد من قدرة الأفراد على إدارة عقدهم الخاصة هو حجم اتصالهم بالإنترنت. فإن بقي حجم الكتل أقل من ١ ميغابايت، فسيكون ضمن قدرة المستخدمين، اما اذا انقسمت الشبكة كليا لزيادة حجم الكتلة،[٦١] فسيترتب زيادة تكلفة إدارة هذه العُقَد مما سيُقلل عددها على الشبكة. وهذا التهديد ممكن تقنيا لكنه بعيد الاحتمال لأن الدافع الاقتصادي للنظام سيمنع ذلك، وهو ما يتبين من رفض محاولات زيادة الكتلة للآن.

وتلعب منصات التداول والتبادل دورًا مهمًا في بيئة تداول العملات الرقمية. أنها تسمح للتبادل بين النقود الورقية والعملات الرقمية، وبالتالي تسهيل نمو الشبكة. وبالرغم من ذلك فإن نموذج التشغيل الخاص بها عرضة للمخاطر المختلفة، حيث تعتبر السرقات أحد أبرز الأمثلة. غالبًا ما تُعتبر منصات التبادل، نظرًا لحقيقة أنها تحتوي على كميات كبيرة من العملات الرقمية نيابة عن عملائها، بمثابة اداة جذب للمنظمات الاجرامية والارهابية لارتكاب السرقة. تجعل مثل هذه الهياكل الهجوم أمرًا سهلاً بشكل خاص نظرًا لأن المتسلل يمكنه كسر أو تجاوز آلية الأمان الخاصة بالتبادل من أجل الوصول إلى الملايين من حسابات العملات الرقمية المخزنة هناك. وصفت فكرة خاطئة شائعة مثل هذه الهجمات بأنها أصبحت ممكنة بسبب نقاط الضعف البلوك تشين فمن المهم تصحيح هذه المغالطات لأنها لا تتعلق بضعف بلوك تشين ويتم الاحتفاظ بمحفظة التبادل خارج السلسلة وفي حالة السرقة، لا يحدث أي تفاعل مع سلسلة الكتل. غالبًا ما يكون سبب حدوث مثل هذه الهجمات هو عدم وجود آلية أمنية قوية، أو وجود نظام ساذج للغاية، مما يجعل من السهل جدًا معالجة إنشاء البورصة وبالتالي سرقة العملات الرقمية المجمعة.

(61) Maria Apostolaki& others ,Hijacking Bitcoin: Routing Attacks on Cryptocurrencies, https://btc hijack.ethz.ch,pp:2-9

وفقًا للإحصاءات التي نشرتها Cipher Trace، فقد سُرقت خلال عام ٢٠١٦-٢٠١٨ ما يقرب من ١,٣ مليار دولار من العملات الرقمية. ومع ذلك، فإن هذه الممارسة موجودة في سوق العملات الرقمية منذ نشأة منصات التبادل حيث كان أحد أكثر الأحداث إثارة هو إفلاس بورصة Mt.Gox التي تتخذ من طوكيو مقراً لها ، حيث فقد حوالي ٧٥٠,٠٠٠ عميل من عملات البت كوين. يمكن تسمية Youbit ، وهي بورصة مقرها كوريا الجنوبية ، كمثال آخر ، حيث تقدمت هذه المنصة بطلب للإفلاس بعد خسارتها حوالي ١٧٪ من مقتنياتها. كانت هناك أيضًا بعض البورصات التي تمكنت من النجاة من الهجمات، بما في ذلك منصة الصرافة Coincheck التي تتخذ من اليابان مقراً لها والتي فقدت في يناير ٢٠١٨ حوالي XM (NEM) بقيمة ٥٣٠ مليون دولار ومع ذلك، فإن الإجراء غير المشروع أضر كثيرا بسمعتها.

إن مقاومة العملات الرقمية للهجمات متجذرة بثلاث خواص: عدم تعقد الأساسيات التي يتكون منها، وطاقة معالجتة التي تضمن أمن التصميمات البسيطه، والعُقَد الموزعة التي تتطلب الوصول لاتفاق على التغيير لاتمامه، ولكي يتم توضيح درجة تحصين العملات الرقمية.(٦٢)

وقد أصبحت مناقلات العملات الرقمية نفسها ضحيةً لهجمات المخترقين أيضًا، فالهجمات التي تستهدف تبادلات العملات الرقمية والمعاملات ليست جديدة وكان آخرها هجوم Coincheck، حيث تم سرقة عملات رقمية بقيمة تصل قيمتها لمليارات الدولارات من خلال اختراق لتبادل العملات الرقمية.

وقد أدّت هذه الهجمات إلى إفلاس العديد من منصّات التداول مثل BitGrail وغيرها من المنصّات، في حين استطاعت منصّات أخرى الدفاع عن أموالها ببسالة أمام المخترقين، وبسبب هذا النوع من الاختراقات ما تزال الكثير من الحكومات رافضة للتعامل بالعملات الرقمية.

(62) (62) Itay Eyal and Emin Gun Sirer, Majority is not Enough: Bitcoin Mining is Vulnerable, from book" Financial Cryptography and Data Security": 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers,pp:5-15

(ISSN: 2356 - 9492)

كيفيه اختراق العملات الرقمية

يكون الترويج لعملات البت كوين أو ايثيريوم أنها آمنة وغير قابلة للاختراق بفضل الآلية المغلقة التي تعمل بها، الا ان التجربة أثبتت إمكانية اختراق العملات الرقمية ومن ضمنها هذه العملات.

وعلى ما يبدو من السهل اختراق العملات الرقمية الضعيفة أو الصغيرة أكثر نظرًا لقلة الكثافة في تبادلها، وبالمقابل العملات التي تمتلك مساحات كبيرة من تكنولوجيا سلاسل الكتل الرقمية Blockchain، فهذه السلاسل تعتمد على فكرة التبادل المباشرة بين المستخدم والمستخدم الآخر دون وجود وسيط، وبالتالي قوة وكثافة هذه السلاسل تؤثر على احتمال حدوث الاختراق ومدى نسبة الضرر الذي قد يحصل.

وبشكل عام هنالك طريقة رئيسية تتيح سرقة الأموال عبر الالتفاف على نظام سلاسل الكتل الرقمية.

تحصين الحواسيب المستخدمة في التعدين

العملات الرقمية هي سجل ملكية فيوجد فقط ٢١ مليون منها، وعدة ملايين عنوان تابع لها، وكل ويتم يوميا نقل عملات لا تزيد عن ٥٠٠ ألف تحويلة. وتتطلب ادارة هذا النظام قوة حوسبة ضئيلة فيمكن للاب توب إدارتها حال تصفح مستخدمة للإنترنت، ولا يتم تشغيل العملات الرقمية على حاسوب واحد لتطلب ذلك الثقة في مالكه، والتيقن من امكانية اختراقه.

فالشبكات الحاسوبية تعتمد في حمايتها على تحصين الحواسيب ضد الهجمات واستعمالها كمرجع نهائي، أما العملات الرقمية فلا تحمي جميع الحواسيب بشكل فردي، بل تفترض أن حواسيب جميع العُقَد هجومية. فتقوم العملات الرقمية بالتحقق من حركات الأعضاء، وعملية التحقق هذه تستهلك كمية كبيرة من طاقة المعالجة. وقد ثبتت فعالية هذا النظام لأنه جعل حماية العملات الرقمية تعتمد على كم طاقة المعالجة، وبذلك فاصبحت منيعه ضد الدخول غير المشروع وتطلبت تأكيد الهوية. لذا يجب على كافة القائمين باجراء التحويلات للسجل العام ان يخضعوا لتلك الضوابط ويتحمل تلك التكلفة، وكل من يضبط وهو يحاول الخداع والتزوير سيخسر المبالغ التي دفعها. وعلى

ذلك ستؤدي الحوافز الاقتصادية لرفع تكلفة الخداع في العملات الرقمية بالاضافة لصعوبة نجاحه، حيث يجب على من يرغب في اختراق العملات الرقمية ان يقوم بإفساد سجل التحويلات لنقل العملات لحساب معين بشكل كاذب أو لجعل الحساب غير قابل للاستخدام، وهو ما سيتطلب من عقدة ما أن تُدخل كتلة غير صالحة إلى للبلوك تشين ويتطلب من الشبكة أن تتبناها وتستمر بالبناء على أساسها. ومع ذلك يصعب تحقيق المخترقون لغايتهم مع تزايد تكلفة إضافة الكتل لأن تكلفة الكشف عن الاحتيال صغيرة جدا بالنسبة للعقد، في حين تتزايد تكلفة إضافة كتلة من التحويلات باستمرار، بالاضافة الى ان معظم العُقَد في الشبكة تهتم باستمرار العملات الرقمية وبقائها، كما ان هناك عدم تماثل تصميم العملات الرقمية بين تكلفة إضافة كتلة جديدة من التحويلات وتكلفة التأكد من صلاحية تلك التحويلات، مما يؤكد أنه بالرغم من أن تزوير السجل ممكن تقنيا إلا أن الحوافز الاقتصادية تمنعه . لذا يعد سجل التحويلات سجلاً موثوقا للتحويلات المؤكدة.[٦٣]

الفرع الثاني

كسر خوارزمية الدمج SHA-256 [٦٤]

تُعتبر خوارزمية الدمج SHA-256 من المكونات الاساسية لنظام العملات الرقمية ويمكن تعريفها بأنها عملية تقوم باخذ سلاسل البيانات كمُدخل وتقوم بتحويلها لقاعدة بيانات ذات حجم ثابت(الهاش) بواسطة معادلة رياضية غير قابلة للعكس. أي يسهل استعمال هذه المعادلة لدمج البيانات، مع عدم امكانية تحديد أصل سلاسل البيانات بواسطة الدمج .ولكن يمكن ذلك من خلال إجراء تحديثات على طاقة المعالجة، فيتمكن الحاسوب من عكس حساب عمليات الدمج فتصبح عناوين العملات الرقمية معرضةً

