تداعيات العملة الافتراضيّة على الأمن القوميّ

البحث في إمكانيّة النشر من جهة فاعلة غير حكوميّة

جوشوا بارون، أنجيلا أوماهوني، دايفيد مانهايم، وسينثيا ديون–شفارتس

(Joshua Baron, Angela O'Mahony, David Manheim, Cynthia Dion-Schwarz)

RAND CORPORATION

للحصول على مزيد من المعلومات حول هذا المنشور، الرجاء زيارة الموقع الإلكتروني: www.rand.org/t/rr1231

البيانات المفهرسة التابعة لمكتبة الكونغرس.
الرقم الدولي المعياري للكتاب: 978-0-8330-9183-3

نشرتها مؤسّسة RAND، سانتا مونيكا، كاليفورنيا.

حقوق الطبع والنشر الإلكتروني محدودة

إدعموا مؤسسة RAND
قدّموا مساهمةً خيريّةً معفاةً من الضريبة عبر الموقع التالي
www.rand.org/giving/contribute

www.rand.org

تمهيد

يبحث هذا التقرير في الجدوى من قيام جهات فاعلة غير حكوميّة بزيادة نفوذها السياسيّ و/أو الاقتصاديّ عن طريق نشر عملة افتراضيّة (VC) لاستخدامها في العمليّات الاقتصاديّة العاديّة. والعملة الرقميّة الإلكترونيّة بتكوين (Bitcoin) هي تمثيل رقميّ لعملة مقيّمة يمكن تحويلها أو تخزينها أو تداولها إلكترونيّاً، شأنها شأن العملة العاديّة. ولا تصدر العملات الافتراضيّة لا عن البنك المركزيّ ولا عن السلطات العامّة، وليست بالضرورة متعلّقة بعملة ورقيّة (كالدولار واليورو...). إنما يقبل الناس بها وسيلة للدفع. وطرحنا الأسئلة البحثيّة الآتية من المنظورين التكنولوجيّ والسياسيّ الاقتصاديّ:

- لماذا قد تقدم جهة فاعلة غير حكوميّة على نشر عملة افتراضيّة؟ وبمعنى آخر، ما الفائدة السياسيّة و/أو الاقتصاديّة من نشرها؟ وكيف يمكن للجهة الفاعلة غير الحكوميّة هذه أن تقوم بعمليّة نشر مماثلة؟ وما هي التحدّيات التي سيتعيّن على هذه الجهات التغلّب عليها؟
- كيف يمكن لحكومة أو منظّمة أن تنجح تقنيّاً في تعطيل نشر عملة افتراضيّة من قبل جهة فاعلة غير حكوميّة، وما هي درجة الإلمام الإلكترونيّ المطلوبة؟
- ما هي القدرات الإضافيّة التي تصبح ممكنة عندما تُستخدم التكنولوجيا المستعملة في تطوير العملات الافتراضيّة وتطبيقها لأغراض أوسع نطاقاً من العملة؟

إنّ هذا التقرير معدّ ليكون ذا فائدة لصانعي السياسات المهتمّين بمسائل التكنولوجيا ومكافحة الإرهاب والاستخبارات ومسائل إنفاذ القانون وللباحثين في العملة الافتراضيّة والأمن الإلكترونيّ.

هذا البحث برعاية مكتب وزير الدفاع الأمريكيّ. وأُجري في مركز سياسات الدفاع والأمن الدوليّ في معهد أبحاث RAND للدفاع الوطني، وهو مركز أبحاث وتطوير مموّل فدراليّاً برعاية مكتب وزير الدفاع الأمريكيّ والأركان المشتركة، والقيادة الموحّدة للقوات المقاتلة، والبحريّة، ومشاة البحريّة ووكالات الدفاع ومصلحة الاستخبارات الدفاعيّة.

للمزيد من المعلومات حول مركز RAND للأمن الدوليّ وسياسات الدفاع، يرجى زيارة الرابط الآتي http://www.rand.org/nsrd/ndri/centers/isdp.html أو الاتصال بمدير المركز (وفق بيانات الاتصال المتوفرة على صفحة الموقع الإلكتروني).

يرجى توجيه أيّ تعليقات أو أسئلة حول هذا التقرير إلى مدير المشروع، جوشوا بارون، على البريد الإلكتروني: Joshua_Baron@rand.org

جدول المحتويات

الأشكال والجداول

الأشكال

الجداول

الملخّص

إنّ العملة الافتراضيّة هي تمثيل رقمي لقيمة يمكن تحويلها أو تخزينها أو تداولها إلكترونيّاً لا تصدر عن البنك المركزي أو السلطات العامة وليست بالضرورة متعلّقة بعملة ورقيّة (الدولار، اليورو...) إنما يقبل الناس بها كوسيلة للدفع. فالعملة الافتراضيّة الأكثر شعبيّة حالياً هي البتكوين (Bitcoin). وقد أصبحت تداعيات بروز تكنولوجيا العملة الافتراضيّة على سياسة الأمن القوميّ موضوع جدل كبير في الآونة الأخيرة، إذ إنّه تمّ التركيز بنوع خاصّ على المجهولية المحتملة للعملات الافتراضيّة مثل بتكوين (Bitcoin) فضلاً عن إمكانيّة استخدامها من قبل مجموعة إرهابيّة أو متمرّدة بطريقة يصعب مواجهتها بالجهود التي تبذلها منظّمات إنفاذ القانون المحلّيّ والدوليّ، والمنظّمات العسكريّة والمخابراتيّة (بما في ذلك تلك التابعة للولايات المتحدة). والهدف من هذا التقرير هو إثراء الحوار حول هذه السياسة من خلال توفير تحليل متعمّق للقضايا التكنولوجيّة المرتبطة بالعملات الافتراضيّة.

ويبحث هذا التقرير في قدرة جهات فاعلة غير حكوميّة، بما في ذلك المجموعات الإرهابيّة والمتمرّدة، على زيادة نفوذها السياسيّ و/أو الاقتصاديّ عن طريق نشر العملات الافتراضيّة كوسيلة للعمليّات الاقتصاديّة العاديّة، مقابل استغلال العملات الافتراضيّة المنتشرة بالفعل، مثل البتكوين، كوسيلة من الوسائل غير المشروعة لتحويل الأموال وجمعها وتبييضها.

نبحث في مسألة نشر العملة الافتراضيّة من المنظورين التكنولوجيّ والسياسيّ الاقتصاديّ، مع التركيز بشكل خاصّ على التحدّيات التي تواجهها الجهات الفاعلة غير الحكوميّة التي تحاول نشر العملة الافتراضيّة. وتُظهِر هذه التحدّيات كيف يمكن للولايات المتّحدة وحلفاؤها والجهات الفاعلة الأخرى في المجال الإلكترونيّ أن تتصرّف حيال نشر العملة الافتراضيّة، هذا في حال تهديده مصالح الأمن القوميّ. وحتى يومنا هذا، لم تحدث أيّ قضيّة بشأن نشر العملة من قِبل جهات فاعلة غير حكوميّة. إنّ هدف هذا التقرير

هو تسليط الضوء على تلك المسائل الرئيسة التي قد تكون اليوم بمثابة حواجز تكنولوجيّة وسياسيّة اقتصاديّة لنفهم لماذا قد يصبح هذا النشر أكثر جدوى وفائدة للجهة الفاعلة غير الحكوميّة في المستقبل.

وسنبحث أيضاً بإيجاز في التداعيات التكنولوجيّة الأوسع للعملات الافتراضيّة وتوافر تكنولوجيّات مشتقّة عنها للمستخدمين غير الملمّين في الفضاء الإلكترونيّ. أوّلاً، سنقوم بالتحقّق من تقنيّات قد يحسّنها تطوّر العملة الافتراضيّة، بما في ذلك الإلمام العام المتزايد بتطبيقات التشفير. وبشكل أعم، نبرهن أنّ المساهمة التكنولوجيّة الرئيسة للعملات الافتراضيّة اللامركزيّة، من منظور الأمن القوميّ، هي مرونة الفضاء الإلكترونيّ، ونسأل: ما هي التداعيات الممكنة على السياسات، في حال تمكّنت جهات فاعلة غير ملمّة في المجال الإلكترونيّ من الوصول الدائم والآمن إلى الخدمات الإلكترونيّة، بغضّ النظر عمّا إذا كانت جهة حكوميّة على درجة عالية من الإلمام تعارض استخدامها؟

أمّا أسئلتنا البحثيّة الرئيسة والإجابات عليها فهي على الشكل التالي:

- لماذا قد تنشر جهة فاعلة غير حكوميّة عملة افتراضيّة؟ وبمعنى آخر، ما هي الفائدة السياسيّة و/أو الاقتصاديّة من وراء عمليّة نشر مماثلة؟ كيف ستقوم الجهة الفاعلة بهذا النشر؟ وما هي التحديّات التي يجب على الجهة الفاعلة التغلّب عليها؟

– قد يكون نشر عملة افتراضيّة ما بديلاً مثيراً للإهتمام للجهات الفاعلة غير الحكوميّة التي تتطلّع إلى تعطيل السيادة وزيادة سلطتها السياسيّة و/أو الاقتصاديّة، من خلال إحلالها محل العملات التي تصدرها الدولة. وتكون عمليّات نشر العملات الافتراضيّة مثيرة للإهتمام بشكل خاصّ في البلدان النامية، وفي البلدان التي تعاني اضطرابات داخليّة حيث تكون البنية التحتيّة الماليّة القائمة إمّا غير كافية أو ضعيفة. إنّ النشر السريع للعملات الافتراضيّة في منطقة جغرافيّة واسعة قد يكون على الأرجح أقل تعقيداً من نشر عملات أكثر شيوعاً، كتلك القائمة على السلع أو كالعملات الورقيّة. وتشمل الأمثلة عن الجهات الفاعلة غير الحكوميّة المعنيّة هنا المنظّمات الإرهابيّة والمجموعات المتمردة وعصابات المخدّرات ومنظّمات إجراميّة أخرى.

– إنّ اعتماد جهة فاعلة غير حكوميّة عملة افتراضيّة مستعملة، مثل بتكوين، لا يوفّر فوائد سياسيّة أو اقتصاديّة كثيرة ومن المرجّح أن يكون عرضة لهجوم إلكترونيّ من قبل خصم ملمّ، في حين أنّ مواجهة العديد من تحديّات التطبيق لعملة افتراضية مستعملة مماثل لمواجهة تحديّات عملة افتراضيّة جديدة.

– لكنّ عمليّة تطوير عملة افتراضيّة من الصفر تتطلّب إلماماً تكنولوجيّاً عالياً وبنية تحتيّة حاسوبيّة وبنى تحتيّة لشبكات الإنترنت واسعة النطاق، مع خبرة كافية لضمان طرحها واعتمادها بنجاح، وكلّ ذلك غير متوفر لدى الجهات الفاعلة غير الحكوميّة. وتشمل التحديّات الخاصّة تطوير البرمجيّات من أجل الحصول على عملة افتراضيّة فاعلة وآمنة؛ ونشر الوسائل للقيام بعمليّات تحويل ماديّة بواسطة عملة افتراضيّة، ولا سيما في البلدان التي تقلّ فيها الهواتف الذكيّة؛ والتغلّب على قدرة الدول القوميّة على شنّ هجمات إلكترونيّة ناجحة على العملة الافتراضيّة.

– ومن منظور اقتصاديّ، قد يواجه التشجيع على اعتماد العملات الافتراضيّة (مقابل اعتماد العملات المستعملة) تحديّات مهمة في قبول المجتمع حيث تطبّق بها كونها عملة جديدة تفتقر إلى الخلفيّة التاريخيّة، وبالتالي إلى الشرعيّة، كونها عملة غير ملموسة في المجتمعات التي اعتادت أن يكون المال فيها ماديّاً. ونتوقّع أن يخفّ حذر المجتمعات حيال العملات الافتراضيّة مع اعتيادها أكثر. وقد تحصل تغيّرات في المواقف عندما تصبح التكنولوجيا التي تقوم عليها العملات الافتراضيّة أكثر شيوعاً وجدارة بالثقة. إضافةً إلى ذلك، ففي الأماكن التي تكون فيها العملة الافتراضيّة الوسيلة الوحيدة للقيام بعمليّات التحويل، سترغم الحاجة الاقتصاديّة الناس على القبول بالعملات الافتراضيّة، رغم رفضهم لها في حالات أخرى.

– وسيكون نشر عملة افتراضيّة من قبل جهات فاعلة غير حكوميّة أسهل وأجدى في الواقع اليوم، عندما تدعمه دولة قوميّة ذات خبرة إلكترونيّة متقدّمة. وقد تسمح هذه الدولة القوميّة بتمكين الجهات الفاعلة غير الحكوميّة في التغلّب على العقبات التقنيّة الكبيرة المرتبطة بنشر العملة الافتراضيّة. وتتعدّد المناطق في العالم التي قد ينشأ عنها دعم مماثل، كإيران (في دعمها حزب الله وسابقاً حركة حماس) وروسيا (في دعمها الانفصاليّين الأكرانيّين).

– وعلى الرغم من العقبات الحاليّة، فإن الإتجاهات تشير إلى مستقبل تتمكّن فيه جهات فاعلة غير حكوميّة أو غيرها من المنظّمات من نشر عملات افتراضيّة، ولا سيما في ظل الوتيرة السريعة التي ستصبح فيها التكنولوجيّات اللازمة متاحة للشراء ونظراً للفهم العام المتنامي للعملات الافتراضيّة وإن تدريجيّاً.

• كيف تستطيع حكومة أو منظّمة أن تعطِّل بنجاح نشر عملة افتراضيّة جديدة من قبل جهة فاعلة غير حكوميّة وما هي درجة الإلمام الإلكترونيّ المطلوبة؟

– سيكون من الصعب على جهة فاعلة غير حكوميّة تنفيذ تصميم هيكلي لعملة افتراضيّة مرنة لمواجهة الهجمات وقابلة للاستخدام من قبل الجميع في منطقة

جغرافيّة خاضعة لنفوذ الجهة الفاعلة غير الحكوميّة. وتتفاقم هذه الصعوبة في المناطق التي يكون فيها الإلمام التكنولوجيّ أكثر ضعفاً وفي المناطق حيث البنية التحتيّة للشبكات غير كاملة.

– تكون العملات الافتراضيّة معرّضة لهجمات ذات درجات إلمام متفاوتة.