(63))Madeleine gart ,Ida linderbrandt,Are Cryptocurrencies the Future of Money?, kth royal institute of technology school of computer science and communication, pp:18-20

(٦٤) دالة هاش SHA-256 هي دالة تشفيريه، تقبل بيانات ادخلت لها حجم غير متغير تُنتج مخرجات حجمها ثابت .وهي "أحادية الاتجاه". فيمكن لأي شخص استخدامها لإنتاج مخرجات عند توافر المدخلات، ولكن لا يمكن استخدام مخرجاتها لإعادة بناء المدخلات المُعطاة. هذه الخاصية القوية تجعل دالة الهاش SHA-256 مثالية لتطبيقات شبكة العملات الرقمية

(ISSN: 2356 - 9492)

لسرقتها. ويصعب تحديد وقت حدوث ذلك وإذا حدث ذلك، فسيكون تهديدا تقنيا خطيرا للعملات الرقمية .ولمواجهته يجب استخدام تشفير أقوى، وهنا تثور صعوبة تنسيق الانقسام الكلي للشبكة، وكيفية إقناع عقد الشبكة على ترك القوانين المشتركة القديمة واعتماد قواعد جديدة في عملية دمج جديدة. وهنا وحيث أن التهديد حقيقي، فإن مالكي العملات الرقمية قد يفضلون الاستمرار كجزء من التطبيقات القديمة وعندئذ يكونون معرضون للاختراق، لذا يمكن أن يشارك المستخدمين في الانقسام الكلي وهنا يثور التساؤل حول ما إذا كان الانقسام الكلي سيكون مُنظَّما وسيشهد انتقال كافة المستخدمين للسلسلة نفسها، أم سيؤدي لانقسام السلسلة لفروع تستخدم تشفيرات متعددة .وبالرغم من امكانية كسر اختراق تشفير ال SHA–256 ، إلا أن دافع المستخدمين الاقتصادي حينها سيكون هو الانتقال إلى خوارزمية أقوى بل الانتقال إلى خوارزمية واحدة تضم الجميع.(٦٥)

"دالة التجزئة" عبارة عن خوارزمية تقوم بتحويل الملفات أو النصوص لمجموعة من الأحرف ذات طولٍ ثابت لا يمكن تكرارها، تسمّى "خلاصة الرسالة وتتميّز العمليّة الحسابية بكونها باتجاه واحد، أي أنّه من الصعب جدًّا إن كنتم تملكون "خلاصة الرسالة" أن تستطيع هذه العملية كشف الرسالة الأصليّة أي "البيانات المدخلة". كما يظهر في الصورة التالية، مهما كان حجم "البيانات المدخلة" (١) يبقى حجم "خلاصة الرسالة" هو نفسه لكلّ "البيانات المدخلة" في "دالة التجزئة" هذه. الاختلاف في "خلاصة الرسالة" كبير حتّى لو كان الاختلاف في "البيانات المدخلة" صغيراً

المبحث الثالث

مستقبل العملات الرقمية في دولة الامارات بين الواقع والمأمول

تمهيد وتقسيم:

المطلب الأول: المبادرة الإماراتية السعودية في العملات الرقمية

المطلب الثاني: نحو استراتيجية امنية في مجال المعاملات الرقمية

(٦٥) سيف الدِّين عَمُّوص - ترجمة: أحمد محمد حمدان - معيار البيتكوين "البديل اللامركزي للنظام المصرفي المركزي"- جون وايلي وأبناؤه، ريفر ستريت، هوبوكن، نيوجرسي – ٢٠١٩م- ص٢٨٠ص٣٠٥ متاح على الموقع الالكتروني: http://www.copyright.com .

المطلب الأول

المبادرة الإماراتية السعودية في العملات الرقمية

أعلنت اللجنة التنفيذية لمجلس التنسيق السعودي الإماراتي، عن إطلاق سبعة مبادرات اساسية بينهما، اهمها العملة الرقمية المشتركة، وتجسد هذه المبادرات التكامل بين الدولتين في الخدمات واسواق المال، والطيران، والأعمال، وأمن الإمدادات.

وتم عقد اللقاء الأول في أبو ظبي للإعلان عن الإنجازات في هذا السياق، والتي تم اطلاقها في إطار خطة "العزم"، وذلك في إطار تنفيذ الاستراتيجية المشتركة للتكامل الاقتصادي بين البلدين وتعزيز النمو والاستدامة في كافة المجالات.

وضمت اللجنة ستة عشر عضوا، من بينهم سبعة وزراء من الإمارات، برئاسة وزير شؤون مجلس الوزراء، ومن السعودية وزير الاقتصاد والتخطيط.

وتم خلال اجتماع اللجنة إطلاق المبادرات التي تضمنت عدة محاور حيوية، وتمت الموافقة على برنامج التكامل في أمن الإمدادات بين الدولتين، على ان تتم متابعة الإنجازات ومناقشة القضايا ذات الاهتمام المشترك من خلال لجنه مشتركة.

وتضمنت المبادرات التي تم إطلاقها خلال الاجتماع، مشروع العملة الرقمية الإلكترونية التجريبية، والذي يعتمد على تجربة البلوك تشين في إنشاء عملة مشفرة تستخدم في المعاملات بين البلدين في اعمال البنوك المشاركة في المشروع ، اعتمادا على استخدام قواعد بيانات موزعة بين البنوك المركزية في البلدين، والبنوك المشاركة.(٦٦)

كما تم إطلاق مبادرة لتسهيل الحركة في المنافذ الجمركية من خلال اعتماد "مسار سريع" والتنسيق المشترك لإنفاذ مشروع المشغل الاقتصادي المعتمد، وتدعم المبادرة الشراكة بين الجمارك والمنشآت الاقتصادية، وتعزيز تأمين سلسلة الإمدادات الدولية، وتوفر العديد من المزايا لتسهيل التبادل التجاري بين البلدين.

---

(٦٦) عملة الرقمية المشتركة والسجلات الموزعة للبنك المركزي السعودي ومصرف الإمارات العربية المتحدة المركزي"مشروع عابر – التقرير النهائي – ٢٠٢٢- ص٢٠ص٢٥ - https://www.sama.gov.sa/ar-sa/News/Documents/Project_Aber_report-AR.pdf

(ISSN: 2356 - 9492)

ويبلغ عدد الشركات المدرجة في برنامج المشغل الاقتصادي واحد واربعين شركة سعودية واربعون شركة من الامارات.

وفي ذات الإطار تم تدشين الية تتيح للشركات السعودية والإماراتية المسجلة في الدولتين الاستفادة من المشتريات الحكومية.

وتسمح تلك المبادرات، بالعديد من المجالات للمنشات المتوسطة والصغيرة من كلا البلدين بالمنافسة على مشتريات الحكومة الاتحادية باستخدام مواقع المشتروات الحكومية لبرنامج المشاريع المتوسطة والصغيرة طبقا للإجراءات في الإمارات والمملكة.

وشملت المبادرات مبادرة برنامج الوعي المالي للصغار، وتهدف لرفع الوعي المالي وتعزيز فهم الادخار والإنفاق الذكي لدى الذكور والإناث من الشباب من خلال ممارسة الاعمال التجاريه واتاحه المهارات المتقدمة لهم، ومحاكاة الأعمال لتطوير ونشر مفاهيم العمل الحر.

كما تم اطلاق مبادرة سوق الطيران المدني، لتحقيق التعاون والتكامل في مجالات الطيران المدني كالملاحة الجوية، والسلامة والأمن، والتحقيق في الحوادث الجوية.

وتمتلك السعودية والإمارات صناديق كبيرة، تعد الثانيه عالمياً، فيما تشغلان الموقع الثامن في الصادرات من السلع والخدمات.

وتم اطلاق مجلس التنسيق السعودي الإماراتي في اطار اتفاقية بين البلدين في ٢٠١٦، لتحقيق رؤية مشتركة تتمثل في اظهار مكانة الدولتين في مجالات الاقتصاد والتنمية البشرية والتكامل السياسي والأمني العسكري، وتحقيق الرفاهية لمجتمع البلدين.

تواصل المملكة والإمارات تعاونهما لإنشاء عملة رقمية موحدة، يتم استخدامها في عمليات الدفع التجاري بين البلدين، من خلال تقنيات البلوك تشين والسجلات الموزعة.[٦٧]

وأعلنت مؤسسة النقد العربي السعودي "ساما" والبنك المركزي الإماراتي "UAECB" عن تبنيهما خططًا لإطلاق مشروع العملة الرقمية المشتركة "عابر"، بهدف السماح

(67) https://uaecabinet.ae/ar/details/news/saudi-emirati-powerhouse-announces-7-joint-initiatives-in-vital-sectors

بشيوع المعاملات المالية عبر أحدث وسائل التكنولوجيا التي تعمل بالطاقة الكهربائية بين المؤسستين الماليتين.

ويعتبر المشروع نتاجًا للعديد من المحادثات حول تطبيق تقنية البلوك تشين في المملكة والإمارات. ففي أكتوبر ٢٠١٨، أعلن المسؤولون عن خطط لإنشاء لوائح تسمح بالعروض الأولية للعملة في البلاد؛ لتحريك الرؤية لعملة رقمية رسمية خطوة إلى الأمام.(٦٨)

وتعمل العملات الرقمية عن طريق شبكات البلوك تشين الخاصة بها؛ حيث يتم إنشاء جميع العملات الرقمية وتخزينها وتبادلها على شبكات «البلوك تشين» المنفصلة الخاصة بها.

وشبكة البلوك تشين الخاصة بالعملة الرقمية هي دفتر الأستاذ العام لجميع معاملات تلك العملة التي حدثت من أي وقت مضى. بحيث يتم تجميع المعاملات الجديدة على هيئة «كتل»، ويتم تأكيد كل كتلة والتحقق من صحتها بواسطة المستخدمين في الشبكة، قبل إضافتها في نهاية السلسلة، علمًا بأن كل مستخدم يمتلك نسخته الخاصة من دفتر الأستاذ، ويتم تحديثه باستمرار.

وهذه الشبكات لا مركزية، بخلاف النقود التقليدية والأوراق البنكية والعملة المعدنية، والسمة المميزة التي تعطي قيمة العملة المشفرة ميزة على الخيارات الاقتصادية الأخرى هي أنها غير تمييزية ومتاحة بسهولة.

وعندما يتم استخراج العملات الرقمية على البلوك تشين أو نقلها بين المستخدمين، يجب أن يتم تخزينها حتى يكون المالك الجديد مستعدًا لاستخدامها، وهنا تظهر محافظ العملات الرقمية وهي قطعة من البرمجيات قادرة على إسكان العملات الرقمية بشكل آمن لفترة غير محددة من الزمن، وتحتوي جميع محافظ العملات الرقمية على مفتاح عام ومفتاح خاص واحد على الأقل.

(٦٨) عملة الرقمية المشتركة والسجلات الموزعة للبنك المركزي السعودي ومصرف الإمارات العربية المتحدة المركزي"مشروع عابر – التقرير النهائي – ٢٠٢٢- ص٤١ - https://www.sama.gov.sa/ar-sa/News/Documents/Project_Aber_report-AR.pdf

(ISSN: 2356 - 9492)

ومن المُقرر أن تركز المرحلة الأولى من تجربة العملة الرقمية المشتركة على الجوانب الفنية لإصدار عملة رقمية مشتركة؛ ففي البداية سيقتصر استخدام عابر على عدد صغير من البنوك في كل دولة. ويتمثل الهدف الرئيس من هذه التجربة في تقليل تكاليف التحويلات واختبار قدرة هذه العملة على العمل بمثابة «نظام احتياطي إضافي للمدفوعات المركزية المحلية».

ويُعد مشروع العملة المشترك السعودي الإماراتي أحد المبادرات السبعة التي أعلنتها اللجنة التنفيذية لمجلس التنسيق السعودي الإماراتي، والتي اجتمعت في ١٩ يناير الجاري في أبو ظبي، بهدف مواصلة العمل على المبادرات المشتركة.

وخلال المرحلة التجريبية، سيتم استهداف المشروع المشترك في البنوك بقصد فهم أفضل لتداعيات تكنولوجيا البلوك تشين وتسهيل المدفوعات عبر الحدود، على أن يتم استخدام قاعدة بيانات موزعة بين البنوك المركزية ومقدمي الخدمات المالية الأصغر من كل من المملكة والإمارات.

كذلك يهدف البرنامج التجريبي إلى تقييم تأثير هذه العملة على السياسات المالية الحالية، وكذلك معالجة قضايا مثل أمن العميل والمخاطر واللوائح.

وتتطلع الإمارات إلى الانضمام إلى قائمة الوجهات الرائدة لشركات البلوك تشين في عام ٢٠١٩ من خلال إنشاء إطار قانوني جديد مؤيد للتشفير.

وفي المملكة، أبرمت السلطات الجمركية مؤخراً مخططاً تجريبياً يربط بين برنامجها التجاري «FASAH» عبر الحدود مع البنية التحتية لـ«Trade Lens» التابعة لشركة IBM وشركة مايرسك[٦٩]

(٦٩) بيان إطلاق مشروع "عابر" للعملات الرقمية المشتركة بين مؤسسة النقد العربي السعودي ومصرف الإمارات العربية المتحدة المركزي

المطلب الثاني
نحو استراتيجية امنية في مجال العملات الرقمية
الفرع الأول
التحديات التقنية للتعاملات بالعملات الرقمية

يمكن أن تستفيد أجهزة انفاذ القانون من هذه التحديّات لعرقلة نشر منظمات إجرامية او ارهابية لعملة الرقمية وثمة العديد من الصلات التي تربط التحديّات التكنولوجية بالقدرة على طرح عملة رقمية للتداول الرقمية بشكل واسع واستخدامها بشكل مناسب في المعاملات المادية، بينما ترتبط ببعضها في مدى الموثوقية في تداولها لتكون متداولة في الاستخدام. وذلك يتطلب قيام الجهات التي تتداول العملات الرقمية لضمان مرونة تلك العملات في مواجهة المخاطر التقنية التي يضعها الخصوم، بما فيها الأخطار الأكثر تطورا التي تضعها الدول. ونقوم في هذا السياق بتناول المعوقات التي تواجه تداول العملات الرقمية. الا ان ثمة تحديّات مرتبطة بالمجهولية، تنطبق أيضاً على استثمار العملة الرقمية ومنها التقنية والتي يمكن ان نوجزها في:

١- تحقيق الإلمام التكنولوجي اللازم لتطوير العملة الرقمية وتداولها وضمانها كعملة رقمية ، يتضمن الفهم التقني للمهارات في مجالات الشبكات والحواسيب ونظم التشفير.(٧٠)

٢- التيقن أن مستخدمي العملات الرقمية يمكنهم الوصول لعملاتهم بما يستلزم المستوى الأدنى الكافي من الإلمام التقنيّ للسماح باستعمالها السوقي وتأمين مستويات كافية من التشفير للعمليّات التي يرغب المستخدمين القيام بها، وتأمين سلامة تلك العمليات ليثق الأطراف للموثوقية من تناسب التبادل، دون تطلب خبرة تكنولوجية كبيرة

٣- حماية سلامة العملة الرقمية (وتوفرها) ضد الأخطار الإلكترونيّة المتقدّمة ولاسيما الدول التي تعارض نشر منظمات ارهابية للعملة الرقمية.

(٧٠) جوشوا بارون واخرين – تداعيات العملة الافتراضية على الامن القومي "البحث في إمكانية النشر من جهة فاعلة غير حكومية"- مؤسسة راند – كاليفورنيا- الولايات المتحدة الامريكية – ٢٠١٥م – ص٣٤ص٤٠ - www.rand.org/t/rr1231

(ISSN: 2356 - 9492)

كما أنّ التحديّات لا تقتصر على العملات الرقمية اللامركزيّة وبالفعل، ليس واضحاً ما إذا كانت المنظمات الاجرامية والارهابية ستفضّل غياب التحكم المركزي في العملات عن طريق البنوك المركزية .ومن ثم يتم تشكيل الية هيكلة البنية التحتيّة، وهي الشبكة الحاسوبية التي تقوم بتنفيذ الخوارزميّات القائمة بذات الوظائف العامة التي تؤديها البنوك المركزية والتي تعتبر إحدى عناصر القرار الأساسيّة لإنشاء عملة رقمية.

٤-تطوير عملة رقمية ونشرها

تعد الخبرة والقدرة الضروريّتان لتطوير العملة ووسائل التعامل بها وتداولها أحد الصعوبات التكنولوجية التي تواجه المنظمات الإجرامية والارهابية في نشرها للعملة الرقمية .في المبدأ، يكون الإلمام التقني اللازم لتطوير العملة الرقمية ونشرها عالي المستوى نسبياً، الا انه في التطبيق الفعلي توجد ثمة تقنيات للاعتماد العام بهدف دعم التداول ويكمن الغرض الرئيسي في تحديد تلك الصعوبات الاساسية والتي إذا تم التغلب عليها، ستؤثّر بشكل كبير على قدرة الجماعات الارهابية على طرح عملات رقمية للتداول.

إنّ العناصر الاساسية التي تتطلب التطوير هي:

أولاً: العملة ذاتها ويتضمن ذلك بدائل التصميم الهامة والعديدة

ثانياً: وسائل الحصول على تلك العملات وحفظها وتحويلها كجزء من العمليّات الماليّة بما فيها وسائل دعم هذه التحويلات كالهواتف الذكيّة

ثالثاً: الخدمات المالية الكافية للدفع الاجل ونظم السداد المباشر لدعم كافة الخدمات بأمان ومرونه

٥-تطوير برمجيّات لعملة رقمية

ترجع تلك الصعوبات للدرجة التي ترغب فيها المنظمات الإجرامية او الارهابية الابتعاد عن عملات رقمية مستعملة وعن برمجيّاتها ذات الصلة ويمكن للمنظمات الإجرامية او الارهابية أن تعتبر بكل بساطة أي عملة رقمية عملتها، لكن ذلك يثير السؤال عن الاستفادة من اعتماد بسيط مماثل. كما يمكن لتلك الجماعات أن تقرر انتاج عملة جديدة، ويستلزم ذلك ايجاد مطورين برمجيّات محترفين في هذا المجال. ويمكن

ذلك أيضا بخلق عملة جديدة باستخدام ذات البرمجيّات التي تستخدمها العملة الرقمية سابقة الاستخدام.(٧١)