- وقد تشمل الهجمات التي تفتقر إلى الإلمام نسبيّاً من قبل الحكومات وغيرها من الجهات الفاعلة غير الحكوميّة، أو حتى مستخدمي عملة افتراضيّة أخرى، هجمات قطع الخدمة الموزّع مقابل خدمات أكثر مركزيّة، مثل مجمّعات التنقيب أو تطبيقات المحفظة الإلكترونيّة على شبكة الإنترنت، أو محاولات السيطرة على عملة افتراضيّة عبر استغلال قواعد سوق العملة الافتراضيّة، كمن خلال توفير معظم القوّة الحاسوبيّة لعملات افتراضيّة شبيهة ببتكوين.
- ويمكن مهاجم آخر أكثر إلماماً بهذا المجال أن يشنّ هجمات فوريّة مباغتة للاستفادة من أيّ ضعف في البرمجيّات لا يكون المُطوِّر على علم به ولا يمكن تصحيحه. ويمكن لهجمات فوريّة مباغتة أن تستهدف خدمات العملات الافتراضيّة، مثل التبادلات والمحفظات، وكذلك تطبيقات الهاتف الخلوي المستخدمة في العمليّات الشائعة.
- ويمكن المنافسون الأكثر إلماماً بهذا المجال مهاجمة البنى التحتيّة الأساسيّة للعملات الافتراضيّة، بما في ذلك الأجهزة، أو القيام سرّاً بإفساد البرمجيّات المستخدمة من قبل المشاركين في العملات الافتراضيّة، بما في ذلك تخريب آليات الأمن الأساسيّة التي تعتمد عليها البرمجيّات.

• ما هي القدرات الإلكترونيّة الإضافيّة، غير استخدام العملات الافتراضيّة، التي تصبح ممكنة، ليس للجهات الفاعلة غير الحكوميّة فحسب، مع إستمرار التكنولوجيّات القائمة بالتطوّر وتطبيق العملات الافتراضيّة في النضوج؟ ويمكن أن يسهم تطوير العملات الافتراضيّة وتطبيقها في التطوّرات التكنولوجيّة المرتبطة بالأمن خارج ساحة العملات، ما قد يساعد جهات فاعلة غير حكوميّة.

– تبرهن العملات الافتراضيّة أنّها وسيلة مرنة لتخزين البيانات بطريقة توزيع متشعّبة يصعب إفسادها. أمّا التداعيات المحتملة لذلك فتشمل نشر المعلومات (في مدوَّنات إلكترونيّة ووسائل التواصل الإجتماعيّ ومنتديات ومواقع إخباريّة) الذي يكون في نهاية المطاف مرناً تماماً في مواجهة تدخّل الدولة القوميّة.

– قد تشجّع الحاجة إلى تطوير آليات أمن للعملات الافتراضيّة على تطوير تقنيّات تشفير متقدّمة، مثل الحوسبة الآمنة المتعددة الأطراف، التي تسعى إلى أداء حوسبة موزّعة فيما تحافظ على سرّيّة المُدخَلات والمُخرَجات في ظلّ وجود نشاط خبيث.

– تشكّل العملات الافتراضيّة أحدث خطوة نحو خدمات إلكترونيّة لامركزيّة. وعلى وجه الخصوص، يوحي الإتجاه التاريخيّ بتطوّر أرضيّة إلكترونية أساسيّة عامة ومرنة يُعرِّف عنها هذا التقرير بأنّها قدرة جهات فاعلة غير ملمّة في المجال الإلكترونيّ على الوصول إلى الخدمات الإلكترونيّة بشكل دائم وآمن، بغضّ النظر عمّا إذا كان هناك جهة فاعلة حكوميّة على درجة عالية من الإلمام تعارض استخدامها. ويؤثّر ذلك على جدران الحماية الوطنيّة والوصول إلى الخطاب المتطرّف وإمكانية شنّ قراصنة الحاسوب هجمات والقدرة على الحفاظ على روابط مشفّرة غير قابلة للإنقطاع ومغفلة.

يجب أن تعي إدارة الدفاع ما يلي: العملات الافتراضيّة أداة تتزايد إمكانيّة تنفيذها على المستوى التكنولوجيّ لتنشرها الجهات الفاعلة غير الحكوميّة. وإنّ الجهود الرامية إلى زعزعة الثقة في أيّ عملة افتراضيّة جديدة هي جهود فعّالة، في حين أنّ المجتمع لا يزال لا يثق بالعملات الافتراضيّة للقيام بالعمليّات الشائعة؛ فالعملات الافتراضيّة هي تماماً مثل أيّ خدمة أخرى في الفضاء الإلكترونيّ. أمّا طرق مهاجمتها بنجاح فلا تختلف كثيراً عن أيّ عمليّة هجوم أخرى في الفضاء الإلكترونيّ. وتتيح اللامركزيّة مرونة أكثر، وإن غير كاملة، للتكيُّف مع الإضطرابات الناتجة عن الهجمات الإلكترونيّة. وأخيراً، سيسهّل الإتجاه نحو خدمة إلكترونيّة لامركزيّة على الجهات الفاعلة غير الملمّة في المجال الإلكترونيّ الوصول المرن والمتزايد إلى الخدمات الإلكترونيّة. ويشكّل ذلك طريقاً ذا إتجاهين قد يتيح، بشكل غير مسبوق، الوصول العالمي إلى خدمات المعلومات والإتصالات التي، بجوهرها، قد تكون مفيدة وضارّة في آن معاً لمصالح الأمن القوميّ في الولايات المتحدة.

شكر وعرفان

لما كان هذا العمل ممكناً من دون قيادة عدد كبير من الزملاء في مؤسسة RAND وتوجيههم. ونحن ممتنّون بشكل خاصّ لريان هنري (Ryan Henry) الذي دفع بهذا المشروع إلى عتبة التنفيذ. نشكر سيث جونز (Seth Jones) لدعمه وتوجيهه ومايكل ماكنيرني (Michael McNerney) لعمله في تحديد نطاق المشروع منذ بدايته وكريستوفر تشيفيس (Christopher Chivvis) لتوجيهه القيّم لمشروع هذا العمل. ونشكر أيضاً ليليان أبلون (Lillian Ablon) والملازم الكولونيل وليام فراي (William Fry) من القوّات الجوّيّة الأمريكيّة) وريتشارد نو (Richard Neu) وهاورد شاتز (Howard Shatz) وكورتني وينباوم (Cortney Weinbaum) على إشراكنا خبرتهم الواسعة.

نتوجّه بالشكر أيضاً لياشا تبريزي (Yasha Tabrizy) (من وزارة المالية) ولريان أوتيسون (Ryan Otteson) (من مكتب التحقيقات الفدراليّ سابقاً) لتوفيرهما الرؤية والإطار القيِّمَين والهامَّين.

ونحن ممتنّون لآرون برانتلي (Aaron Brantly) من أكاديميّة وست بوينت العسكريّة الأمريكيّة، ولزميلينا كريشنا كومار (Krishna Kumar) من مؤسسة RAND وتيم ماورر (Tim Maurer) من منظّمة أمريكا الجديدة (New America) لمراجعاتهم الدقيقة للمُخطّطات.

كما نشكر هولي جونسون (Holly Johnson) وجيمس كييزا (James Chiesa) وإرين ديك (Erin Dick) وتيريزا ديماجيو (Theresa DiMaggio) وكريستوفر ديركس (Christopher Dirks) ونيدا رحمة (Nedda Rahme) على مساعدتهم في تحرير هذه الوثيقة.

لا يعني دعم الأشخاصّ الذين تقدّمنا لهم بالشكر ومساعدتهم لنا أنّهم يتفقون مع الآراء المطروحة في هذا التقرير. كما أنّ أيّ أخطاء وردت فيه هي أخطاء المؤلّف دون سواه.

الإختصارات

DARPA	وكالة الدفاع لمشاريع البحث المتقدمة
DDoS	قطع الخدمات الموزَّع
DoD	وزارة الدفاع
HUMINT	الذكاء البشريّ
IP	بروتوكول الإنترنت
ISIL	الدولة الإسلاميّة في العراق والشام
MPC	الحوسبة الآمنة المتعدِّدة الأطراف
TTP	تكتيكات وتقنيّات وإجراءات
VC	عملة افتراضيّة
VOIP	الصوت عبر بروتوكول الإنترنت
ZK-SNARKs	معرفة منعدمة – حجج مقتضبة للمعرفة

المقدّمة

مع إدخال بتكوين وتزايد الحديث عنها، إزداد الإهتمام بالعملات الافتراضيّة بشكل كبير[1]. ويتنوّع هذا الإهتمام مع تنوّع المجتمعات: ابتداءً من أصحاب المشاريع ورأس المال إلى أكاديميّي الأمن الإلكتروني إلى الاقتصاديين. إضافةً إلى ذلك، قامت مجموعات منظَّمة وحكومات باستكشاف العملات الافتراضيّة أو اعتمادها لأغراض شرعيّة وغير شرعيّة متنوّعة، وإن كان ذلك بدرجات متفاوتة من النجاح. أمّا اليوم، فتبقى الفائدة من استخدام العملات الافتراضيّة، على المديين القريب والبعيد، موضوع نقاش حاد.

إنّ أيّ عملة افتراضيّة عندما تصدر كعملة للعمليّات اليوميّة، تتطلّب بنية تحتيّة ماديّة جديدة أقل بكثير من العملات المدعومة من الحكومة والمستخدمة على نطاق واسع حالياً. ومع ذلك، فإنّ العملات الافتراضيّة تتطلّب أيضاً هندسة شبكات قادرة على دعم

[1] راجع ساتوشي ناكاموتو 2008، (Satoshi Nakamoto)، للمناقشة عن البتكوين. راجع أيضاً في هذا التقرير قسم "أُصول واتّجاهات العملات الإفتراضيّة" في الفصل الثاني للمزيد من الأمثلة حول العملات الإفتراضيّة التاريخيّة والحاليّة. تعطي السلطة المصرفيّة الأوروبيّة ("رأي السلطة المصرفيّة الأوروبيّة بالعملات الإفتراضيّة، 4 تمّوز 2014) تعريفاً عملياً للعملة الإفتراضيّة: "هي تمثيل رقميّ لقيمة لا تصدر لا عن البنك المركزيّ ولا عن السلطات العامّة، وليست بالضرورة متعلّقةً بالعملة الورقيّة (كالدولار واليورو...). ويقبل الأشخاص العاديّون والأشخاص القانونيّون بها كوسيلة للدفع ويمكن تحويلها أو تخزينها أو تداولها إلكترونياً". إنّ مطلب السلطة المصرفيّة الأوروبيّة بعدم إصدار البنك المركزيّ لأيّ سلطة عامّة عملاتٍ إفتراضيّةً سيكون موضوع بعض المناقشات في هذا التقرير. للمزيد من المناقشة عن التعريف بالعملات الإفتراضيّة، راجع أيضاً البنك المركزيّ الأوروبيّ، خطط العملات الإفتراضيّة، تشرين الأوّل 2012. وفي هذا التقرير، على سبيل الاصطلاح، سوف نستخدم عبارة عملات إفتراضيّة بدلاً من العملات الرقميّة أو العملات المشفَّرة. تجدر الإشارة إلى أنّ العملات الإفتراضيّة ليست جميعها عملات مشفَّرة، ولكن، بحسب التعريف المعتمد في هذا التقرير، العملات المشفَّرة جميعها هي عملات إفتراضيّة. وعلى الرغم من أنّه يمكن التمييز بين العملة الإفتراضيّة والعملة الرقميّة من حيث التعريف، سنعتبرهما متماثلتين.

مثل تلك العمليّات اليوميّة. نتيجة لذلك، فإنّ النشر السريع للعملة الافتراضيّة على مساحة جغرافيّة واسعة قد يكون إلى حدّ كبير أقلّ تعقيداً من نشر عملات تقليديّة إذ يمكن أن يكون مقدار العمل ورأس المال والبنية التحتيّة اللازمة لنشر عملة افتراضيّة أقل بكثير. ففي البلدان النامية والبلدان التي تمرّ بإضطرابات داخليّة حيث البنية التحتيّة الماليّة القائمة إما غير كافية أو ضعيفة، وحيث إنفاذ القانون ضعيف، قد يكون نشر العملة الافتراضيّة بديلاً جذّاباً للجهات الفاعلة غير الحكوميّة التي تسعى إلى زعزعة السيادة وزيادة قوّتها السياسيّة و/أو الاقتصاديّة الخاصّة. وتشمل الجهات الفاعلة غير الحكوميّة المعنيّة مثلاً المنظّمات الإرهابيّة والمجموعات المتمرّدة وعصابات المخدرات والمنظّمات الإجراميّة.

يجب على مجتمع الأمن القوميّ الأمريكيّ أن يفهم كيف يمكن لهذه الجهات الفاعلة غير الحكوميّة استغلال العملات الافتراضيّة بمثابة أداة أخرى لزيادة نفوذها في مناطق تهمّ سياسة الولايات المتحدة من حيث الأمن القوميّ والخارجيّ من أجل فهم التهديد وتقويم أفضل السبل لإحباطه. وعليه، فإنّ هذا التقرير يُعنى أساساً بدراسة كيف يمكن الولايات المتحدة أو أيّ معارض آخر لنشر العملات الافتراضيّة استغلال التحديّات أو زيادتها في وجه نشر العملات الافتراضيّة في العمليّات الشائعة. هذا البحث هو جزء صغير من حوار أكبر بشأن جدوى العملات الافتراضيّة، سواء من منظور العلوم الاجتماعية (أي العملة الافتراضيّة بمثابة عملة) أو من منظور تكنولوجي (أي العملة الافتراضيّة بمثابة خدمة إلكترونيّة آمنة ومرنة ومغفلة).

وسيبحث هذا التقرير في إمكانيّة المجموعات الإجراميّة أو المتمرّدة أو الإرهابيّة زيادة قوّتها السياسيّة و/أو الاقتصاديّة عن طريق نشر عملة افتراضيّة لاستخدامها عملة للعمليّات الاقتصاديّة العاديّة بدلاً من استخدامها وسيلة للتحويل غير المشروع أو لجمع التبرعات أو لتبييض الأموال. وقد اخترنا في المقام الأول البحث في نشر العملة الافتراضيّة بدلاً من البحث في استخدامها وذلك لعدّة أسباب. أولاً، في حين أننا نعلم بوجود دراسات تبحث في استخدام العملات الافتراضيّة لهذه الغاية[2]، قليلة هي الدراسات التي تبحث في

[2] على سبيل المثال، راجع راج ساماني (Raj Samani)، "الجرائم الإلكترونيّة المكشوف عنها: الجرائم الإلكترونيّة بمثابة خدمة"، دراسة الشركة التقنيّة، سانتا كلارا، كاليفورنيا: مختبرات مكافي (McAfee Labs)، 2013a "والتبييض الرقميّ: دراسة تحليليّة عن العملات المتداولة على الإنترنت، وإستخدامها في الجرائم الإلكترونيّة"، دراسة تقنيّة للمؤسّسة، سانتا كلارا، كاليفورنيا: مختبرات مكافي، 2013b؛ وآرون برانتلي (Aaron Brantly)، "تمويل الرهبة رويداً رويداً"، مجلّة سانتينل التي ينشرها مركز مكافحة الإرهاب التابع لأكاديميّة ويست بوينت (CTC Sentinel)، المجلّد رقم 7، العدد رقم 10، تشرين الأوّل 2014، الصفحات 5-1.

استخدام عملة افتراضيّة كبديل كامل للعملة الأصليّة أو غيرها من العملات الشائعة. ثانياً، إنّ دراسة استخدام عملة افتراضيّة في هذا الإطار سوف تزيد أيضاً في فهم موضوع العملة الافتراضيّة بصفة عامة؛ ففي حال قامت جهة غير حكوميّة بنشر عملة افتراضيّة في بلد ما تعارض حكومته الشرعيّة استخدام تلك العملة، ستنشأ جرّاء ذلك مسائل هامة تتعلّق بالأمن والسريّة ومرونة التعرّض للهجمات الإلكترونية. الإجابة على هذه الأسئلة، ولا سيما في الحالة التي يتشكّل فيها تحالف دوليّ من دول قوميّة ذات قدرات ملمّة إلكترونيّاً (مثل الولايات المتحدة) حين يحاول هذا التحالف تعطيل نشر عملة افتراضيّة من قبل جهات غير حكوميّة، مما يعزز فهمنا الحالي لموضوع العملات الافتراضيّة ومن المرجّح أن يكون له ترددات إيجابيّة على تقنيّات أمن الفضاء الإلكترونيّ. أخيراً، تجدر الإشارة إلى أنّ هذا البحث سيساعد على كشف تلك المسائل الرئيسة التي تُمكِّن أو تُعيق من نشر العملة الافتراضيّة بشكل أساسي، تاركة تداعياتها على استخدام العملة الافتراضيّة.

بعد إعطاء خلفيّة عن تطوّر العملات الافتراضيّة وصلتها بالجهات الفاعلة غير الحكوميّة (الفصل الثاني)، يمضي هذا التقرير في مسارين استكشافيين: المسار السياسيّ والاقتصاديّ والمسار التكنولوجيّ. سوف نناقش كيف يمكن أن تسهم العملات الافتراضيّة في إسقاط السلطة السياسيّة (الفصل الثالث). ومن ثمّ نبحث كيف يمكن لجهات فاعلة غير حكوميّة (وبالأخصّ الإرهابيين والمتمردين) نشر عملة افتراضيّة عملياً في البلدان النامية أو المفككة (الفصل الرابع). ونبحث أيضاً كيف يمكن أن تتعطل العملات الافتراضيّة على صعيدي النشر والعمليّات، إما من خلال أفعال متعمَّدة من قبل طرف ثالث أو من خلال إخفاقات في التطبيق.

أخيراً (الفصل الخامس)، نبحث في العملات الافتراضيّة من منظور تكنولوجيّ أوسع: ما هي القدرات التي تصبح متاحة عندما تُستخدم التكنولوجيّات الأساسيّة للعملات الافتراضيّة لأغراض مختلفة تتخطّى كونها عملات تُستخدم في عمليّات اقتصاديّة؟ على وجه الخصوص، نبحث في التداعيات المترتبة على تمكين جهات فاعلة غير ملمّة إلكترونياً من الوصول إلى الخدمات الإلكترونيّة المرنة التي لولا ذلك لكانت متاحة فقط للجهات الفاعلة التي هي على درجة إلمام أعلى بكثير.

منهج

يستند هذا التحليل إلى مراجعة الدراسات السابقة ولقاءات مع خبراء متخصصين في كل من الجوانب الفنيّة وكذلك في استخدام العملات الافتراضيّة. وقد اعتمدنا قدر الإمكان

على الدراسات الأكاديميّة المنشورة والدراسات في السياسات، ودراسات تقنيّة وبيانات من منظّمات أمنيّة قائمة، والوثائق الرسمية لمختلف العملات الافتراضيّة. وقد تجنّبنا المدوّنات الإلكترونيّة ومواقع الإنترنت قدر الإمكان نظراً لضعف موثوقيّتها. ومع ذلك، فإنه ليس من الممكن تجنّبها تماماً، لا سيما في عالم من العملات الافتراضيّة يتغيّر بشكل حيويّ[3].

في هذه الدراسة، نشير إلى خصوم الجهة الفاعلة غير الحكوميّة التي تنشر عملة افتراضيّة بلفظة المعارضين، ويمكن أن ينضمّ إلى هؤلاء المعارضين الدولة أو الدول القوميّة التي جرى فيها نشر العملة الافتراضيّة فضلاً عن حلفاء تلك الدولة القوميّة "الضحيّة" التي قد تمتلك قدرات إلكترونيّة أكثر تقدماً إلى حدّ كبير (مثل الولايات المتحدة).

[3] على وجه الخصوص، نشير إلى مواقع wikis المستخدمة للحصول على معلومات حول العملات الإفتراضيّة في مرّات عدّة، وتحديداً في ما يتعلّق ببتكوين، وذلك لأنّ هذه المواقع هي أفضل المراجع وسيتمّ ضبط هذه المواقع مع الوقت لتوفير الصورة الحاليّة الأكثر دقّة لبيئة العملة الإفتراضيّة التي تتغيّر بشكل دائم. ومن سيّئات هذه المقاربة تعذّر الوصول إلى بعض الإقتباسات بعد وقت من نشر هذا التقرير.

الوضع الراهن للعملات الافتراضيّة

يشكّل هذا الفصل مقدِّمة للعملات الافتراضيّة التي سنبني عليها في بقيّة أجزاء التقرير. لذا قد يكون مهماً بحدّ ذاته على اعتباره مقرَّراً تمهيدياً عن العملات الافتراضيّة للمهتمين من القرّاء. علينا أولاً البحث في التقدم الاقتصاديّ الذي أدّى إلى استخدام العملات الافتراضيّة من أجل فهمها من منظور العلوم الإجتماعيّة. ثم نبحث في أحدث التكنولوجيّات الحاليّة للعملات الافتراضيّة ونقدّم العملات الرئيسة، ومن أبرزها البتكوين. وأخيراً، نلقي الضوء على استخدام جهات فاعلة غير حكوميّة لتلك العملات الافتراضيّة حالياً.

التطوّر نحو العملات الافتراضيّة

نبحث هنا بإيجاز التطور التاريخيّ للعملات، من الذهب وصولاً إلى العملات الافتراضيّة، وذلك للتأكد من أسباب تحفيز استخدام عملات افتراضيّة. وكدافع لهذا التحليل، فإنّ العديد من مستخدمي العملات يفضّلون العمليّات الآمنة والمغفلة. لذا يفضّل جميع المستخدمين عملياً إجراء العمليّات داخل نظام مستقر ومرن وسهل الاستخدام. ظاهرياً، إنّ أيّ عملة افتراضيّة لامركزية مثل البتكوين تبدو بعيدة عن العملات الذهبيّة التي غالباً ما تُستخدم على سبيل المقارنة. لكنّ العملات الافتراضيّة ليس لها مظهر مادي ولا قيمة جوهريّة، وقيمتها غير مدعومة عموماً من أيّة حكومة.

وقد استُخدمت العملات الذهبيّة كمخزن للقيمة ووحدة حساب، ووسيط للتبادل منذ ما لا يقلّ عن 700 عام قبل المسيح[1]. وبصفة الذهب كعملة، فإنّ له الكثير من الخصائص

[1] راجع بيتر ل. بيرنشتاين (Peter L. Bernstein)، قوّة الذهب: تاريخ من الهوس، هوبوكين، نيو جيرسي: شركة وايلي وأولاده، 2004، ص. 24. هذه هي وظائف المال الثلاثة المتعارف عليها. وقد إستخدم الذهب على شكل ألواح بمثابة عملة لفترة طويلة من الزمن.

المرغوبة[2] لا بل هو سلعة ذات قيمة سوقيّة في حدّ ذاتها ومن ذاتها (أي قيمة جوهريّة). على كلٍّ وكما يلاحظ بيتر بيرنشتاين:

> القيمة وحدها غير كافية لتؤهّل مادة ما لتعتبر مالاً. فالكثير من الأشياء لها قيمة ولكن لا تستخدم كالمال. في الواقع، إنّ أشكال المال الأكثر فعاليّة قد تطوَّرت من أشياء كانت عقيمة عديمة الفائدة، مثل الورق والومضات الحاسوبيّة[3].

وخلافاً للوُدَع الذي كان يستخدم كعملة تداول في غرب أفريقيا، بقي الذهب قياساً بغيره لا يُقهر[4]. وكانت إمدادات الذهب في العالم وفيرة بما فيه الكفاية للحفاظ على استخدامها كعملة، ولكن ليست وفيرة بمعنى أن تتآكل قيمتها وذلك على نقيض المعادن الأخرى، مثل البلاتين النادر جداً والألمنيوم الوفير. كما يمكن أن يقسَّم الذهب بسهولة، مما يجعله سهل القياس.

على الرغم من أنّ نقود الذهب والفضّة يمكن أن تصدر من قبل الحكومة، فإنّ قيمتها تكمن في المقام الأول في الوزن والنقاء. ونتيجة لذلك، فإنّ إنفاذ قيمة عملة معتمدة على سلعة أساسيّة لا يتطلّب بالضرورة تدخّل السلطة المركزيّة. إنّ العملات القائمة على السلع الأساسيّة هي أيضاً مغفلة إلى حدّ كبير ولا يوجد سجلّ في صلب أيّ من العمليّات التي تُستخدم فيها العملة يساعد على تعقُّب المستخدمين أو الاستخدامات. ورغم أنّ معظم العملات القائمة على السلع الأساسيّة قد حافظت على قِيَم مستقرّة على مرّ الزمن، فهي كانت عرضة لتقلّبات في القيمة تتخطّى سيطرة أيّ من السلطات النقديّة، ذلك أنّ أساس قيمة العملة يعكس العرض والطلب على السلعة. وعلى سبيل المثال، فإنّ قيمة الفضّة مقابل الذهب قد انخفضت بمقدار النصف حوالى العام 1870، إذ إنّ اكتشافات الفضّة في المكسيك، وكذلك إنخفاض الطلب على الفضّة لاستخدامه كعملة في أوروبا، زادت من حجم العرض على الفضّة وخفَّضت الطلب بصورة أساسيّة[5]. بالإضافة إلى نقاط

---

[2] للفضّة خصائص مماثلة. ولتبسيط الأمور، نركّز على الذهب في هذه المناقشة.

[3] بيرنشتاين (Bernstein)، 2004.

[4] راجع ماريون جونسون (Marion Johnson)، "عملات أصداف الودع الخاصّة بأفريقيا الغربيّة، الجزء الأوّل"، مجلّة التاريخ الأفريقيّ، المجلّد رقم 11، العدد رقم 1، 1970، الصفحات 17 إلى 49.

[5] جفري أ. فرايدن (Jeffry A. Frieden)، الرأسمالية العالميّة: سقوطها ونهضتها في القرن العشرين، نيويورك: شركة دبليو دبليو نورتون أند كومباني (W. W. Norton and Company)، 2006.

ضعف العملات القائمة على السلع الأساسيّة في مقابل عدم إستقرار القيمة، فإنه يَصعُب استخدامها لأي شيء أكثر من عمليّات صغيرة محليّة، لأنّ نقلها غير ملائم ماديّاً في الحجم والمسافة.

وعلى مرّ الزمن، حولّت معظم الدول عملاتها من تلك القائمة على السلع الأساسيّة إلى العملات الورقيّة. وهذه العملات هي عملات رسميّة صادرة عن السلطة المركزيّة بمرسوم لتكون عملات قانونيّة ليس لها أيّ قيمة ذاتيّة، وتكون فقط قابلة للتحويل إلى سلعة مثل الذهب وفقاً لتقدير السلطة المركزيّة[6]. وبالنتيجة، فإنّ قيمة العملات الورقيّة ترتكز على ثقة مستخدميها بأن السلطة المركزيّة ستكون قادرة على الحفاظ على قيمة العملة. والجدير بالذكر أنّ العملات الورقيّة تمتاز بمزايا رئيسة على العملات القائمة على السلع الأساسيّة. فهي أخفّ وزناً وأسهل للاستخدام، على الرغم من أنّه لا يزال من الصعب نقلها (التعامل بها) عبر المسافات، وهي كذلك توفّر المزيد من النفوذ للحكومات للسيطرة على السياسة النقديّة والماليّة. وعلى غرار العملات القائمة على السلع الأساسيّة، يمكن للعملات الورقيّة توفير عمليّات أكثر مجهولية. إلّا أنّ العملات الورقيّة تعتمد اعتماداً كبيراً على السلطة المركزيّة من أجل الحفاظ على قيمتها، أما استقرار العملات الورقيّة فيعتمد على سياسات الاقتصاد الكليّ للحكومات وقد يواجه تقلّبات كبيرة، حتى تفقد العملة الورقيّة قيمتها كليّاً (على سبيل المثال، خلال فترات التضخم الجامح).

وقد سمحت الإبتكارات الماليّة للناس إجراء عمليّات اقتصاديّة تتخطّى القيود التي تفرضها العملة الماديّة، فظهرت الكمبيالات أثناء المعارض التجاريّة الأوروبيّة الكبيرة التي أُقيمت في خلال مئوية العام 1200 لتسهيل التجارة دون الحاجة لشحن كميّات كبيرة من

---

[6] لا يناقش هذا التطوّر المبسّط جّداً للنظم النقديّة البدائل للأنظمة النقديّة الإقليمية. لإجراء مناقشات أكثر تفصيلاً، راجع بنيامين كوهين (Benjamin J. Cohen)، جغرافيا المال، إيثاكا، نيويورك: مطبعة جامعة كورنيل، 1998؛ غلين دايفيز (Glyn Davies)، تاريخ النقد: من العصور القديمة إلى يومنا هذا، شيكاغو: دار نشر جامعة شيكاغو، 2005؛ إريك هيلينر (Eric Helleiner)، "صنع النقد الوطنيّ: العملات الإقليميّة من منظور تاريخيّ، إثاكا، نيويورك: دار نشر جامعة كورنل، 2003؛ وجاك ماكايفر واثرفورد (Jack Mclver Weatherford)، تاريخ النقد، نيويورك: كراون للنشر، 1997. الخطوة الهامّة التي ربطت بين نظام النقد الحاليّ والنظام الذي كان مطّبقاً بعد الحرب العالميّة الثانية والقائم على السلع الأساسيّة هي ما كان يعرف بنظام بريتون وودز النقديّ (1971–1944)، حيث كان الدولار الأمريكيّ مدعوماً من احتياطيّ الذهب، وارتبطت العملات الأخرى للبلدان المتقدّمة بالدولار، في حين ارتبطت عملات الدول النامية بسلّة عملات البلدان المتقدّمة (فريدن، 2006).