وسيقوم هؤلاء المطورين بتصميم برامج لتنظيم العملة، بالإضافة الى استخدام تطبيقات برمجيه تمكّن المستخدمين من حفظ العملة الرقمية والتعامل بها. ويجب ان يكون هذا التحديث ملائما لتشجيع اعتماد العملة الرقمية واستعمالها بشكل كبير، ونظرا للأمن الأساسي والمتأصل اللازم لتطبيقات مشابهة، ينبغي أن يكون تقدير درجة فهم المطور على مستوى إنشاء برمجيّات تشفير مخصصة تستعمل بشكل كبير. والأمثلة في هذا الشأن قليلة ومنها أنّه إذا تمكنت احدى المنظمات الارهابية بدعم احدى الدول بما يجعلها قادرة على الوصول لخبرائها ومطوريها الإلكترونييّن، يمكن تنفيذ تطوير مشابة بطريقة اوسع. وهنا تتوافر أمثلة عن قدرات إلكترونيّة متطورة تواجه صعوبات في إنشاء خدمات رقميه منتشرة بشكل كبير، حتى في الأمكنة الأكثر تساهلاً كتطوير الولايات المتحدة عمليّات التبادل على الإنترنت لدعم قانون الرعاية الصحيّة. وقد تعتمد المنظمات الاجرامية والارهابية على "منظّمات القراصنة على شبكات الإنترنت" أو منظّمات الجرائم الإلكترونيّة التي تتحالف معا. كما أنّ بعض المنظمات الارهابية، تبدو على الأقل ذات قدرة محدودة على تقديم خدمات رقمية آمنة كالتشفير أما الوسيلة الافضل لتطوير عملة رقمية جديدة فيتضمن تعديل عملة رقمية مستخدمة من قبل اي الحفاظ على التكنولوجيا الأساسيّة للعملة وتحديثها بمسمى جديد. وهذا الإعداد يختلف عن استخدام العملات الرقمية. فقد تكون برمجية معينة لعملة رقمية معينه لكنها تستخدم كخدمة إلكترونية اخرى فعند تعديل العملة الرقمية، قد تستخدم التنظيمات الارهابية العملات الرقمية واحيانا يتطلب انشاء عملة رقمية جديدة امكانيات رقمية بسيطة عند

(٧١) كاثرين ستيوارت – العملة الرقمية"اجراء المعاملات وتبادل القيمة في العصر الرقمي " - لمحةٌ حول الندوة الاستشارية المعنية بالعملة الرقمية التي عقدت كجزء من برنامج معهد كوشام للقيادة الفكرية لعام ٢٠١٧م – مؤسسة راند للنشر – ص٧ص٩ - https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF371/RAND_CF371z1.arabic.pdf

(ISSN: 2356 - 9492)

توافر خدمات على الإنترنت تروّج لإنتاج عملة رقمية.[٧٢] وقد يترتب على استعمال برمجيّات قديمة وجود نقاط ضعف رقمية تتضمنها تلك البرمجيّات.

٦-تداول عملة رقمية بطريقة ماديّه:

يعد التداول الماديّ للعملات الرقمية تحديّاً كبيرا. ويعني تحديد الوسيلة التي يتعامل بها الشخص العادي مع مقدم السلعة او الخدمة في العالم الحقيقي. وإذا كان الحاسوب يقوم بعمليّات تحويل العملة الرقمية، فان مستخدمو العملة الرقمية سيحتاجون لإتاحة التداول اليومي للأموال لعدد أكبر من الأجهزة المحمولة التي تقوم بالتحويل. وتشكّل تركيبة هذه التحويلات عائقاً أمام التداول لأنّ المستخدم ليس لدية وسائل تساعدة على التحويل.

حيث انّ حل هذه المشكلة يتمثل في استعمال الهواتف المحمولة، لتمتعها بقدرات للحوسبة والتواصل. فمثلا لدى العملات الرقمية تطبيقات كثيرة على الهواتف الذكيّة يمكن استخدامها لإتمام عمليّات التحويل.

ويستخدم التجار في بعض البلدان هواتفهم الذكيّة أو اللوحية الهواتف الذكيّة لإتمام تحويل العملات الرقمية للبطاقة الائتمانية من خلال تطبيقات كسكوير ويشكّل الاعتماد على نظام عملات قائم على الهواتف الذكيّة تحديّاً وذلك لان المشكلة هي أنّ إنشاء عملة تستخدم على الهواتف الذكيّه يحتاج الى هاتف ذكيّ لكل من يقوم بالتحويل ، أما المشكلة الأخرى فهي أنّه إذا كان تصميم العملة يقوم على الهواتف الذكيّة دون غيرها، فان المستخدم يكون معرضا لسرقة عملاته إذا تمت سرقة الهاتف . وفي حالة العملات الرقمية تسمح سرقة كلمة السرّ التي تيسر وصولة للمحفظة الإلكترونيّة أو التطبيق بسرقة العملات المتصلة بكلمة السرّ. اما العملات الماديّة، فتقتصر السرقة على المال المتداول ماديا أو حدّ السحب من الصراف الآليّ أو إلغاء الشيك الشخصي قبل استعماله. لذا ستستفيد كثيرا أيّ عملة رقمية يصل إليها عدد قليل من الأجهزة من وسائل

(٧٢) سيف الدّين عَمُّوص - ترجمة: أحمد محمد حمدان - معيار البيتكوين "البديل اللامركزي للنظام المصرفي المركزي"- مرجع سابق - ص٢٩٠ص٣٠٠.

الأمن المتطورة، كالتوثق من البصمة البيو مترية أو أيّ تصديق آخر متعدد العوامل تستخدمه آبل باي كتطلّب اتصال بين هاتف وجهاز اخر كأساس للعملات الرقمية فيتيح ثقة اكبر وامكانيات إلغاء اعتماد اكثر .

لا يكون استخدام الهاتف الذكيّ هو السبيل الوحيد للتحويلات الرقميّة. بل يمكن ذلك عن طريق هواتف مماثلة من خلال استعمال الرسائل النصيّة وتطبيقا لذلك نجد نظام تحويل العملة الأفريقي المعياريM-PESA ، لكنّ هذه الأنظمة تستخدم بشكل أساسيّ سيرفر آمن لتأمين التعامل على المحفظة الرقمية. ولما كانت الثقة في مقدم الخدمة لابد ان تكون متوفرة بشكل أساسي فان انشاء عملة رقمية جديدة بذات الاعدادات يرتبط بالثقة فقط وانها ستكون كافية في هذا الشأن. كما انه يمكن تحميل تطبيق للهواتف العادية الا انه يتعذر الى حد كبير تحميل محافظ الكترونية على الهواتف غير الذكية، لأن تلك الهواتف ليست مجهّزة لعمليّات تحميل تلك المحافظ وتشكّل تطبيقات المحفظة تحدي أمني للهواتف الذكيّة نظرا لخصائصها؛ وتوجد العديد من الوسائل لأداء مهام تحويل العملة الرقمية تتعدى الهواتف أو البطاقات. لكنّها تتطلّب أجهزة إضافيّة، مثل اليو. أس. بي ، مما يتطلّب توزيعاً واسعا لهذه الأجهزة من العصابات الاجرامية، مما يشكّل زيادة صعوبة تداول العملة الرقمية عامة ، و قد تكون هذه الأجهزة عرضة للهجمات الالكترونية [٧٣]

٧-تحفيز عمليّات التنقيب للعملات الرقمية اللامركزيّة

تواجه جماعات الارهاب تحديّاً آخر تجاه نشر العملات الرقمية تتعلق بكيفيّة تحفيز عمليّات التنقيب التي تضمّ العنصر الأمنيّ الرئيسي للعملات الرقمية. فإذا كان لدى تلك الجماعة سمعة عالميّة سيّئة كتنظيم داعش، حيث سيقوم افراد من كل مكان بتفادي التنقيب عن عملتها فإذا افترضنا أنّ ايسلكوين هي عملة التنظيم الرقمية فسوف يكون التنقيب غير قانونيّ في بعض الدول وفقا قوانين مكافحة الإرهاب. فإذا قل تنوع

(٧٣) دليل التعاملات الرقمية – البرنامج الوطني للذكاء الاصطناعي – صادر عن مكتب وزير الدولة للذكاء الاصطناعي– ص٤٦ص٤٩ – ٢٠٢٠
-https://ai.gov.ae/wp-content/uploads/2020/01/Blockchain_AR_v1-online.pdf

(ISSN: 2356 - 9492)

المنقبون جغرافيا، فقد يشكل ذلك تحديا امنيا كبيرا لسهولة استهدافهم. كما ان هذا التنوع قد يخفف من حدّتها. وكذلك عند التعامل مع العملة من موقع جغرافي ثابت وعلية فإن الحل هنا هو التيقن أنّ تلك العملات المشفرة تستحقّ الجهد لاستخدامها في المعاملات المالية عبر الإنترنت، ومع ما يثيره هذا من تحديّات منها ان العملات الرقمية المستعملة قد تهاجم العملات الحديثة منها، فان ثمة طرق متعددة لتحفيز التنقيب. منها ان يكون التنقيب للصالح العام، مما قد يشجع المستخدمين على التنقيب. كعملة "برايم كوين" حيث يتمّ التفتيش عن الأعداد الأوليّة في عمليّة التنقيب، والتقنية الأخرى لتحفيز عمليات التنقيب هي دمجه ضمن عمليات التنقيب عن العملات الرقمية. الا ان إمكانية أن تختار إدارة العملات الرقمية تعديل الاجراءات لعدم حدوث هذا التضمين حيث قد لا ينظر المنقّبين الى تمويل الإرهاب بالشكل الواجب وهو ما قد يؤدي لانهيار العملة.

ويعد التحدي الرئيس لترويج عملة رقمية هو كيفيّة إنشاء مثيل لها، أي الانتقال من صفر إلى كافة المستخدمين في المناطق التي يستهدفها التنظيم الإرهابي ، وقد عملت العملات الرقمية لأربع سنوات للوصول لقيمة بارزة كعملة، وقد فشلت عمليّات تداول العملة الافتراضية في كسب القبول في الواقع، لذا فإنّ أفضل وقت لاستهداف عملة رقمية هي انطلاقتها الأولى حيث تكون الثقة في العملة في حدّها الأدنى بالإضافة إلى أنّ احترافية القائمين على الدفاع ضد الهجمات تكون متواضعه جدا وأنّ الحساسية العامة لمدى استقرار ونجاح العملات تكون مرتفعة، فيصبح هذا التوقيت هو الأفضل للحد من تداول العملة وهز ثقة مستخدميها في موثوقيتها.(٧٤)

بالإضافة لوجود استراتيجية للحد من دعمها بعملة رقمية سابقة الوجود أو عملات مركزية أو سلع لترسيخ قيمة النقود الافتراضية. فإذا حصلت المنظمات الارهابية على دعم من احدى الدول، تستطيع تقييم العملة الرقمية بسعر صرف ثابت بعملتها أو بسلع استراتيجية تملكها لكن يتطلب ذلك التخلي عن سيطرتها الاقتصاديّة على العملات

(74)Muhammad Saad & others, End-to-End Analysis of In-Browser Crypto jacking- arXiv:1809.02152v1 [cs.CR] 6 Sep 2018 ,

الافتراضية، ومقايضة السرعة التي يتمّ بها قبول العملة الرقمية بعوائد التداول السياسيّة والاقتصاديّة.

٨- **ضمان مجهولية العملات الرقمية عند الاستخدام:** ويتضمن درجة قدرة العملات الرقمية على تحقيق المجهولية لمستخدميها، وأيضاً مدى صعوبة إزالة مجهولية بعض العمليات التي تتم باستخدام تلك العملات الافتراضية، ومدى المام المستخدم يكون هاما لأجل ضمان المجهولية. نركّز على العملات الرقمية ومسائل المجهولية المتعلّقة بها، وهنا سنبحث قدرة العملات الرقمية الجديدة والتقنيّة المرتبطة بها على تحقيق مجهولية المستخدم.

كما انّ التيقن من مجهولية العملة الرقمية أمر هام لأنّها تعد أهم خصائص العملات، لان أطراف المعاملة ينصبّ تركيزهم على مجهولية التحويلات غير المشروعة وان تكون مستحيلة التعقّب من قبل المؤسسات العسكريّة أو الأجهزة الامنية والاستخباريّة، وتنشأ مشكلات أخرى من استخدام عملة رقمية باعتبارها وسيلة يوميّة للتحويل. فبدون المجهولية يحجم المستخدمون عن استعمال العملات الرقمية في معاملاتهم. و"المجهولية" تعد مفهوم واسع، كما أنّ هجمات كشف المجهولية تتراوح بين هجمات تحتاج لجهد وفهم عميق لإزالة مجهولية مستخدم واحد وهجمات قراصنة تتطلّب بعض الجهد والإلمام لإزالة مجهولية المستخدمين. فإنّ تأكيد مجهولية مستخدم تختلف عن ضمان المجهولية من السلطات بواسطة مجموعات متمكّنة وملمّة تقنيّاً. ولكن عمليا، لا تقوم العملات الرقمية بهذا التمييز. حيث ان المسألتان متلازمتان حاليّاً لأنّ تمييز مصدر الهجوم والإلمام ليسا معيارين تصميمين في البنية التحتيّة المركزيّة. ففي إطار السلطة المركزيّة للعملة الرقمية تم مناقشة الطرق التي يمكن بها التمييز، وعمليا فإنّ العديد من العملات الرقمية، تحمي هويّة المستخدم من الملاحقة الامنية او القانونية فبرغم اهمية الثقة في سلطات اصدار العملات المركزية للقيام بذلك، بالاضافة الى ان العملات الرقمية ترتكز في تأمينها على المسلمات الرياضيّة فان الواقع يبين أنّ العملات الرقمية مستهدفة من سلطات انفاذ القانون بشكل كبير لأنّها تحاول تحقيق المجهولية

(ISSN: 2356 - 9492)

ولكنها معرضة للهجمات بسبب طبيعتها اللامركزية وهو ما يحفز حالة العملات الرقمية اللامركزية. (٧٥)

اما العملات الرقمية شبه المركزيّة فهي غير منتشرة بشكل كبير، لذا يتعذر تقييمها وتعد " ريبل " أفضل عملة رقمية شبه مركزيّة معروفة لانها مصممة للاستعمال العام فهي موجهه للمؤسسات الماليّة وليس الافراد.

كما اكدت دراسات التشفير ان العملات الرقمية شبه المركزيّة هي الأفضل للحفاظ على الأمن والخصوصيّة للمستخدمين بينما تتيح المجال في الوقت عينه للسلطات لوضع أنظمتها، مالم يتم تداول تلك العملة الرقمية.(٧٦)

ولما كان مسمى العملات الرقمية هو اسم مستعار لأنّ كل مستخدِم يمكن تمييزة من خلال سلسلة أرقام عشوائيّة تم توليدها بعمليات تقنية تسمي الهاش، بحيث لا تنكشف الهويّة الحقيقيّة للمستخدم فاذا لم يغيّر المستخدم عنوانه عند الانتقال من عمليّة لأخرى، يصبح تاريخ العمليّات بأكمله مكشوفا لمن يعرف عنوان العملات الرقمية المستخدم .لأنّ بلوك تشين العملات الرقمية، بدفتر الحسابات العام يعد هو السجل العام لكل العمليّات التي تمّت .لذا، فإنّ تكرار عمليّات العملات الرقمية باستخدام نفس العنوان يهدد مجهوليتها .كما أنّ عنوان العملات الرقمية سيصبح معروفاً للكافة ممن يتعامل مع المستخدم كالتجار والشركات، والأصدقاء المحول لهم أموال، والعملات الرقمية مغفلة فكل عمليّة مصرفيّة أو حساب مصرفيّ معروف للمتصلين بالإنترنت، والمعلومات الوحيدة التي تظل مجهولة هي هويّة مالك الحساب، وهو ما يمكن الاستدلال عليه من تفاعلات المستخدم.

(٧٥) العملات المشفرة - دائرة الإشراف والرقابة على نظام المدفوعات الوطني – البنك المركزي الاردني – ٢٠٢٠ - ص٣٥ ص٤٠
-https://www.cbj.gov.jo/EchoBusV3.0/SystemAssets/8f23f11e-de4c-4538-91f7-82aab2d7bf04.pdf

(76)Alan Lloyd Paris -Srinivasa Manikant Upadhyayula- Bitcoin: Currency of the future or money laundering vehicle? – global research &analytics – June 2017 – p:6

وعلى ذلك فالمجهولية غير مقبولة في المعاملات المالية، لذا يجب ايجاد ضمانات إضافية حيث تتطلب العمليّات الحاليّة للحفاظ على المجهولية إلى تعلّم التشغيل الإلكترونيّ أو" التقنيّات "لتحقيق الأمن المستهدف والتي تعد صعبة التحقق للشخص العاديّ .

وعند دراسة اسباب إحقاق مجهولية العملات الرقمية كممثلة للعملات الرقمية الأخرى نجد ان ذلك يرجع لسببين:

١-إنّ العملات الرقمية هي أكثر العملات الرقمية شعبية وبذلاً للجهود لحماية المعلومات

٢-تم بناء الكثير من العملات الرقمية باستخدام العملات الرقمية أساساً لها، لذا يمكن تحقيق مجهولية العملات الرقمية على عملات رقميه أخرى.

كما تضمّ مجهولية العملات الرقمية جانبين هما:

- مجهولية العمليّات الفرديّة
- مجهولية أنماط العمليّات .

ويتمّ ضمان مجهولية العمليّات الفرديّة في الغالب عن طريق تعيين اسم مستعار عشوائيّ لكل فرد الا انه يمكن تحديد العمليّة الفرديّة عن طريق فحص عناوين بروتوكول الإنترنت للمستخدمين، مما يكشف تاريخ صفقة المستخدم بالكامل لذا يمكن استخدام تقنيّات إخفاء بروتوكول الإنترنت إذا كانت المجهولية هي الهدف .لذا يفضل استخدام هذه التقنيّات، ويبدو محرك بحث تور لحماية الخصوصيّة في الصدارة لأنّ إزالة مجهولية هوية مستخدمي العملات الرقمية مع تور ممكنة بسبب طريقة صياغة العملات الرقمية.

بالإضافة الى ان عمليّة الاسم المزيف، لا تحفظ المجهولية بذاتها وعندما تتاح الفرصة للوصول لاسم مستعار لمستخدم آخر، يمكن لأيّ شخص رؤية جميع العمليّات والأرصدة المرتبطة به، لذا فان مواقع العملات الرقمية تطلب من المستخدمين تغيير الاسم المزيف عقب الاستخدام، برغم أنها لا تفرض ذلك، اما العملات الرقمية المتداولة يوميا، فهذه الاجراءات تكون مُدمجة وتعد جزء من النظام.