[7] راجع شارلز كيندلبرغر (Charles Kindleberger)، تاريخ أوروبا الغربيّة الماليّ، أوكسفورد: دار نشر جامعة أوكسفورد، 1993.

الذهب من مدينة إلى أخرى ومن بلد إلى آخر[7]. لقد تمّ إصدار هذه الكمبيالات بحسب عملات الدول على غرار النموذج الحديث لكتابة شيك مقابل رصيد ماليّ في حساب جار. لقد أتاح وجود المزيد من الإبتكارات التكنولوجيّة الحديثة للمستخدمين الإبتعاد عن نُظُم الصرف الورقيّة (كالشيكات) والتوجّه إلى الأنظمة الإلكترونيّة (كبطاقات الدفع الآلي التي تُمسح بواسطة قارئ بطاقات عند نقطة بيع) واستخدام تكنولوجيا الإتصال ذات المجال القريب (NFC) للسماح بالإتصالات اللاسلكيّة من خلال منصّات الحوسبة المحمولة (كالتطبيقات على الهواتف الذكيّة)[8]. فكما هو الحال مع كمبيالات القرن الثالث عشر، هذه الإبتكارات هي آليات ملائمة تسمح للمستخدمين باستخدام العملات التقليديّة بفاعليّة أكبر إذ إنّها لا تشكّل عملات جديدة على عكس العملات الافتراضيّة.

والجدير بالذكر أنّ العملات الافتراضيّة أصبحت شائعة وبشكل متزايد في السنوات الأخيرة، ولكن حتى الآن، هذه العملات الافتراضيّة لم تتحول بعد إلى عملات ورقيّة ولم تعتمد أيّ حكومة بعد أيّاً من العملات الافتراضيّة كعملة رسميّة، ومع ذلك فهي تمثّل قيمة لمجتمع معيّن يستخدمها وسيلة للتبادل. لقد استخدمت العملات الافتراضيّة في مجتمعات الألعاب عبر الإنترنت وبرامج التقديمات مثل برامج أميال المسافر الدائم أو نقاط السفر المتكرِّر، وذلك لتعقّب أرصدة العضويّة القابلة للإسترداد الذي بدونه لا يوجد قيمة لها مقارنة بالعملة الورقيّة[9]. إن العملات الافتراضيّة كالأموال المستخدمة في الألعاب عبر الإنترنت أو أميال السفر المتكرِّر، تمّ تصميمها لتكون بمثابة مخزن للقيمة ووحدة حساب ووسيط للصرف داخل مجتمع من ذوي ذات الإهتمام. إلاّ أنّ هذا المجتمع لا يشغل بالضرورة وحدة جغرافيَّة أو سياسيَّة واحدة.

إذ إنّ بعض أحدث العملات الافتراضيّة مثل البتكوين يختلف عن العملات الافتراضيّة السابقة من حيث أنّه مصمَّم صراحة ليُستخدم عملة في الاقتصاد الحقيقيّ وهو قابل للصرف مقابل العملات الورقيّة الصادرة عن الحكومة. وبالعودة إلى المقارنة مع العملات الذهبيّة، فإن البتكوين يشارك الذهب في العديد من خصائصه، وهناك كميّة محدودة من العملة في التداول. على غرار سلعة مثل الذهب، فإن سعر صرف البتكوين يمكن أن يكون متقلِّباً. إن البتكوين قابلة للقياس والقسمة بسهولة، لكن على نقيض الذهب،

---

[8] هذه هي تطبيقات التكنولوجيا الأساسيّة، مثل محفظة غوغل (Google Wallet) وخدمة آبل للدفع الإلكترونيّ (Apple Pay) وفنمو (Venmo).

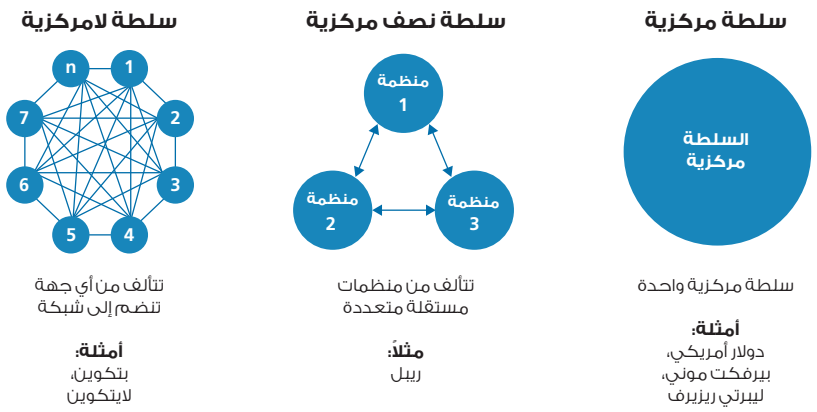
[9] قد تتطوّر المبادلات بحيث تسمح للمستخدمين بصرف عملات إفتراضيّة بعملات ورقيّة، ولكنّ ذلك لا يشكّل ميزةً للعملات الإفتراضيّة ولا مطلباً خاصّاً بها.

فهي قابلة للنقل بسهولة ولا تحتاج إلى عبور الحدود الدوليّة كعملة ممّا قد يزيد في سهولة استخدامها ويقلّل تكاليف العمليّات عبر الحدود (إضافةً إلى أنّها تشكّل تحدّياً لإنفاذ القانون والجهود الاستخباريّة). وأخيراً، لا تعتمد البتكوين على وجود سلطة مركزيّة لحماية قيمتها.

ولعلّ أهمّ فرق بين البتكوين والعملات الافتراضيّة السابقة هو أنّه في حين لا تتطلّب العملات الافتراضيّة من الناحية الفنيّة أيّ سلطة مركزيّة، فإنّ واحدة من السِمات الرئيسة للبتكوين هي السلطة اللامركزية التامّة وقد اتبعت عملات افتراضيّة عديدة البتكوين في هذا الإتجاه تحديداً. ونتيجة لذلك، لا يمكن أن تبني العملات الافتراضيّة مثل البتكوين الثقة في استقرار عملتها إستناداً إلى سياسات سلطة مركزيّة وقدراتها. لا بل تعتمد على ثقة المستخدمين في العملات الافتراضيّة وعلى ثقتهم في الآليات اللامركزيّة التي تدعم العملة الافتراضيّة وتضمن أمنها. وتجدر الإشارة إلى أنّ العملات الافتراضيّة الحاليّة لديها هيكليّة سلطويّة تتراوح بين مركزيّة تامّة ولامركزيّة تامّة (راجع الشكل 1–2).

بعد أن تمَّ البحث في التطوّر نحو العملات الافتراضيّة من منظور نقديّ، سوف نقوم الآن ببحث تطوّر العملات الافتراضيّة نفسها من منظور تكنولوجيّ.

الشكل 1–2
العملات الافتراضيّة تتمتّع بهياكل سلطة متنوّعة



أصول وإتجاهات العملات الافتراضيّة

إنّ التقدم المرحلي الأول نحو العملات الافتراضيّة قد أُحرِز من قبل باحث التشفير دايفيد تشوم (David Chaum) الذي استخدم عملات رمزيّة مشفّرة[10]. أعطى هذا التقدّم، كما المقترحات اللاحقة ذات الصلة، إهتماماً كبيراً للعملات المغفلة غير القابلة للتعقّب والصادرة مركزيّاً ومدعومة من قبل مصارف أو مؤسسات أخرى (قد تتمتع بقدر معيّن من الثقة من قبل المستخدمين). وقد قامت شركة النقد الرقمي ديجيكاش (Digicash) التي أسسها تشوم بإدارة فترة تجريبيّة من ثلاث سنوات فقط وفي مصرف واحد، ولكن لم تتمّ متابعتها لاحقاً[11].

الأنظمة الأولى

وُضِعَت العملات الافتراضيّة قيد التداول قبل اختراع نظام بتكوين بوقت طويل على الرغم من أنّ تلك العملات لم تكن لا مركزيّة. تجدر الإشارة إلى أنّ عملات ذهبيّة رقميّة ونظماً مماثلة شملت الموجة الأولى من العملات الافتراضيّة التي تمّ خلقها واستخدامها. والجدير بالذكر أنّ الإتجار الإلكترونيّ بالذهب بدأ في العام 1996 كتمهيد لنوع من النظام المقترح من قبل تشوم حيث تمّ استخدام هيكليّة حساب مركزيّ لتتبع ونقل شهادات مدعومة بالذهب في مستودع مركزيّ دون وجود ضمان الأمن والتشفير والمجهولية، بوصفها عمليّة ثقة في القيّمين على تشغيل نظام الإتجار الإلكترونيّ بالذهب[12]. ولكن بما أنّ الإتجار الإلكترونيّ بالذهب كان خارج النظام الرقابيّ الماليّ، فقد أتاح توفير الأمن والمجهولية الفعليّين من

---

[10] راجع دايفد شوم (David Chaum)، "تواقيع عمياء لدفعات غير قابلة للتعقّب"، في طبعات دايفد شوم، رونالد ل. ريفست (Ronald L. Rivest)، وألان ت. شيرمان (Alan T. Sherman)، أوجه التقدّم في علم التشفير CRYPTO 2013: المؤتمر السنوي الثالث والثلاثين لعلم التشفير، سانتا باربرا، كاليفورنيا، آب 2013، الصفحات 90 إلى 108.

[11] راجع دايفد شوم (David Chaum)، أموس فيات (Amos Fiat) وموني ناور (Moni Naor)، "نقود إلكترونيّة غير قابلة للتعقّب"، في طبعة شافي غولدفاسر، "النقد الإلكترونيّ غير القابل للتعقّب"، في طبعة شافي غولدواسر، نتائج مؤتمر Crypto لعام 1988، برلين: سبرينغر–فيرلاغ، 1990، الصفحات 319 إلى 327، وجولي بيتا (Julie Pitta)، "وداعاً للفكرة اللامعة"، صحيفة فوربس الإلكترونيّة، 1 تشرين الثاني 1999.

[12] دوغ جاكسون (Doug Jackson)، قال مؤسّس الذهب الإلكترونيّ: "من الناحية العمليّة، كان الذهب الإلكترونيّ نقيض الغفليّة"، كما إقتُبِسَت في كيفن داود (Kevin Dowd)، "الأنظمة النقديّة الخاصّة المعاصرة"، دراسة من نشر المؤلّف، آب 2013. كان التشفير يستخدم في الإتّصالات، لكنّه لم يكن سمة أصيلة للعملة.

خلال الثقة المضمونة في ممارسات عمل الشركات التي تقوم بتشغيل هذه النُظُم. بالإضافة إلى ذلك، فإن نظم مماثلة، مثل نظام تأمين إرسال الدفعات الماليّة واستقبالها (Liberty Reserve) ونظام الدفع عبر الإنترنت (WebMoney) وجيل جديد من نظام دفع الأموال وتحويلها (Perfect Money) كانت هدفاً متكرراً للأنشطة غير المشروعة، سواء من قبل مستخدمين يستغلّون المجهولية والسهولة النسبيّة للتحويل التي تتخطّى سيطرة المنظِّمين أو من قبل المشغلِّين القيِّمين على إدارة مخططات بونزي (Ponzi) وغيرها من المشاريع الإحتياليّة[13]. وتتميّز جميع هذه النظم بهيكليّتها ذات السلطة المركزيّة، إذ من أجل دعم الأنشطة غير المشروعة، يجب على الجهات الفاعلة أن تثق بأصحاب العملة في الحفاظ على الأمن والمجهولية وهو أمر امتاز به بعض من هذه العملات تاريخيّاً.

بتكوين

كان الإهتمام الرئيس في ما يتعلّق بالعملات الافتراضيّة في مجتمع الأمن القوميّ منصبّاً على العملة الرقميّة الإلكترونيّة أو البتكوين، ولا سيما في ما يتعلّق بالاستخدام الواسع لهذه العملة مع ما تضمنه من أمن ومجهولية. جرى إدخال نظام بتكوين في العام 2009 وهو موجود خارج سيطرة حكومة أو شركة واحدة. فهو خاضع لتعريف وسيطرة مجموعة لامركزيّة من المستخدمين ينفّذون بروتوكول بتكوين عبر الإنترنت كما هو موضح أدناه[14].

إعتباراً من شهر حزيران من العام 2015، جرى تداول حوالى 14.2 مليون بتكوين، وقد بلغ إجمالي القيمة السوقية 3.5 مليار دولار أمريكيّ (بمعدل صرف حوالى 240

---

[13] راجع داود، 2013.

[14] راجع ناكاموتو (Nakamoto)، 2008. تشير عملة بتكوين إلى نوعٍ جديدٍ من الخوارزميّة لدفتر حسابات عام آمن يدعى سلسلة الكتل، وإلى نقود تدعى بتكوين، تُراقب بواسطة دفتر الحسابات وتُستخدم بمثابة عملة. من أجل مراجعة متعمّقة وممتازة للبتكوين والعملات الإفتراضيّة ذات الصلة، والدراسات الأكاديميّة التي تبحث فيها، راجع جوزيف بونو (Joseph Bonneau) وأندرو ميلر (Andrew Miller) وجيريمي كلارك (Jeremy Clark) وأرفيند نارايانان (Arvind Narayanan) وجوشوا أ. كرول (Joshua A. Kroll)، وإدوارد فلتن (Edward W. Felten)، "آفاق البحث عن البتكوين والجيل الثاني من العملات المشفّرة"، نتائج ندوة الأمن والخصوصيّة على الإنترنت لعام 2015 التي نظّمتها جمعيّة مهندسي الكهرباء والإلكترونيّات، سان خوسيه، كاليفورنيا: جمعيّة مهندسي الكهرباء والإلكترونيّات، أيّار 2015. للحصول على مقدّمة أكثر توجّهاً نحو السياسات، راجع أدوارد ف. مورفي (Edward V. Murphy) وم. مورين مورفي (M. Maureen Murphy) ومايكل ف. سايتزنغر (Michael V. Seitzinger)، بتكوين: أسئلة وأجوبة وتحليل المسائل القانونيّة، واشنطن: دائرة الأبحاث التابعة لمكتبة الكونغرس، 14 آب 2015.

دولاراً أمريكيّاً لكل بتكوين أي أقل من أعلى قيمة سوقيّة لما يقرب من 14 مليار دولار أمريكيّ في آذار من العام 2013 (بمعدل 1,150 دولاراً أمريكيّاً لكل بتكوين). كذلك حاليّاً يتمّ تنفيذ أكثر من 110,000 عمليّة بتكوين يوميّاً، مع زيادة خطيّة تقريبيّة في العمليّات من شهر حزيران 2012، إذ إنّ عند هذه النقطة أُحصي تنفيذ نحو 20,000 عمليّة في اليوم[15].