(ISSN: 2356 - 9492)

وقد أظهر مجتمع الأبحاث الأمنيّة القدرة على تحليل المسائل المرتبطة بالحدّ من الخصوصيّة على البلوك تشين الخاصّ بالعملات الرقمية لتحديد الهوية من نوعية العملية، وحلّا لهذه المشكلة، تم استخدام "خلط الخدمات" لاخفاء هذه العمليّات؛ حيث تقوم هذه الخدمات بتكديس العمليّات فيصعب تتبعها من العناصر الإرهابية او الاجرامية، وتشمل الخدمات المجهولية في عمليّات العملات الرقميّة" كوين جوين" وبروتوكولات تيسير الدفعات المجهلة من العملات الرقمية والمحافظ المظلمة" ميكس كوين" والتي توفِّر مستوى كاف من التأمين لهوية المستخدم، الا انه يبقى دائماً التهديد من المستجدات نتيجة التطور في تكنولوجيا العملات الرقمية والبلوك تشين لكشف الهوية والعمليّات السابقة، والتي تمت بإجراءات تضمن عدم امكانية كشف الهوية(٧٧)

ومن الناحية الاقتصادية، قد يواجه التشجيع على الاعتراف بالعملات الرقمية الجديدة بدلاً من اعتماد العملات المستعملة تحديّات عديدة من حيث قبولها كعملة جديدة، وبالتالي قد تفتقر للمشروعيّة لعدم تمتعها بتمثيل واضح كنقود في مجتمعات المال الماديّ. ويمكن للعملات الرقمية ان تلقى القبول المجتمعي عندما تنتشر تكنولوجيا العملات الرقمية وتصبح جديرة بالثقة. كما انه إذا كانت العملة الرقمية الوسيلة الوحيدة للقيام بالمعاملات في مكان ما، فقد يرغم الوضع الاقتصادي الناس على قبول العملات الرقمية، المرفوضة في احوال أخرى.

لذلك، فالأفضل لمنع المنظمات الاجرامية من تداول عملة رقمية هي استهداف خصائصها الأكثر زيادةً لقبولها، تحديدا مجهولية التحويل وأمانه وتوافره.

ومن الناحية التقنية : يشكّل تداول عملة رقمية بدلا من العملة المركزية في المعاملات التجاريّة تحدياً هاما .وتشمل التحديّات الوصول للإلمام التقني لتطوير عملة رقمية كخدمة إلكترونيّة وتداولها والحفاظ عليها وتأمين هوية المعاملات والمتعاملين لتأمين سلامة التعامل بها، حتّى يتأكّد أطراف المعاملات التجارية من صحة التبادل، دون الحاجة لإلمام تكنولوجيّ متقدّم، وأخيرا حماية سلامة العملة الرقمية الإجماليّ

(77)George Danezis -Sarah Meiklejohn- Centrally Banked Cryptocurrencies - arXiv:1505.06895v2] cs.CR] 18 Dec 2015- pp:5-7

وتوافرها من الأخطار الإلكترونيّة المتقدّمة، خاصة الدول المعارضة لتداول المنظمات الارهابية للعملات الرقمية كما يمكن ان يسبب وجود هذه التكنولوجيّات تسهيل عمليّة تداول المنظمات الارهابية للعملة الرقمية.

ويمكن ان تتّخذ السلطات الحكوميةقرارات بتحديد مستوى الفهم الإلكتروني اللازم لإبعاد عملة رقمية كما ان الاستثمار في الإمكانيات والوقت والأبحاث يحقق الابعاد المطلوب للعملات الرقمية.

وعندما تدعم دولة تتمتّع بإلمام إلكترونيّ متقدّم منظمة إجرامية او ارهابية، يصبح تداول هذه المنظمات الاجرامية للعملة الرقمية أكثر قابليّة للتنفيذ .وقد تسمح دولة للمنظمات الإجرامية والارهابية بالتغلّب على العقبات التقنيّة المهمّة التي ترتبط بتداول عملة رقمية، ويشمل ذلك قدرة الدولة على الدفاع عن منظمة إجرامية او إرهابية وحمايتها بهجوم إلكترونيّ بدرجة إلمام عالية من خصم آخر للدولة.

ويتمتع تداول العملات الرقمية بالقدرة على تطوير تكنولوجيات مرتبطة بالأمن القوميّ، كالخدمات الإلكترونيّة التي تزداد مرونةً مما يسهل استعمالها من قبل المنظمات الارهابية، كنشر المعلومات وتخزينها .وقد زاد التركيز المتنامي على العملات الرقمية الإلمام بالتشفير، مما يؤدّي إلى ظهور برمجيّات مؤمنه بشكل أكبر ومعدّات إلكترونيّة فعالة بشكل كبير في اختراق التشفير من جهة أخرى، ويشير الاتجاه التاريخيّ إلى تطوّر الخلفية الإلكترونيّة عامّة ومقاومة تتمثل في قدرة المنظمات الارهابية القليلة الإلمام في المجال الإلكترونيّ على الوصول الدائم والآمن للخدمات الرقمية، ولو عارضت سلطة دولة ملمّة باستعمالها .ويفرض ذلك مسئولية على حماية السلطات لمراقبة محتوى الإنترنت؛ وعلى الوصول للمحتوى المتطرّف؛ وعلى قدرة شنّ الدول لهجمات إلكترونيّة؛ وقدرتها على الحفاظ على اتّصال آمن ومجهول وغير قابل للانقطاع.[٧٨]

(٧٨) د. هبة عبد المنعم - واقع وآفاق إصدار العملات الرقمية – صادرة عن صندوق النقد العربي - موجز سياسات: العدد (١1) فبراير2020 – ص٣ص٧ - https://www.amf.org.ae/sites/default/files/publications/2021-12/issue-11-reality-prospects-digital-currencies-arab-countries.pdf

(ISSN: 2356 - 9492)

الفرع الثاني

محاور مواجهة مخاطر استخدام العملات الرقمية

من المتصور تزايد التعاملات بالعملات الرقمية المختلفة وذلك في اطار المضاربة لتحقيق الربح الا ان الأخطر على الاطلاق هو استخدامها على ما بينا في متن الدراسة سواء في الجريمة كشراء الأسلحة او تمويل الإرهاب او في الاعتداء على المنظومة الالكترونية للعملات الافتراضية ذاتها وتقليدها او سرقتها مما سيترتب علية خسائر اقتصادية فادحة وعلى ذلك فقد يتصور القيام بمواجهة تلك المخاطر المترتبة على انتشار استخدام العملات الرقمية في دولة الامارات من خلال عدة محاور تعمل معا في تناغم للوصول الى تنفيذ خطة متكاملة للوقاية من مخاطر استخدام العملات الرقمية وتتمثل تلك المحاور في محور قانوني تشريعي ومحور امني شرطي ومحور تقني ويمكن تفصيل تلك المحاور من خلال الاتي:

أولا: المحور القانوني التشريعي:

وذلك من خلال إقرار نصوص قانونية تضاف الى قانون العقوبات بتجريم الأفعال التي تمثل اعتداء على المنظومة الإلكترونية للعملات الرقمية مع وضع ضوابط قانونية لتحديد تلك العملات المشمولة بالحماية القانونية حيث ان الموقف الحالي انه طبقا **للمادة (٢٠٦) من قانون البنك المركزي المصري رقم ١٩٤ لسنه ٢٠٢٠م** : يحظر إصدار العملات المشفرة أو النقود الإلكترونية أو الاتجار فيها أو الترويج لها أو إنشاء أو تشغيل منصات لتداولها أو تنفيذ الأنشطة المتعلقة بها دون الحصول على ترخيص من مجلس الإدارة طبقاً للقواعد والإجراءات التي يحددها .

بينما تنص المادة ٥ فقرة ١من القانون الاتحادي لدولة الامارات رقم ١٠ لسنة١٩٨٠م بشأن المصرف المركزي الإماراتي والنظام النقدي وتنظيم المهنة المصرفية –أن للمصرف المركزي الاماراتي ممارسة امتياز إصدار النقد.

وقد حذر البنك المركزي من التعامل بالعملات الرقمية الافتراضية، وهو ما وجب علية القيام به كونه جهة إصدار العملة الوطنية، وعدم الاستعجال في التصريح بقبول

التعامل بها لحين الاستقرار على طبيعتها وطرق تنظيمها ومتابعتها وتأثيرها على العملة المركزية

بينما أطلقت إمارة دبي أولَ عملة رقمية رسمية مرتبطة بالدرهم الإماراتي تعتمد على تقنية البلوك تشين، سميت إم كاش وتتميز بتنظيمها القانوني .وتعد دولة الإمارات من اوائل دول العالم التي استخدمت تقنية بلوك تشين في القطاع المالي، لانها من الدول المهتمة بالتحول الذكي في كافة القطاعات، إلا أنها لم تَعترف بعملة البت كوين والعملات المشابهة لها؛ بسبب عدم تنظيمها من قبَل الجهات الرسمية والمنظمات الدولية .

وقد طرحت هيئة الأوراق المالية في الإمارات العملات الرقمية الافتراضية في أسواقها في عام ٢٠١٩م ، وتعمل الجهات الرسمية في الدولة بالتعاون مع المستشارين الدوليين في سنّ القوانين واللوائح الخاصة بالعملات الرقمية، وتطوير منصات التداول في أسواق الأسهم وقد أعلن نائب رئيس دولة الإمارات العربية المتحدة ورئيس مجلس الوزراء حاكم دبي في يناير ٢٠١٨ عن استراتيجية بلوك جين الإماراتية؛ لربط جميع الجهات الاتحادية والمحلية وإتمام التعاملات دون استخدام الاوراق، ويتجه مستثمرو الإمارات لتجارة العملات المشفرة من منصات عالمية ومحلية ، وتم إطلاق أول عملة رقمية من شركة Onegram ٢٠١٧م في دبي مدعومة باحتياطيّ الذهب وعلى ذلك فان دولة الإمارات تعمل على إصدار تشريع ينظم العملات الرقمية وإصدار عملة رقمية خاصة بها، ولم تمنع دولة الإمارات تداول البت كوين، وإنما حذرت من التعامل بالعملات التي تستخدم في المضاربات والاستثمارات الوهمية.[٧٩]

وفي هذا الشأن نرى ان هناك حاجه ماسة لوضع تنظيم تشريعي قانوني يمكن ان يلحق بقانون مكافحة جرائم تقنية المعلومات لحماية العملات الرقمية المشفرة وتداولها

(٧٩) عبد الله ناصر عبيد نصيري الزعابي - التنظيم القانوني للعملات الرقمية المستحدثة في التشريع الإماراتي والمقارن "دراسة تحليلية مقارنة" – الجامعة الامريكية بالإمارات – كلية القانون – قسم القانون الخاص – أطروحة مقدمة للحصول على الماجيستير في القانون الخاص – ص٤٣ص٤٥ – ٢٠١٨م - https://scholarworks.uaeu.ac.ae/private_law_theses/17

(ISSN: 2356 - 9492)

ومن ناحية اخرى اتاحه تداولها لما لذلك من اثر ايجابي على الاقتصاد المصري والتحول الرقمي الحتمي

ثالثا: المحور الأمني الشرطي:

تتعدّد التحديّات التي يجب أن تُدرَس في المستقبل، اولها إيجاد فهم أوضح للمقارنات بين العقبات التكنولوجيّة لولوج العملات الرقمية وقبول المجتمع لاستخدامها في المعاملات التجارية. وقد تكون امكانية الاستخدام محل دراسة بشكل خاصّ .ومن التحديّات أيضا معرفة مدى رغبة المستخدمين في الثقة بالعملات المشفرة القائمة على نظم تشفير متطورة .وما سيترتب على ذلك من اثار على العملات الجديدة، كعملة زيروكاش، التي تعتبر تقدما كبيرا نحو تحقيق المجهولية.

وثمة حاجة لمزيد من العمل للبحث في قدرات الجماعات الاجرامية والإرهابية على استثمار عملة افتراضية بدلا من مجرد تداولها .فمتى قد تختار تلك المنظمات الارهابية أن تستخدم عملة افتراضية بدلاً من النقود للقيام بتحويلات أو جمع التبرّعات أو تبييض الأموال بطريقة غير شرعيّة؟ وما هي العملات الافتراضية التي تصلح للاستعمال في هذه الطريقة؟ وما هي كمّيّة العملات الممكن استخدامها في التحويلات مع الحفاظ على المجهولية؟

لذا نحتاج لتحديد التكنولوجيّات المرنة التي تتيحها العملات الافتراضية أو العكس، ولا يبدو واضحاً ما إذا كانت الحوافز الاقتصاديّة ستسهم في تطوير خدمات إلكترونيّة اشمل .بالإضافة لدراسات إضافيّة لاكتشاف الأفكار بشأن البنية الرقمية العامّة والمرنة، لفهم التداعيات السياسيّة على المدي القريب والبعيد، فيما تصبح الخدمات الإلكترونيّة اكثر مرونة وانتشارا عند المستخدم الأقلّ إلماماً بالتقنيات.

الخاتمة:

تناولت في الدراسة بشكل أساسي العملات الرقمية مبينا ماهيتها وكيفية عملها وتبادلها وتاريخها وأنواع العملات الرقمية المختلفة ، وأوضحت في الدراسة اهم الأنماط المختلفة التي تستخدم في ارتكابها ومضاعفة خطورتها من خلال الدور الذي تلعبه تلك العملات الرقمية في تسهيل ارتكابها ومضاعفة الاثار السلبية للجريمة سواء في ذلك

الجنائية او الإرهابية ثم تناولت الجرائم التي ترتكب لسرقة وتزوير العملات الرقمية والالية الفنية التي ترتكب بها لتوضيح العملية الفنية التي تتم بها تلك الجرائم لكون العملات الرقمية هي برمجية رقمية لا توجد على ارض الواقع وانما هي برمجية مشفرة ذات قيمة مادية وفي الجزء الأخير من الدراسة تناولت مستقبل العملات الرقمية في دولة الامارات من خلال عدة محاور تركزت في المجال الأمني تحديدا حيث تناولت بالدراسة كيفية إيجاد استراتيجية امنية لاستشراف المخاطر الأمنية لاستخدام العملات الرقمية وكيفية التغلب على تلك المخاطر من خلالها مبينا التحديات التقنية والأمنية المختلفة في هذا الشأن ومنها ما يتعلق بالجماعات الارهابية

أولا: النتائج:

١- توصلت الدراسة الى ان العملات الرقمية لها دور كبير في تحقيق الرقمنه وسوف يكون لها دور فاعل من خلال الاليات الاقليمية كالشراكات الاقليمية في انتاج عملات مشفرة خاصة بها من خلال تعاون ثنائي ومتعدد الاطراف

٢- بالرغم من مخاطر الجرائم التي يمكن ان تقع على العملات المشفرة وتهدد امنها وموثوقيتها او ترتمب بواسطتها الا انها اثبتت في الفترة الاخيرة انها اصبحت لا غني عنها في الاقتصاد العالمي وانه يجب على السلطات مكافحة هذه النشطة الاجرامية والحد منها لتعزيز الاقتصاد الرقمي المعتمد عليها

ثانيا: التوصيات:

١- إذا كان استخدام العملات الرقمية لابد منه في ظل التحول الرقمي الكامل المرتقب فلابد من المبادرة بوضع استراتيجية امنية ذات عدة محاور تتضمن محور تقني يتمثل في إيجاد بلوك تشين خاص بالدولة ويتم من خلاله انتاج عملات رقمية وطنية تكون سلسلة الكتل التي يتم تبادلها من خلال خوادمها موجودة داخل الدولة ، والمحور الثاني يتعلق بالأمن الجنائي من حيث متابعة الأنشطة الاجرامية التي تتم عبر الشبكة العميقة وتنسيق الجهود مع الأطراف المعنية لتتبع وضبط عمليات التمويل لجماعات الإرهاب وتبادل الأموال وغسلها لصالح جماعات الجريمة المنظمة وذلك للحد من الاثار الأمنية السلبية للعملات الرقمية المحور الثالث هو المحور التشريعي حيث يتم تقنين تلك

(ISSN: 2356 - 9492)

العملات ووضع مواصفاتها الخاصة والجهات القائمة على انتاجها وكافة التفصيلات الخاصة بإنتاجها وتداولها والعقوبات المقررة للاعتداء على منظومتها الالكترونية في تقنين خاص او الحاق ذلك بقانون مكافحة جرائم تقنية المعلومات

٢- ادراج برامج تدريبية على فهم منظومة عمل العملات الرقمية والبلوك تشين الخاص بها في الدولة ضمن البرامج التدريبية للضباط العاملين في المجال وتخصصهم ضمن ضباط مكافحة الجرائم المالية.

قائمة المراجع:

أولا: الكتب:

١) المبادئ الأربعة للاستشارات الإدارية – النهج اللين في الرقمنة- ٢٠١٧م – متاح على الموقع الالكتروني: www.fourprinciples.com

٢) إيمانويل دورو واخرين – ديلويت" الرقمنةفي الشرق الأوسط "رحلة رقمية"– متاح على شبكة الانترنت على الرابط:

e.huawei.com/ae/edm/global/NationalTransformationInTheMiddleEast

٣) جوشوا بارون واخرين – تداعيات العملة الافتراضية على الامن القومي "البحث في إمكانية النشر من جهة فاعلة غير حكومية"- مؤسسة راند – كاليفورنيا- الولايات المتحدة الامريكية – ٢٠١٥م – www.rand.org/t/rr1231

٤) سيف الدِّين عَمُّوص – ترجمة: أحمد محمد حمدان – معيار البيتكوين "البديل اللامركزي للنظام المصرفي المركزي"- جون وايلي وأبناؤه، ريفر ستريت، هوبوكن، نيوجرسي – ٢٠١٩م- متاح على الموقع الالكتروني: http://www.copyright.com .

٥) ليندا بن طالب: غسل الأموال وعلاقته بمكافحة الإرهاب، دراسة مقارنه – دار الجامعة الجديدة –الإسكندرية – ٢٠١١م

ثانيا: الدوريات العلمية:

١) تقرير فيوتشر بيرفكت ١٠ – مشروع بحثي مقدم من قبل ذراع حلول المحتوى لمجلة" تكنولوجي ريفيو "الصادرة عن معهد" ماساشوستس للتكنولوجيا MIT (" Technology Review)بالتعاون مع القمة العالمية للحكومات – ٢٠١٨ م –متاح على الموقع الالكتروني:
https://www.iccia.com/sites/default/files/library/files/Future%20Perfect%2010%20Reports_Arb_Low%20res.pdf

٢) جوشوا بارون واخرين – تداعيات العملة الافتراضية على الامن القومي "البحث في إمكانية النشر من جهة فاعلة غير حكومية"– مؤسسة راند – كاليفورنيا– الولايات المتحدة الامريكية – ٢٠١٥م – www.rand.org/t/rr1231

٣) ساسكيا كالباكيس واخرين – الدليل الدراسي لامتحان شهادة اختصاصي معتمد في مكافحة غسيل الأموال – ط٤ – ميامي – الولايات المتحدة الامريكية – ٢٠٠٧م

٤) بسام أحمد الزلمي – دور النقود الإلكترونية في عمليات غسل الأموال – مجلة جامعة دمشق للعلوم الاقتصادية والقانونية –المجلد 26 العدد الأول– 2010 –

٥) عبد القادر شهيب، ممولو الإرهاب في مصر، دار الهلال، القاهرة، ط١ ١٩٩٤

٦) تشيلسي اية لويس – التخفي "نظرة متعمقة في شبكة تور (شبكة تخفي) وآثارها على امن الحاسوب وحرية الرأي والتعبير في العصر الرقمي" – مقال منشور في مجلة معهد دبي القضائي – السنة الثالثة – العدد الخامس – فبراير ٢٠١٥م