إنّ الميزة التكنولوجيّة المركزيّة لبتكوين هي دفتر حسابات عام عالميّ يحتوي على جميع عمليّات بتكوين التي تمّ تنفيذها بالكامل. ويضمّ دفتر الحسابات هذا سلسلة مما يسمى كتلاً. وتحتوي كل كتلة على قائمة من العمليّات، فضلاً عن الهاش، أو التوقيع الرقمي للكتلة السابقة المكوّنة لدفتر الحسابات (من هنا جاء مصطلح سلسلة الكتل)، إذ إنّه يتمّ ربط كل كتلة بسابقتها كما يتمّ توزيع سلسلة الكتل على كل الحواسيب التي تشغّل بروتوكول بتكوين. بالتالي، تحوي جميع العقد في شبكة بتكوين نسخاً من كل العمليّات المنفَّذة بالكامل. ويثبت المشاركون بالتكافل صحة العمليّات الجديدة كتلة بكتلة. من ناحية أكثر تقنيّة، تعتبر هذه العملية بروتوكول إجماع لامركزي، بحيث أن الإجماع هو على إدراج أو عدم إدراج كتلة جديدة في سلسلة الكتل.

إنّ الهويات في بروتوكول بتكوين هي عناوين تُوَلّد بشكل مشفَّر. وبشكل أعمّ، فإنّ كلّ عمليّة هي أمر نقل من عنوان إلى آخر[16]. ويشكّل دفتر الحسابات التاريخ المسجَّل لكل من هذه العمليّات ويسمح بمعالجة أيّ عمليّة جديدة إذا أظهر دفتر الحسابات أنّ عنوان المُرسِل لديه ما يكفي من رصيد لنقل المبلغ المقترح إلى عنوان المتلقّي. وبناء عليه، يتمّ تضمين الرصيد الجديد علناً في دفتر الحسابات عن طريق تقديم العمليّة وإدراجها في سلسلة الكتل بصفتها دفتر الحسابات لضمان تنفيذ جميع العمليّات المستقبليّة. وفقاً لذلك، فإن عدد بتكوين التي يملكها المستخدم هو تحديداً العدد الإجمالي لبتكوين المرتبط بالعنوان أو العناوين التي يمتلك المستخدم حق الوصول إليها، لذا فإنّ السبب في أنّ بتكوين تُعتَبر "مُغْفَلَة" هو أنّ المجهولية لامتلاك بتكوين تُصان من خلال عدم القدرة على ربط العنوان بمستخدم محدّد.

---

[15] راجع موقع Blockchain الإلكترونيّ، "رسملة الأسواق"، غير مؤرخ (b). تجدر الإشارة إلى أنّ البيانات المقدّمة هنا قد تتغيّر إلى حدٍّ كبير. وبالإضافة إلى ذلك، فإنّه من الصعب تقدير نسبة العمليّات المشروعة مقابل تلك التي نفّذت لأغراض جرمية.

[16] وبشكل أكثر شموليّة، يمكن أن تتمّ عمليّة واحدة من عنوان واحد على الأقلّ إلى عنوانٍ واحدٍ آخر على الأقلّ.

والجدير بالذكر أنّ المستخدم لا يمتلك البتكوين. إنما له الحق في صرف عدد من البتكوين التي ترتبط بعناوين مختلفة يقدر الوصول إليها. وفقاً لذلك، فإن محفظة من البتكوين هي في الواقع المعلومات المطلوبة التي تثبت ملكيّة عنوان متعلّق بالبتكوين والذي بدوره يسمح للمستخدم بصرف البتكوين المرتبطة بذلك العنوان. وعلى وجه التحديد، تقوم هذه العناوين على أساس مفتاح مزدوج عامّ/ خاصّ يولّد بشكل مشفَّر، فالمفتاح الخاصّ يسمح بإنفاق النقود في عمليّة جديدة. إذ إنّه نظريّاً يشبه الموضوع وجود عنوان مع صندوق بريد حيث يمكن لأيّ شخص تسليم البريد، ولكن وحده الشخص الذي يملك المفتاح يستطيع أن يخرج الرسائل من الصندوق ويرسلها إلى عنوان جديد، وبالتالي نقلها أو صرفها. وفي هذه الحالة، ليس بالضرورة لأحد أن يعرف من الذي لديه المفتاح، وعلب البريد موجودة في سلسلة الكتل.

إنَّ مجهولية مستخدمي بتكوين، أو عدمها، هو عنصر حاسم للعملة؛ وفي هذا الصدد، راجع المناقشة عن سريّة ومجهولية مستخدمي العملة الافتراضيّة في الفصل الرابع من أجل مناقشة مفصّلة لهذه المسألة، مع التركيز بشكل خاصّ على البتكوين.

ويتمّ التحقق من صحّة كتل سجلاّت العمليّات الصحيحة من خلال توظيف قوّة حوسبة هامة، وذلك من خلال عمليّة تسمّى التنقيب، وهي عمليّة إضافة سجلاّت العمليّات إلى كتل العمليّات السابقة، وأولئك الذين يقومون بعمليّات الحوسبة يُسمّون المنقّبين[17]. أمّا عملية التنقيب عن كتل سجلاّت العمليّات فتتمّ بنجاح عندما يعثر المنقّب على المدخل الصحيح إلى عمليّة رياضيّة معقَّدة تسمى دالَّة الهاش (hash function) التي تربط بشكل فعّال محفظة سجلاّت العمليّات التي تمَّ التحقُّق من صحّتها بكتل العمليّات السابقة. تتميّز سمات بنية بتكوين التحتيّة بسمة محددة هي أنّه من الصعب للغاية حسابيّاً تغيير كتل سجلاّت العمليّات التي تمَّ التحقق من صحتها حديثاً في حال إرتبطت بسلسلة العمليّات أخرى، وبالتالي لا يمكن إحداث تغييرات على تاريخ العمليّات. ولكي يجد المنقّب المدخل الصحيح لدالَّة الهاش، عليه أن يخمِّن بفعالية المدخل عشوائياً، وذلك لأنّ العثور على مدخل بأيّ طريقة أخرى لا يمكن تحقيقه حاسوبياً نظراً للضمانات الأمنيّة لدالّة

[17] تتمّ عمليَّة التحقُّق عن طريق التأكُّد ممّا إذا كان هاش العمليّات، بالإضافة إلى قيمة خاصّة ذات استعمال واحد، مطابق لصيغة محدَّدة. إنّ وظيفة الهاش هي حسابيّاً مكلفة للتشغيل، ولأي مجموعة محدَّدة من العمليّات بالإضافة إلى قيمة خاصّة ذات استعمال واحد تتضمَّن نسبة منخفضة جداً من إحتمال مطابقتها مع الصيغة أو الشكل. ولذلك، حاول المنقّبون تجربة قيم متعدِّدة ومختلفة خاصّة ذات استعمال واحد على أمل العثور على واحدة من شأنها أن تؤكِّد صحَّة الكتلة.

الهاش. عمليّاً، تتمّ هذه التخمينات من خلال تسخير عدّة آلاف من المُعالِجات الحاسوبيّة، ويتمّ بعد ذلك نشر التخمين الصحيح وتوفير ما يسمى إثبات العمل، لأنّه يثبت أنّ المنقّب قد عمل بجدّ للعثور على المدخل الصحيح (لأنّ العثور على المدخل المطلوب تطلبَّ عملاً حسابياً كبيراً). أمّا المستخدمون الآخرون، فيمكنهم التحقُّق بسهولة من صحّة أنّ المنقّب قد وجد المدخل الصحيح للتحقُّق من صحّة كتلة العمليّات، وبمجرّد التحقُّق منها، يُمنح المنقّب مكافأة من بتكوين (عمليّاً، يتمّ تضمين صفقة المكافأة هذه في محفظة العمليّات التي تحقق منها المنقّب)[18]. وتبعاً لذلك، فإنّ الطريقة الوحيدة للحصول على عملات بتكوين جديدة هي إمَّا بطريقة التنقيب عنها أو إجراء صفقة مع مستخدم آخر كان يملك البتكوين كما هو الحال مع خدمة التحويل عبر الإنترنت لتحويل العملة المدعومة من الحكومة إلى بتكوين[19].

تتطلّب اللاّمركزية والبنية التحتيّة القائمة على التنقيب عن بتكوين بأن يقوم الكثير من المستخدمين بتكريس موارد مهمّة من أجل الحفاظ على النظام العام وتأمينه. وعليه، فإنّ قدرة المستخدمين على التعامل ببتكوين تعتمد على قدرة النظام اللاّمركزي على إضافة كتل عمليّات جديدة إلى سلسلة كتل العمليّات السابقة بثبات وأمان، وبالتالي التحقُّق من صحَّة العمليّات الفرديّة. وفي الوقت عينه، فإنّ عمليّة التنقيب أصبحت أكثر تركيزاً حسابيّاً لأنَ الصعوبة الحسابيّة للتنقيب عن بتكوين قد صمّمت لكي تزيد مع المنقّبين. أمَّا اليوم، ولكي يكون لدينا فرصة جادة في التنقيب بنجاح، فنحتاج إلى أجهزة لأغراض خاصّة مطورَّة تحديداً للتنقيب عن بتكوين[20].

---

[18] في الواقع، إنَّ المنقّب عن العملة الذي يؤكِّد بنجاح صحَّة كتلة بتكوين يحصل على عملات بتكوين من جهتين، واحدة بمثابة مكافأة عن عمليَّة التنقيب كما تم وصفها أعلاه، والأخرى عن طريق ما يسمَّى برسوم العمليّات والتي يمكن تضمينها في كلّ عمليّة من عمليّات بتكوين. والجدير بالذكر أنّ عدد عملات البتكوين التي تمَّ الحصول عليها عن طريق مكافآت التنقيب قد تمَّ تصميمها لكي تنخفض مع مرور الوقت لتصل إلى الصفر حوالى سنة 2140؛ وتقضي النظريَّة بأنَّ رسوم العمليّات ستزداد في المقابل للحفاظ على التحفيز الإقتصاديّ للتنقيب، ما يؤمّن نظام بتكوين.

[19] تجدر الإشارة إلى أنَّ هذا هو وصفٌ ذو مستوى عالٍ للبتكوين. ويمكن للقارئ المهتمّ أن يستشير مصادر أخرى للحصول على وصف أكثر تفصيلاً. راجع، على سبيل المثال، موقع Bitcoin Help الإلكترونيّ، الصفحة الرئيسة، غير مؤرّخ؛ وراجع أيضاً موقع Bitcoin Wiki الإلكترونيّ، الصفحة الرئيسة، 13 آب 2015b.

[20] للمزيد من المناقشة، راجع مايكل بدفورد تيلور، "بتكوين وعصر السيليكون المكيّف حسب الطلب"، دراسة قدّمت للمؤتمر الدوليّ حول المجمّعين والهندسة والتلخيص للأنظمة المدمجة (CASES)، مونتريال، كيبيك، من 29 أيلول إلى 4 تشرين الأوّل 2013.

يحتوي الفصل الرابع على مناقشات إضافيّة حول نظام بتكوين، بما في ذلك إجراء فحص للأمن ومجهولية بتكوين، فضلاً عن مناقشة كيفيّة استخدام بتكوين والعملات الافتراضيّة ذات الصلة في العمليّات المشتركة على الأجهزة كالهواتف الذكيّة مثلاً.

العملات الافتراضية بعد بتكوين: ألتكوين (Altcoins)

إنّ بتكوين ليست العملة الافتراضيّة الوحيدة التي يمكن أن تختارها جهة فاعلة غير حكوميّة أو تبني عليها لنشر العملة الافتراضيّة الخاصّة بها، إذ إنّ العديد من العملات الأخرى قد استندت إلى الأفكار التأسيسيّة لبتكوين بحيث يمكن لجهة فاعلة غير حكوميّة أن تستعملها.

وعقب صدور بتكوين واعتمادها الواسع النطاق والإهتمام بها، أُطلق الكثير من المشاريع الجديدة التي وردت مجموعة مختارة منها في الجدول رقم 1–1 وتستند هذه المجموعة إمّا على الهندسة أو، في معظم الحالات، على تكرار شبه تامّ من شِفْرَة المصدر من البتكوين. ونظراً إلى أنّ سلسلة الكتل هي ذات خاصّيّة نوعيّة محدّدة بالنسبة إلى شبكة البتكوين، استخدمت عملة ألتكوين سلاسل كتل جديدة، مع تعديلات مختلفة على البروتوكول. وتجدر الإشارة إلى أنّ معظم تلك التعديلات كانت فعليّاً من مخططات بونزي (Ponzi) والتي استخدمها مبتكرو العملات في الإحتيال المالي (بطرحها وسحبها السريع من السوق للتلاعب بسعرها الفعليّ)، أو بطرق أخرى لم يقصد بها قط استخدامها كعملة شرعيّة[21].

نسلِّط الضوء على ثلاث فئات من بدائل البتكوين كعملات جديرة بالذكر. فالبديل الأول هو عملة ألتكوين البحتة التي ابتُكِرَت بتعديل التفاصيل الماليّة والتشفيريّة للبتكوين. وقد شمل هذا انتاج نقود بشكل أسرع أو استخدام دلالات الهاش (hash functions)

[21] تمّ إطلاق النقود على سبيل الفكاهة (مثلاً دوجكوين، بيتزاكوين، بيركوين) أو بمثابة إثباتاتٍ للمفاهيم وتمارين تعليميّة (مثلاً غايستغيلد (GeistGeld)، تنبريكس (Tenebrix). وفي حالة واحدة – هي الليكويدكوين (Liquidcoin) – تمّ الإعلان بصراحة أنّها "مبنيّة على المضاربة" (راجع منتدى بتكوين، [نشر] شركة ليكويدكوين (المستندة إلى التخمين)"، خطّ نقاش بدأ في 18 كانون الثاني 2012). في حالة الدوجكوين، لم تعد العملة الهزليّة تعتبر مزحة مع رسملة أسواق تبلغ 13,874,871 دولاراً أمريكيّاً إبتداءً من 24 شباط 2015 (راجع موقع Bitcoin Wiki الإلكتروني، "مقارنة العملات المشفّرة"، 24 كانون الأوّل 2014، وموقع CoinMarketCap الإلكترونيّ، "رسملة سوق العملات المشفّرة"، 30 أيلول 2015a).