٧) دومينيك هيرمان ، رولف ويندولسكي وهانز فيدراث ، التسلل الى المواقع الالكترونية : تقنيات تعزيز التسلل الى الخصوصيات العامة مع مصنف متعدد الحدود مبني على خوارزمية (Naïve Bayes)، (2009
/http://dl.acm.org/citation.cfm?doid=1655008.1655013

٨) فيناي غوبتا , كونسينسيس – بناء المستقبل لعالم فائق الاتّصال عبر تقنيات بلوك تشين – دراسة منشورة على شبكة الانترنت على الموقع :
https://govtechprize.worldgovernmentsummit.org

(ISSN: 2356 - 9492)

ثالثا: الاطروحات العلمية:

١) أيمن عز الدين ابو صلاح – العملات الرقمية وعلاقتها بالتجارة الالكترونية" دراسة حالة: دولة الامارات العربية المتحدة –دبي"– رسالة ماجيستير – جامعة الشرق الأوسط – كلية الاعمال – قسم المحاسبة – ٢٠١٨م

٢) ايمن عز الدين أبو صلاح – العملات الرقمية وعلاقتها بالتجارة الالكترونية "دراسة حالة " دولة الامارات العربية المتحدة (دبي) – رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجيستير في المحاسبة – جامعة الشرق الأوسط – عمان – الأردن – ٢٠١٨م

٣) ايمن عز الدين أبو صلاح – العملات الرقمية وعلاقتها بالتجارة الالكترونية "دراسة حالة " دولة الامارات العربية المتحدة (دبي) – رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجيستير في المحاسبة – جامعة الشرق الأوسط – عمان – الأردن – ٢٠١٨م

٤) د/ شامي يسين – تبييض الأموال عن طريق العملات الرقمية كجريمة مستحدثة – ورقة عمل مقدمة للمؤتمر الدولي الخامس عشر لكلية الشريعة والدراسات الإسلامية بجامعة الشارقة "العملات الافتراضية في الميزان"– المنعقد بجامعة الشارقة ١٦، ١٧ ابريل ٢٠١٩م

٥) عبد الله ناصر عبيد نصيري الزعابي – التنظيم القانوني للعملات الرقمية المستحدثة في التشريع الإماراتي والمقارن "دراسة تحليلية مقارنة" – الجامعة الامريكية بالإمارات – كلية القانون – قسم القانون الخاص – أطروحة مقدمة للحصول على الماجيستير في القانون الخاص – ٢٠١٨م https://scholarworks.uaeu.ac.ae/private_law_theses/17

٦) كاثرين ستيوارت – العملة الافتراضية "اجراء المعاملات وتبادل القيمة في العصر الرقمي"– لمحةٌ حول الندوة الاستشارية المعنية بالعملة الرقمية التي عُقِدَت كجزءٍ من برنامج معهد كورشام للقيادة الفكرية لعام ٢٠١٧م – www.rand.org/t/CF371

رابعا: المراجع الأجنبية:

1) Vittorio Aronica & others, digital transformation Leading our customers towards a new economy of digital ecosystems, 2018, www.eng.it

2) Vittorio Aronica & others, digital transformation Leading our customers towards a new economy of digital ecosystems, 2018, www.eng.it

3) Rick Wright & others, Destination (un)known" Key steps to guide your digital transformation journey", pp:3-7 ,available on : www.kpmg.com/digital

4) Dong He, Karl Haber Meier & others , Virtual Currencies and Beyond: Initial Considerations,2016

5) Alan Lloyd Paris& Srinivasa Manikant Upadhyayula, Bitcoin: Currency of the future or money laundering vehicle?, June 2017,global research &Analytics

6) Geo_ Goodell& Tomaso Aste, Can Cryptocurrencies Preserve Privacy and Comply with Regulations?, arXiv:1811.12240v3 [cs.CY] 7 May 2019

7) Alan Brill, Lonnie Keene, Cryptocurrencies: The Next Generation of Terrorist Financing?, Defense Against Terrorism Review, Vol. 6, No. 1, Spring &Fall 2014

8) Geo_ Goodell& Tomaso Aste, Can Cryptocurrencies Preserve Privacy and Comply with Regulations?, arXiv:1811.12240v3 [cs.CY] 7 May 2019,pp:

9) SEC "office of investor –education –advocacy" ,Investor Alert Ponzi schemes Using virtual Currencies, SEC Pub. No. 153 (7/13),available online: www.investor.gov

10)Ittay Eyal and Emin Gun Sirer, Majority is not Enough: Bitcoin Mining is Vulnerable,

11)Muhammad Saad, Aminollah Khormali, Aziz Mohaisen, End-to-End Analysis of In-Browser Cryptojacking,pp:3-5,2018,available online: https://arxiv.org/pdf/1809.02152.pdf

12)ciupa katarzyna, cryptocurrencies: opportunities, risks and challenges for anti-corruption compliance systems, OECD global anti-corruption& integrity forum , 20-21 march 2019 ,Paris, OECD conference ,p:3

13)The Telegraph. Britain’s first Bitcoin heist as trader forced at gunpoint to transfer cyber currency. 28 January 2018

(ISSN: 2356 - 9492)

http://www.telegraph.co.uk/news/2018/01/28/britains-first-bitcoin-heist-trader-forced-gunpoint-transfer/ accessed 2 February 2018.

14) Malte Möser& others,An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem, Pre-publication copy. To appear in the proceedings of the 2013 e-Crime Researchers Summit (e-Crime) published by IEEE, pp:3-9 , available on: https://maltemoeser.de/paper/money-laundering.pdf

15)A n d r e w t a r p e y, The money laundering risk of cryptocurrencies, Southpac Group, New Zealand,2018,available on: www.southpacgroup.com

16)ciupa katarzyna, cryptocurrencies: opportunities, risks and challenges for anti-corruption compliance systems ,OECD global anti-corruption &integrity forum , 20-21 march 2019 ,Paris ,OECD conference

17)Vandervort, David, Dale Gaucas, and Robert St. Jacques, "Issues in Designing a Bitcoin-Like Community Currency," paper presented at the Second Workshop on Bitcoin Research, San Juan, Puerto Rico, January 30, 2015

18)History of Bitcoin: the world's first decentralized currency, http://historyofbitcoin.org/(last visited Jan.23,2016).

19)Satoshi Nakamoto , bitcoin : A Peer – to – Peer Electronic Cash System , Bitcoin Project , https://bitcoin.org/bitcoin.pdf(last visited Jan.22,2016).

20)Paul Anning , Stuart Hoegner,& Jerry Brito , The Law of Bitcoin, 2015.

21)Deborah Hastings ,Va. Teen gets 11 years in prison for tweeting about ISIS , aiding the terrorist group ,N.Y. Daily News (Aug.28,2015),http://www.nydailynews.com/news/national/va-teen-11-years-rpison-aiding-isis-article-1.2340577.

22)Marry-Ann Russon, Paris attacks: EU to crack down on bit coin transfers in attempt to strange Isis funding, Int'1 Bus. Times (Nov.20, 2015, 11:50 AM),http://wwwibtimes.co.uk/paris-attacks-eu-crack-down-bitcoin-transfers-attempt-strangle-isis-funding-1529693.

23)Mark Koba , The federal Reserve: CNBC Explains ,CNBC (Mar.18,2015, 9:21 am), http://www.cnbc.com/id/43752521.

24)Kevin Drumm , Bitcoin is a fait Currency ,But That's not Its big Problem , Mother Jones (Feb.25,2014,11:54am) ,http://www.motherjones.com/Kevin-drum/2014/02/bitcoin-fait-currency-that's-not-its-big-problem.

25)Edward Murphy , Federation of American Scientists , Cong .Research Serv.(Nov.12,2015) ,http://www.fas.org/sgp/crs/mist/R43339.pdf.

26)Andes: Bitcoin's kryptonite: The 51% attack. https://bitcointalk.org/index.php?topic=12435 ,(June 2011)

27)Itay Eyal and Emin Gun Sirer, Majority is not Enough: Bitcoin Mining is Vulnerable, from book" Financial Cryptography and Data Security": 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers

28)Maria Apostolaki& others ,Hijacking Bitcoin: Routing Attacks on Cryptocurrencies, https://btc hijack.ethz.ch

29)Madeleine gart ,Ida linderbrandt,Are Cryptocurrencies the Future of Money?, kth royal institute of technology school of computer science and communication

30)Muhammad Saad& others, End-to-End Analysis of In-Browser Crypto jacking- arXiv:1809.02152v1 [cs.CR] 6 Sep 2018

خامسا: مواقع الانترنت:

١) الدكتور/ عدنان مصطفى البار – تقنيات الرقمنة– دراسة منشورة على شبكة الانترنت على الموقع الالكتروني: www.kau.edu.sa › GetFile

٢) وسام العباس لوتاه – البلوك تشين عالم من الفرص – مقال منشور على الموقع الرسمي لحكومة دبي:
:https://government.ae/ar-ae/participate/blogs/blog?id=40

3) https://arabic.rt.com/news/808846D8%AA%D9%86%D8%B8%D9%8A%D9%85%D8%A7%D8%AAD8%A5%D8%B1%D9%87%D8%A7%D8%A8%D8%AF%D8%A7%D8%B9%D8%B4%D8%A7%D9%86%D8%AA%D8%B%86%D8%AA%D8%AF%D8%A7%D8%B1%D9%83%D9%88%D9%8A%D8%A8/

4) http://www.huffpostarabi.com/2016/01/25/story_n_9059062.html

5) http://www.migliorisiabogados.com/que-es-la-deep-web-que-peligros-esconde/?lang=ar