الجدول رقم 1.1

وعن تطبيقات سلسلة الكتل (Appcoins) أمثلة عن عملات رمزيّة رقميّة تطبيقيّة أبكوينز

الأمثلة	تاريخ الإدخال	التطبيق
عملة نايم كوين[a]	نيسان 2011	تخزين نظام أسماء النطاقات في سلسلة الكتل
عملة ماستر كوين[b]	كانون الثاني 2012	سوق مخطّطة، إتصالات ذكيّة
عملة نكست كوين[c]	تشرين الثاني 2013	تبادل الأصول
عملة ريبل[d]	كانون الأول 2012	العمليات داخل المصرف
عملة مايد سايف كوين[e]	نيسان 2014	حوسبة سحابيّة آمنة ومغفلة (ما عدا سلسلة الكتل)

[a] نايم كوين، صفحة موقع نايم كوين الرئيسة، غير مؤرّخ.

[b] راجع ج. ر. ويلت، الدراسة التقنية الثانية حول البتكوين، النسخة 0.5 (مسوّدة لتعليقات العموم)، بحث من نشر المؤلف، غير مؤرخ. يراجع أيضاً غيتهاب،"تحديد بروتوكول أومني"،(ماستر كوين سابقاً)، غير مؤرّخ.

[c] موقع نكست ويكي الإلكترونيّ، دراسة تقنية من إعداد نكست"، معدّلة في 13 تموز 2014.

[d] راجع موقع ريبل الإلكترونيّ، "فقرة الأسئلة المتكررة"، غير مؤرخ.

[e] لا تزال الشبكة قيد الإختبار، إعتباراً من شهر شباط 2015.

من أجل التحقّق من صحّة سلسلة الكتل[22]. ومع ذلك عملت فئات أُخرى من النقود على تغيير طريقة التحقق بشكل جذريّ، وذلك باستبدال طرق إثبات العمل بخطط أُخرى[23]. ومن عملات ألتكوين البارزة عملة لايتكوين[24] (Litecoin) وهي أسرع من البتكوين في عملية

[22] تمّ إقتراح مجموعةٍ متنوّعةٍ من وظائف الهاش ومجموعات من وظائف الهاش وهي تتمحور بشكلٍ أساسيٍّ حول قلق مركزيّة سلطة التنقيب بسبب تطبيق التنقيب المستند إلى الدوائر المتكاملة (ASIC). وكذلك، فقد تمّ إنشاء خطط بديلة، من مثل إثبات صحة ملكيّة الرصيد، أو حوسبة سلاسل كانينغهام في برايمكوين. لهذه الخطط إيجابيّاتٌ وسلبيّات، ولكنّ التفاصيل ليست متّصلة بالإجمال بما يلي مناقشته.

[23] للحصول على قائمة من هذه العملات، راجع موقع Altcoins الإلكترونيّ، الصفحة الرئيسة، غير مؤرّخة. راجع أيضاً موقع Bitcoin Wiki الإلكترونيّ، "مقارنة العملات المشفّرة"، 24 كانون الأوّل 2014.

[24] موقع Litecoin الإلكترونيّ، الصفحة الرئيسة، غير مؤرّخ.

دلالة الهاش (hashing process). وكذلك ظهرت عملة دوغيكوين (Dogecoin)، التي بدأت بدعابة إذ لم يكن من المفترض أن تُؤخَذ على محمل الجدّ، ومن ثم أصبحت تدريجيّاً أكثر قبولاً. وبموازاة ذلك أُدخِلت عملة رقمية أُخرى تدعى بيركوين(Peercoin) وهي تستخدم نهجاً هجيناً للتنقيب بوصفه بديلاً عن نظام إثبات صحة العمل العائد للبتكوين[25].

أما الفئة الثانية، والتي سندعوها نقود مُغفَلة، فقد استخدمت تقنيّات تشفير جديدة أو بروتوكول لخلق مجهولية أكبر مما تقدّمه البتكوين. وهذا إما تمّ في شكل ألتكوين تسمح أو تفرض مستوى من المجهولية في البروتوكول أو في إضافات البتكوين باستخدام تقنيّة تسمّى كوين جوين (CoinJoin). ولهذا يجب مراجعة موضوع المناقشة في الفصل الرابع عن مجهولية العملة الافتراضيّة لمزيد من المعلومات حول النقود المغفلة.

وفي الآونة الأخيرة، تركزت معظم الجهود الجديدة على الفئة الثالثة، أي ما يسمى عملات رمزيّة رقميّة أو أبكوين (Appcoins) والتي تستخدم سلاسل كتل لأغراض أخرى. وفي حين أنّه يمكن استخدام العديد من الأبكوين كعملات مفيدة لأنواع مختلفة من العمليّات الماليّة، إلاّ أنّها تخلق وتعتمد على بنية تحتيّة أكثر تعقيداً ولا تختلف كثيراً عن غيرها من العملات الافتراضيّة في الجوانب الأكثر ملاءَمة لهذا التقرير[26]. ويبدو أنّ هذه الفئة الجديدة مثيرة للإهتمام لأنها تشير إلى تطبيقات تكنولوجيّة جديدة لسلسلة الكتل، على الرغم من أنها قد تكون تسمية خاطئة لهذه الفئة كعملة نظراً للأغراض المعدّة لها (راجع الفصل الخامس لمزيد من النقاش حول التطبيقات الممكنة في المستقبل التي تتخطّى العملات الافتراضيّة).

وبعد أن قدمنا لمحة عامة عن العملات الافتراضيّة وبعض من خيارات تصميمها، نسلّط الضوء الآن على التداعيات المترتبة على الاختيار الهام للتصميم: كيف يتمّ بناء آليات السلطة وتحويلها من بنية مركزيّة لعملات افتراضيّة أكثر قدماً مثل نظام الدفع عبر الإنترنت (WebMoney) إلى البنية اللامركزيّة بالكامل للبتكوين.

---

[25] تستعين بيركوين أيضاً ما يسمّى نظام تنقيب لإثبات صحة ملكيّة الرصيد؛ راجع ساني كينغ (Sunny King) وسكوت نادال (Scott Nadal) "عملة النظير للنظير: عملة النظير للنظير المشفّرة مع نظام إثبات ملكية الرصيد"، دراسة من نشر المؤلّف، 19 آب 2012.

[26] راجع الفصل الخامس لمزيدٍ من النقاش حول تداعيات تقنيّة العملات الافتراضيّة.

لامركزيّة السلطة وتداعيات تصميم العملة الافتراضيّة

لعلّ اختيار تصميم عملة افتراضيّة ما، يتحدد وفق اختيار درجة المركزيّة لآلية سلطتها. وعليه، فإنّ التصاميم الأولى للعملات الافتراضيّة، كما عند تشوم، كانت تتمتع بآليات سلطة مركزيّة وبوجود خادم إلكترونيّ مركزيّ يوفر الخصائص الأمنيّة بعدم حدوث الإنفاق المزدوج والتزوير، مثلاً. لكنّ عيوب هذه البنى هي أنّها تتطلّب على الأقل بعض الثقة في السلطة المركزيّة (أي ألاّ تتجاهل مثلاً ببساطة العمليّات الواردة) حيث يمكن أن تكون عرضة لنقطة واحدة من الفشل أو هدفاً واحداً للهجوم. على سبيل المثال، فإن نظام أم–بيسا (M–PESA)، وهو آلية نقل للعملة تعتمد فقط على الرسائل النصيّة لإجراء المناقلة في الدول مثل كينيا، يرتكز على مزوِّد خدمة الهاتف الخلويّ، إذ إنّ كل ما سيستغرق لتعطيل نظام M–PESA هو الحطّ من فعاليّة الشبكة الخلويّة لدولة معيّنة أو لخوادم مختارة من المزوِّد. وتجدر الإشارة هنا إلى أنّ الجهات الفاعلة غير الحكوميّة، مثل الدولة الإسلاميّة في العراق والشام لا تهتمّ مطلقاً بمدى مركزيّة أيّ عملة من منظور السياسات الماليّة. إلاّ أنّ قابلية التعرض للهجمات الإلكترونيّة قد يكون مصدر قلق كبير.

تتميز البتكوين والغالبية العظمى من الجيل الثاني من العملات الافتراضيّة بآليّة لامركزيّة للسلطة. إذ إن الخادم المركزيّ أو الخدمة المركزيّة غير موجودة، ويمكن لأي مستخدم أن يسهم في موارد آليّة السلطة. تحتاج مثل هذه الهياكل اللامركزيّة بطبيعتها إلى مزيد من المعلومات العامة عن المستخدمين والعمليّات المالية لأنّ كل مستخدم مشارك في آليّة السلطة يجب أن يكون لديه ما يكفي من المعلومات للمساهمة المجدية. وبالإضافة إلى ذلك، قد يستغرق التوافق وقتاً طويلاً بسبب وجوب إتفاق العديد من المستخدمين على أفضل مسار للعمل (لئلاّ تقوم مجموعات صغيرة من المستخدمين يضمرون الشرّ بإختراق أمن المخطط اللامركزي). من ناحية أخرى، حتى وإن كان بعض المستخدمين المساهمين في السلطة اللامركزيّة يضمرون الشرّ، لا يمكنهم إعاقة السلوك الصحيح من جانب مجمل النظام اللامركزيّ بسبب وجود نظام التحقق من التوافق. وبنتيجة هذه المرونة وعدم الحاجة للكثير من الثقة لاستعمال هذه العملة، إتجه العديد من المستخدمين إلى استعمال هذه العملات اللامركزية وخاصة البتكوين.

لكن هناك أرضية مشتركة بين البديلين: هي ما يسمى بعملات افتراضيّة شبه مركزيّة، حيث يتمّ توزيع آليّة السلطة على مجموعة محدودة من المشاركين، (على سبيل المثال مجموعة من عشرة أشخاصّ)، وحينما يقوم جزء كبير منهم بالتآمر عندها فقط تتكشّف المعلومات ويتمّ انتهاك الأمن. قد يكون هذا النهج مفيداً لعدد قليل من المستخدمين يتمتعون بمستوى عالٍ من الأمن وجديرين بالثقة في عدم التآمر مع بعضهم البعض

الآخر. وقد يكون مثال على ذلك المصارف المركزيّة (أو الوحدات العسكريّة) للبلدان المتعددة التي لا تقيم علاقات ثقة متبادلة بالكامل بعضها مع البعض الآخر. إنّ الفائدة من العملات الافتراضيّة شبه المركزيّة هي أنّها توازن بين الثقة ومسائل نقطة الفشل الفرديّة وبين النموذج المركزيّ ومسائل التشتّت الجماعيّة مع النموذج اللامركزيّ. حتى الآن، يبدو أنّ وجود العملات الافتراضيّة شبه المركزيّة هو وجود نظريّ إلى حدّ كبير[27]. إذ إنّ العملة الرمزيّة المصرفيّة (Ripple) هي العملة الوحيدة المدعومة بآليّة سلطة شبه مركزيّة، ولكنّها ليست مصممة بهدف حماية خصوصيّة المستخدم بطريقة مُجدية؛ ولمزيد من التفاصيل، راجع النقاش حول موضوع المجهولية في العملات الافتراضيّة في الفصل الرابع[28].

وبعد مناقشة الحالة الراهنة للعملات الافتراضيّة، سنقوم الآن بالتحقيق لمعرفة مدى استخدام الجهات الفاعلة غير الحكوميّة للعملات الافتراضيّة بالإضافة إلى القيام ببحث موجز عن عمليّات نشر عملات افتراضيّة سابقة ذات دوافع سياسيّة.

العملات الافتراضيّة والجهات الفاعلة غير الحكوميّة

في هذا القسم، نقدّم لمحة موجزة عن استخدام الجهات الفاعلة غير الحكوميّة للعملات الافتراضيّة، ولا سيما لأغراض إجراميّة، وكذلك نقوم ببحث عن حالات نشر سابقة لعملات افتراضيّة ذات دوافع سياسيّة.

تتوافر أدلّة كثيرة على كون الجهات المنظّمة الفاعلة غير الحكوميّة، وخاصّة مجرمي الإنترنت، تستخدم العملات الافتراضيّة [29]. مع ذلك، لا يبدو أنّ هناك دليلاً دامغاً على أن هذه الجهات الفاعلة تُجري بانتظام عمليّات تجاريّة اقتصاديّة باستخدام عملة

---

[27] راجع، على سبيل المثال، كريم الدفراوي وجوشوا لامبكينز (Joshua Lampkins)، "تأسيس العملات الرقميّة على الحوسبة الآمنة"، أمن الحواسيب والإتّصالات 2014: نتائج المؤتمر الذي نظّمته المجموعة ذات المصالح المشتركة حول الأمن والتدقيق والرقابة التابعة لرابطة مكائن الحوسبة حول أمن الحواسيب والاتّصالات، آذار 2014، الصفحات 1 إلى 14.

[28] تتمتّع العملة الإفتراضية داش (التي كانت تعرف سابقاً ب"دارك كوين") ببنية هجينة تضمن الغفليّة بفضل هندسة شبه مركزيّة، ولكن معظم العناصر الأخرى لهذه العملة تخضع لبنيةٍ لامركزيّة؛ راجع موقع Dash الإلكترونيّ، الصفحة الرئيسة، غير مؤرّخة (a)، وموقع Dash الإلكترونيّ، "خادم ماسترنود وإثبات الخدمة"، غير مؤرّخ (b).

[29] راجع، على سبيل المثال، سماني، 2013a و2013b.

افتراضيّة. في الواقع، تستخدم العملات الافتراضيّة كوسيلة لنقل العملة بشكل آمن ومُغْفَل، من أجل خدمات متخصصة. وبالنتيجة، لا يوجد دليل على أنّ المجموعات المنظّمة (الشريرة) قد طوّرت ونشرت عملات افتراضيّة، ولكن هناك أدلة على أنّ بعضاً من تلك المجموعات قام باستغلال عملات مثل البتكوين في عمليّات غير شرعيّة.

إنّ أحد الاستخدامات الجنائيّة الأكثر شيوعاً للعملات الافتراضيّة، لا سيما البتكوين، هو في عمليّات الحصول على فدية، حيث يقوم مجرمو الإنترنت بتشفير بيانات الضحية وعدم الإفراج عنها إلاّ بعد أن يتمّ دفع مبلغ بالعملة الافتراضيّة، وغالباً ما تكون البتكوين[30]. كذلك تستخدم العملة الافتراضيّة جنائيّاً لشراء البضائع غير المشروعة، كالمخدرات، بواسطة خدمات الإنترنت مثل طريق الحرير[31] (Silk Road). لكنّ هذا يختلف عن عملة افتراضيّة مستخدمة في العمليّات التجاريّة اليوميّة الأمر الذي يتطلب بنية تحتيّة ماديّة لدفع المال والتمكّن من تسديد المدفوعات إلى بائعين فعليّين بدلاً من مجرّد مواقع إلكترونيّة. من هنا، فإنّ التقنيّة المطلوبة لتمكين تسديد تلك المدفوعات تشمل الهواتف الذكيّة (راجع المناقشة في الفصل الرابع عن قابليّة نشر العملات الافتراضيّة).

إنّ الأدلّة على أن الإرهابيين يستخدمون عملات افتراضيّة على مستوى مؤثر قليلة جداً لا سيما بالمقارنة مع المنظّمات الإجراميّة، وبالتالي فإنّ أفضل الأمثلة على ذلك، إعلانان الكترونيّان لأنصار ما يسمّى الدولة الإسلاميّة في العراق والشام يحثون بهما على جمع التبرعات عبر استخدام البتكوين[32]. لقد لاحظ آرون برانتلي (Aaron Brantly)، وهو من أكاديميّة ويست بوينت العسكريّة،

---

[30] راجع، على سبيل المثال، مكتب التحقيقات الفيدراليّ، "إرتفاع عدد برامج الفدية الخبيثة: يعمل مكتب التحقيقات الفيدراليّ وشركاؤه على مكافحة هذا التهديد الإلكترونيّ"، 20 كانون الثاني 2015.

[31] للاطّلاع على إحدى تحاليل خدمات الإنترنت الشبيهة بسوق المخدّرات غير المشروعة، راجع نيكولاس كريستن (Nicolas Christin)، "السفر عبر سوق الإنترنت الشبيهة بسوق المخدّرات غير المشروعة: تحليل قياس سوق إلكترونيّ ضخم ومغفل"، نتائج المؤتمر الدولي الثاني والعشرين حول الشبكة العنكبوتيّة العالميّة (WWW 2013)، ريو دي جينيرو: مؤتمر حول الشبكة العنكبوتيّة العالميّة، 2013، الصفحات 213 إلى 223.

[32] راجع تقيّ الدين المنذر، "بتكوين وصدقة الجهاد"، مقال من نشر المؤلّف، آب 2014. إبتداءً من 26 شباط 2015، وآدم تايلور (Adam Taylor) "الدولة الإسلامية (أو جهة تنتحل هويّتها) تحاول جمع تبرّعات باستخدام البتكوين"، موقع صحيفة واشنطن بوست الإلكترونيّ، 9 حزيران 2015.

وجود أدلّة كافية على أنّ الإرهابيين يبحثون في استخدام العملات الرقميّة مثل العملة الرقميّة الإلكترونيّة لتمويل أنشطتهم حتى أنّهم يستخدمونها في حالات محدودة. وفي حين أنّ هذه الأدوات اكتسبت شعبيّة في السنوات الأخيرة، فإنّ توسع نطاقها إلى المنظّمات الإرهابيّة المختلفة كان بطيئاً ومتأنياً ولم يواكب وتيرة الاستخدامات الإجراميّة العابرة للحدود للتقنيّات نفسها[33].

قد يتغيّر هذا الوضع في المستقبل إذا شعرت الجهات الفاعلة غير الحكوميّة أنّ لديها الكثير لتكسبه سياسيّاً واقتصاديّاً أو على مستوى سلاسة العمليات المالية، مما سيدفعها للتحرّك نحو زيادة استخدام العملات الافتراضيّة.

وفي الآونة الأخيرة، ظهرت حالات نشر للعملة الافتراضيّة ذات دوافع سياسيّة من أجل أن تحلّ محلّ العملة الماديّة السياديّة المتداولة في دولة ذات سيادة (وذلك مع موافقة الحكومة أو بدونها). فتمّ نشر عملة اوروراكوين (Auroracoin) في ايسلندا من قبل مصدر مجهول في آذار 2014 كوسيلة لتوفير عملة من شأنها أن تكون أقل عرضة للتضخم وغير خاضعة للأنظمة الحكوميّة[34]. وكذلك قام ديريك نيسبت (Derek Nisbet) بإطلاق عملة سكوتكوين (Scotcoin) كعملة اسكتلندية جديدة مستقلّة[35]. وتقوم الإكوادور بدراسة إمكانية استخدام عملة افتراضيّة كبديل للعملة الماديّة[36]. والجدير بالذكر أنه في ايسلندا واسكتلندا مثلاً لم تعاقب الحكومة الشرعيّة صراحة نشر العملة الافتراضيّة، بينما في الإكوادور، يبدو أنّ الحكومة دعمت الجهد المبذول لنشر تلك العملة. غير أنّه إلى الآن لم يتمتع نشر أيّ عملة افتراضيّة بديلة باعتماد واسع النطاق.

تجدر الإشارة هنا إلى أنّ أحد الأهداف الأساسيّة من هذا التقرير هو البحث في التحديّات الرئيسة التي ينبغي التغلب عليها، إذ من شأنها أن تمكن الجهات الفاعلة

---

[33] راجع برانتلي (Brantly)، 2014، ص. 1.

[34] راجع موقع Auroracoin الإلكترونيّ، "لماذا أيسلندا؟ أساءت حكوماتٌ عدّة استخدام عملاتها الوطنية، ولكن لمَ تشكّل أيسلندا مكاناً جيّداً لإنطلاق أوّل عملة مشفّرة لوطنية؟" غير مؤرّخ.

[35] راجع موقع Folding Coin الإلكترونيّ، "إطلاق سكوت كوين"، 5 شباط 2015. ألكس هورن (Alex Hern)؛ "بتكوين تنتشر على المستوى الوطنيّ مع سكوتكوين وأوروراكوين"، موقع صحيفة غارديان الإلكترونيّ، 25 آذار 2014؛ ويوليو بريسكو (Giulio Prisco)، "دولة إسكتلنديّة مستقلّة تعتمد على البتكوين؟" موقع CryptoCoinNews.com، 17 أيلول 2014.

[36] راجع نايثن غريل (Nathan Grill)، "الإكوادور تتجّه إلى العملات الافتراضيّة بعد قروض النفط"، موقع بلومبورغ نيوز الإلكترونيّ، 11 آب 2014.

غير الحكوميّة، بما في ذلك المجموعات الإرهابيّة، استغلال العملة الافتراضيّة من أجل مكاسبها السياسيّة والاقتصاديّة و/أو على مستوى سلاسة العمليات المالية. وفي حين أنّ جهة فاعلة غير حكوميّة قد تفضّل عملة ورقيّة أكثر قياسيّة على العملة الافتراضيّة، فإن التغيّرات في النظرة إلى العملات الافتراضيّة في المستقبل، لا سيما من حيث الثقة بالعملات الافتراضيّة كعملة مضمونة ومرنة ومتاحة، قد يزيد كثيراً من إحتمال اعتمادها. وعلى وجه الخصوص، إنّ دعماً من قبل دولة قوميّة حليفة ملمّة إلكترونيّاً قد يؤثّر بشكل كبير على جهة فاعلة غير حكوميّة إزاءَ نشر عملة افتراضيّة.

هل يمكن للعملات الافتراضيّة زيادة القوّة السياسيّة؟

يتناول هذا الفصل إحتمال استخدام عملات افتراضيّة من قبل جهات فاعلة غير حكوميّة لزيادة قوّتها السياسيّة و/أو الاقتصاديّة بنشر العملة الافتراضية واستخدامها في العمليات المالية بدلاً من العملة الماليّة العاديّة. وتأسيساً على تحليلاتنا للأسس الإجتماعيّة والسياسيّة لاستخدام العملات من قبل جهات فاعلة غير حكوميّة، فإنّ السيطرة على تلك العملات يمكن أن توفّر لتلك الجهات، مثل المجموعات المتمرّدة، أداة هامّة لزيادة نفوذها السياسيّ والاقتصاديّ في المناطق المتنازع عليها.

تاريخيّاً، أصدر المتمرّدون عملات جديدة في محاولة لفرض سيطرتهم السياسيّة والاقتصاديّة. من هنا، فإنّ إعلان الدولة الإسلاميّة في العراق والشام في 13 تشرين الثاني 2014، بأنّها ستصدر عملتها الخاصّة المرتكزة على السلع الأساسيّة، يدخل ضمن هذا الإطار[1]. فاختيار الدولة الإسلاميّة في العراق والشام العملة المرتكزة على السلع بدلاً من العملة الافتراضيّة قد يكون نتيجة للصعوبات التي ينطوي عليها نشر العملة الافتراضيّة في منطقة متنازع عليها سياسيّاً وتتميّز نسبيّاً ببنية تحتيّة ماديّة ضعيفة وبانخفاض مستوى الإختراق لمنصات تكنولوجيا الإتصالات مثل الهواتف الذكيّة. وكما نوقش في الفصل السابق، فإنّ نيّة الدولة الإسلاميّة في العراق والشام المعلنة لاستخدام عملة مرتكزة على سلعتيّ الذهب والفضّة تؤكّد المصداقيّة الاقتصاديّة التي تنقلها العملة بحيث تنشأ قيمتها من التبادلات الدوليّة للسلع.

ولكن حتى الآن، لم تُستخدم العملات الافتراضيّة بنجاح على نطاق واسع كمنافس كامل للعملات الورقيّة للدول. وكما هو مُتوَقّع، لم تكن العملات الافتراضيّة خياراً مطروحاً

[1] راجع بورزو داراغاهي، "تعلن الدولة الإسلامية في العراق وسوريا عملتها الخاصّة"، صحيفة فاينانشل تايمز الإلكترونيّة، 13 تشرين الثاني 2014.

بالنسبة إلى المتمرّدين المتورّطين في حروب أهليّة، نظراً لمتطلّباتها الكبيرة لبنية تحتيّة تقنيّة.

وقد قام بعض أنصار الحركات الإنفصاليّة في البلدان المتقدّمة، مثل اسكتلندا[2]، بإصدار عملات افتراضيّة، (على سبيل المثال السكوتكوين، Scotcoin)، ولكن من دون أيّ دعمٍ شعبيّ. كما أطلقت في أيسلندا أوروراكوين بمثابة وسيلة للإعتراض على النظام الحكوميّ الصارم تجاه تطبيق ضوابط رأس المال. على هذا النحو، لم يُعتبر هذا التحرّك وسيلة للتمرّد أو الإنفصال، ولكنّه شكّل احتجاجاً سياسيّاً قويّاً ضدّ سياسات الاقتصاد الكليّ للحكومة. لذلك، اعتمد المطوّرون شعار "أُمّة تكسر أغلال العملة الورقيّة"[3]. وبصفتها عملة افتراضيّة، مثّلت أوروراكوين تجربة مثيرة للإهتمام ولكنّها، مع ذلك، فشلت في جذب مستخدمين لها بسبب أنّ سكّان أيسلندا غير راغبين بعد في التحوّل من الكرونا إلى الأوروراكوين، على الرغم من وجود نظام ضوابط رأس المال في أيسلندا.

ولهذا، فإنّ هذه الأمثلة توضح الجدوى التقنيّة من نشر عملة افتراضيّة من قبل جهات فاعلة غير حكوميّة، فضلاً عن التحدّيات التي تواجه تلك الجهات بغية تشجيع المشاركة المجتمعيّة في استخدام عملة افتراضيّة جديدة عندما تبقى خيارات العملة التقليديّة متاحة. وبناءً عليه، نتوقّع أن تقوم الجهات الفاعلة غير الحكوميّة على الأرجح بحمل الناس على استخدام عملة افتراضيّة جديدة عندما تمتلك تلك الجهات الفاعلة ما يكفي من السيطرة الإقليميّة والقدرة على إنفاذ وفرض استخدام عملتها الافتراضيّة.

تظهر عملات غير رسميّة عندما تصبح العملات الرسميّة غير قادرة على تلبية احتياجات المجموعات

مع الإهتمام الكبير الذي تتمتّع به العملات الافتراضيّة مثل البتكوين، قد يعتقد شخص ما أنّ العملات الافتراضيّة كانت تلعب دوراً هامّاً بمثابة وسيط تبادل جديد للعمليّات اليومية في دول مثل الولايات المتّحدة. ولهذا تصف مقالة بلومبرغ الأخيرة تزايد شعبيّة العملة الرقميّة الإلكترونيّة بقولها[4]:

---

[2] راجع موقع Scotcoin الإلكترونيّ، الصفحة الرئيسة، غير مؤرّخ.

[3] راجع موقع Auroracoin الإلكترونيّ، غير مؤرّخ.

[4] راجع أولغا خريف، "بتكوين: "لم يعد استعمال البتكوين محصوراً بالتحرّريّين والفوضويّين"، موقع *BloombergBusiness.com* الإلكترونيّ، 9 تشرين الأوّل 2014.

> المستهلكون يتبنّون العملة الرقميّة... الآباء والأمّهات يحوّلون البدلات والعلاوات إلى البتكوين لتعليم أولادهم ليكونوا مواطنين رقميّين. مدخّنو الماريجوانا يشترون أعشاب التدخين القانونيّة من آلات بيع تعمل بالبتكوين. والمستهلكون في الأسواق الناشئة مثل البرازيل وروسيا بدأوا باستخدام البتكوين ليحتاطوا من تقلّبات عملاتهم.

إنّ الطلب الإجمالي على العملات الافتراضيّة كعملات كاملة منافسة للعملات الورقيّة المُدارة مركزيّاً في بلدان ذات قدرات قوية وسياسات اقتصاد كلّيّ مستقرّة لا يزال ضئيلاً نسبيّاً. ولذلك، قامت البنوك المركزيّة والحكومات في الدول المتقدّمة بتقويم مخاطر السيطرة النقديّة الناجمة عن العملات الافتراضيّة المتداولة في مناطق مسؤوليّتها على أنّها مخاطر منخفضة، على الأقلّ عند المستويات الحاليّة والمتوقّعة لتداول العملات الافتراضيّة[5].

ومن هنا، إتّضح أنّ هناك شرطين من المرجح أن تلقى العملات الافتراضيّة في ظلّهما رواجاً كخيار العملة المفضّل لدى الجهات الفاعلة في السوق. الشرط الأول هو ألّا توفّر السلطة المركزيّة بيئة مستقرّة للاقتصاد الكليّ، ونتيجةً لذلك، تصبح العملة الورقيّة الإقليميّة غير موجودة أو تصبح قيمتها غير مستقرّة[6]. لذا، فإنّ الهيئة المصرفيّة الأوروبيّة تسلّط الضوء على هذه البيئة باعتبارها واحدة من النتائج الرئيسة لتقريرها عن العملات الافتراضيّة[7].

> في المناطق الخاضعة لسلطة قضائيّة حيث الخدمات الماليّة غير متوفّرة على نطاق واسع، أو حيث يواجه المستخدمون مخاطر عالية، أو حيث العملة الوطنيّة غير قابلة للتحويل إلى عملات ورقيّة أخرى، أو حيث تكون الخدمات الماليّة مكلفة للغاية بالنسبة إلى الأفراد، أو حيث يكون العبء

---

[5] راجع البنك المركزيّ الأوروبيّ، 2012، وميرفي، ميرفي وسايتزينغر (Murphy, Murphy and Seitzinger)، 2015.

[6] من المهم أن نلاحظ أنّ العملة الإفتراضيّة ليست البديل النقديّ الوحيد للعملة الورقيّة في منطقة تفتقر إلى بيئة مستقرة للاقتصاد الكلّيّ. يمكن للمشاركين في السوق أيضاً الانخراط في المقايضة وتطوير عملة مجتمعهم الخاصّة على أساس أنّها ورقيّة، أو استخدام عملة دولة أخرى. وقد تمّ استخدام الدولار الأمريكي على نطاق واسع خارج الولايات المتّحدة. يركّز هذا التقرير على إمكانيّة الجهات الفاعلة غير الحكوميّة نشر عملة إفتراضيّة. لكنّه لا يوفّر تقييماً للمقايضات عبر قائمة كاملة من خيارات ترتيب عملة بديلة متاحة للجهات الفاعلة غير الحكوميّة.

[7] راجع السلطة المصرفيّة الأوروبيّة، 2014.

الإداريّ للحصول على حساب مرتفعاً، عندها توفّر مخطّطات العملة الافتراضيّة وسيلة بديلة للأفراد لتحقيق الغاية عينها: الوصول إلى التجارة وتفعيل عمليّات الدفع.

تتعدد الأسباب التي قد تجعل المناطق تفتقر إلى عملة وطنيّة مستقرة. فقد تكون المنطقة المعنيّة جزءاً من أراضي دولة مفككة بدون حكومة فاعلة أو جزءاً من بلد غارق في خضمّ حرب أهليّة أو حتى في دولة ذات حكومة مستقرّة، إنما ذات سياسات اقتصاد كليّ غير مستقرة أو سياسات تجمّد المشاركة الاقتصاديّة من قبل جزء كبير من سكّانها، (وذلك مثل البلدان التي فيها سوق سوداء كبيرة). وفي بيئة لا يمكن للسلطة المركزيّة فيها الحفاظ على استقرار العملة الورقيّة وسهولة الوصول إليها، قد تتوفّر للجهة الفاعلة غير حكوميّة الراعية لعملة افتراضيّة حلّاً قابلاً للتطبيق.

والحالة الثانية التي قد تلعب فيها العملات الافتراضيّة دوراً هامّاً هي حالة بناء المجتمعات والحفاظ عليها. وعلى الصعيد المحليّ، قامت مجتمعات عديدة بإنشاء أنظمة تبادل تجاريّ إقليميّة[8]. فضلاً عن ذلك، إنّ العملات المحليّة توسّع نطاق البنية التحتيّة للتبادل في المجتمع المحليّ إلى مدى أبعد من التبادلات الاقتصاديّة من أجل دعم الأبعاد الإجتماعيّة والأخلاقيّة والبيئيّة التي تحتلّ مكانة قيّمة في المجتمع المحلّيّ. إنّ معظم العملات في المجتمع المحليّ مقيّدة جغرافيّاً وتُتداول جنباً إلى جنب مع العملات الوطنيّة[9]، وقد تعكس قيمتها في مجتمع محلّيّ معيّن بالتحديد أهداف هذا المجتمع علاوةً على أنّ إنشاءها قد يعكس دفع ثمن مقابل الخدمات المقدّمة فقط لهذا المجتمع. ومن أمثلة العملات المتداولة في المجتمع المحلّيّ الساعات الزمنية إيثاكا (Ithaca Hours) ودولارات الينابيع المالحة (Salt Spring Dollars)[10] أو عملات أكثر عالميّةً مثل برنامج المسافر الدائم (frequent–flier miles). فبينما تستخدم معظم المجتمعات العملات الورقيّة، جرت محاولات قليلة للتسلّل داخل العملات الافتراضيّة للمجتمع المحلّيّ. ونظام جنيه توتنس (The Totnes Pounds System) يدعم كلّاً من العملتين الورقيّة والإلكترونيّة[11].

---

[8] على الرغم من أنّنا نركز هنا على أمثلة حديثة من عملات المجتمع المحلّي، تقوم كريستين ديزان (Christine Desan) بدرس أهمية نظم الصرف في المجتمع المحلّيّ ودور أصحاب المصلحة في المجتمعات الإنجليزيّة في العصور الوسطى (كريستين ديزان، جني الأموال: النقود والعملات وظهور الرأسمالية، أوكسفورد: دار نشر جامعة أوكسفورد، 2014).

[9] راجع جيروم بلان (Jerome Blanc)، "ثلاثون عاماً من المجتمع والعملات التكميلية،" المجلّة الدولية لبحوث عملات المجتمع، المجلّد 16، 2012، الصفحات D1 إلى 4.

[10] راجع موقع Ithaca Hours الإلكترونيّ، الصفحة الرئيسة، غير مؤرّخ، وموقع Salt Spring Dollars الإلكترونيّ، الصفحة الرئيسة، غير مؤرّخ.

[11] راجع موقع Totnes Pound الإلكترونيّ، الصفحة الرئيسة، غير مؤرّخ.

لقد قام دايفيد فاندرفورت (David Vandervort) وزملاؤه في مركز أبحاث بالو ألتو بتحديد عملة مازاكوين[12] (Mazacoin)، العملة الوطنيّة المزعومة لأمّة لاكوتا، وكذلك عملة آيريش كوين[13] (Irish Coin)، وهي عملة مجتمع وضعت لتعزيز صناعة السياحة الإيرلندية، كنموذجين من العملات الافتراضيّة المجتمعيّة[14]. وكلّما تحسّنت تقنيّات العملات الافتراضيّة، تزايد احتمال استخدام العملات الافتراضيّة المجتمعيّة.

والجدير بالذكر أنّ معظم المجتمعات المحلّيّة التي اعتمدت العملات المجتمعيّة قد فعلت ذلك ضمن بنية نظام ماليّ متطوّر، أيّ في بلد مستقرّ وديمقراطيّ عموماً أو نظام دوليّ بسياسات اقتصاد كلّيّ مستقرّة[15] أو قواعد سلوك مشتركة. إلاّ أنّه ليس كل الجهات الفاعلة غير الحكوميّة قد تختار تطوير عملات بديلة تتكامل عمليّاً مع العملات الورقيّة في بلادهم. لذا، فإنّ العديد من الجهات الفاعلة المذكورة، مثل الانفصاليّين والمجموعات المتمرّدة، وكذلك المناطق المتنازع عليها، تُصدر عملاتها الخاصّة من أجل تسليط الضوء على السيادة الاقتصاديّة وترسيخ السيطرة الاقتصاديّة في المناطق التي تقع ضمن نطاق سلطتها أو الأراضي التي ترغب في السيطرة عليها[16]. على سبيل المثال، منطقة الحكم الذاتيّ في الصومال التي تستخدم الشلن الخاصّ بها، وكذلك منطقة الحكم الذاتيّ في ترانسنيستريا التي لديها الروبل الخاصّ بها وبلدة أورانيا في جنوب أفريقيا التي يسكنها البيض فقط حيث تستخدم عملة تُسمّى أورا[17] (Ora). وبالإضافة إلى إعلان الدولة

---

[12] راجع موقع Mazacoin الإلكترونيّ، الصفحة الرئيسة، غير مؤرّخ.

[13] راجع موقع Irish Coin الإلكترونيّ، الصفحة الرئيسة، غير مؤرّخ.

[14] راجع دايفيد فاندرفورت (David Vandervort)، دايل غوكاس (Dale Gaucas)، وروبرت سانت جاك (Robert St. Jacques)، "مسائل تصميم عملة مجتمعيّة تشبه بتكوين"، دراسة قدّمت في خلال ورشة العمل الثانية حول الأبحاث التي تتناول عملة بتكوين، سان خوان، بويرتو ريكو، 30 كانون الثاني 2015.

[15] دامجان بفاجفار (Damjan Pfajfar)، جيوفاني سغرو (Giovanni Sgro)، وولف واغنر (Wolf Wagner)، "هل تحلّ العملات البديلة محلّ العملة الورقيّة أو تكمّلها؟ إثباتات من بيانات مجمّعة من بلدان عدّة"، المجلّة الدوليّة للأبحاث حول العملات المجتمعيّة، المجلّد رقم 16، 2012، الصفحات 45 إلى 56، وجدوا أنّ استخدام عملات المجتمعات المحليّة مرتبط بشكل إيجابيّ بالاستقرار في العملة الورقيّة في الدولة، بتطوُّر القطاع المالي وبالتنمية الإقتصاديّة الشاملة.

[16] راجع دانيال ترايزمان (Daniel Treisman) "نهضة روسيا الأخلاقيّة: الفاعليّة الإنفصاليّة للقادة الإقليميّين في النظام ما بعد الشيوعيّة"، وورلد بوليتكس، المجلّد رقم 49، العدد 2، 1997، الصفحات 212 إلى 249.

[17] راجع موقع Wikipedia الإلكترونيّ، "أورا (عملة)"، 27 نيسان 2015.

الإسلاميّة في العراق والشام لإطلاق عملتها الخاصّة، أعلن البنك المركزي في باروتسلاند في العام 2012 إدخال الموبو (mupu) عملة له في العام 2012 [18].

وباستخدام مثال المجموعة متمرّدة المسيطرة على منطقة معيّنة متنازع عليها، فإنّ لدى هذه المجموعات المتمرّدة ثلاثة خيارات عند اعتماد عملة ما.

الخيار الأوّل هو تبنّي العملة القائمة على السلع الأساسيّة حيث تكون العملة المتداولة هي السلعة الأساسيّة نفسها كالنقود الذهبيّة مثلاً. وهذه هي إستراتيجيّة الدولة الإسلاميّة في العراق والشام المعلنة. فالمصلحة الأساسيّة من هذا الخيار هي أنّ مصداقيّة العملة تصبح مدعومة من قيمتها الجوهريّة والسوق الدوليّة للسلعة. وبذلك، لم يعد هناك حاجة للثقة بالسلطة النقديّة حيث أن الذهب أو الفضّة سيضمن قيمة تلك العملة. ولكنّ الحدّ الأساسيّ لهذا الخيار هو أنّه من الصعب بالنسبة إلى معظم المجموعات المتمرّدة جمع إمدادات كافية من الذهب والفضّة لطرح هذا النوع من العملة للتداول.

أمّا الخيار الثاني، فهو تبنّي واعتماد عملة بلدٍ آخر. هذا الخيار يمكن أن يتراوح بين تداول العملة الموجودة أصلاً مباشرةً في الاقتصاد المحلّيّ (كالدولرة على سبيل المثال) إلى سكّ عملة جديدة مدعومة بنسبة 1:1 من احتياطيّات عملة بلد آخر (كاستخدام صندوق إصدار النقد). في هذا الإطار، فإنّ قادة جمهوريّة دونيتسك الشعبيّة المُعلنة من جانب واحد قد حاولت إقامة منطقة روبل في شرق أوكرانيا. على أنّ التكاليف والفوائد لهذا الخيار تشبه إلى حدّ ما تكاليف وفوائد العملة المرتكزة على السلع الأساسيّة. من هنا، فإنّ العملة الجديدة تكسب مصداقيّتها على أساس إستقرار عملة البلد الذي يُصدرها واعتماد تلك العملة في جميع أنحاء الإقليم. لذلك، إذا هبطت قيمة عملة هذا البلد سوف تهبط أيضاً قيمة العملة الجديدة. وبالنتيجة، إنّ جدوى هذا الخيار تعتمد على قدرة المجموعة المتمرّدة على جمع إمدادات كافية من العملة المعتمدة لإصدارها في أراضيها أو استخدامها لتخزينها كإحتياطي للعملة الخاصّة بها. ولهذا، من السهل التغلّب على هذه العقبة، خاصّةً بوجود دعم من البلد المُصدر. في الواقع، إنّ دعماً من قبل دولة أخرى، لا سيما عندما تمتلك تلك الدولة قدرات إلكترونيّة متطوّرة، هو مساعد رئيس لنشر عملة الجهة الفاعلة غير الحكوميّة (راجع الفصل الرابع لمزيد من النقاش).

[18] راجع دولة باروتسلاند المستقلّة، قانون عملة موبو الخاصّة بدولة باروتسلاند لعام 2012، 28 شباط 2012. باروتسلاند هي منطقة متنازع عليها بين زامبيا وأنغولا. أصدر البنك المركزيّ عيّنات من فواتير بعملة موبو (mupu)، ولكنّه لا يملك الموارد اللازمة لإصدار عملة مستقرّة والحفاظ عليها.

أمّا خيارها الثالث، فهو اعتماد عملة خاصّة بها. وفي هذا الخيار، قد لا تكون العملة مدعومة بالضرورة بنسبة 1:1 من سلعة أساسيّة أو من أسهم عملة الإحتياطيّ. وأحد الأمثلة على ذلك ما حدث عندما أقدمت السلطات الإنفصاليّة في الصومال على إطلاق الشلن الصوماليّ للتداول على أساس عملة ورقيّة دون أن تكون مرتبطة بشكل واضح بسلعة أساسيّة أو عملة إحتياطيّة. وفقاً لذلك، فإنّ الفائدة من هذا الخيار هي في أنّ المجموعة المتمرّدة تحتاج فقط إلى احتياطيّات صغيرة من السلع الأساسيّة أو من العملات الأجنبيّة لطرح عملتها الجديدة للتداول. إلاّ أنّ عيب هذا الخيار هو عدم وجود قيمة جوهريّة في صلب العملة عند طرحها في البداية[19]. قد يساعد معدّل سعر الصرف الثابت على مكافحة التقلّبات في قيمة العملة؛ ومع ذلك، ما لم يصادق السوق على أنّ قيمة العملة قد قُيِّمت بدقّة أو أنّ المجموعة المتمرّدة لديها إحتياطيّات من العملات الأجنبيّة للدفاع عن سعر الصرف الثابت، لن تكون المجموعة المذكورة قادرة على الحفاظ على قيمة العملة[20].

قد لا تكون العملات غير الصادرة عن الدولة حالياً عملات افتراضيّة إنما قد تصبح كذلك في المستقبل

على الرغم من محاولات بعض المجموعات الإنفصاليّة اعتماد عملات خاصّة بها، فإنّنا لا نتوقّع أن تكون العملة الافتراضيّة الشكل المفضّل لديها على المدى القريب بسبب وجود ثلاثة أسباب رئيسة تصبّ كلّها في سؤال وهو لماذا قد يشكّل نشر عملة افتراضيّة صعوبات أكبر من الخيار القائم على السلع الأساسيّة أو على العملة الورقيّة؟ فالسبب الأوّل هو أنّ معظم المنظّمات المتمرّدة تفتقر حالياً إلى المهارات الضروريّة لنشر عملة افتراضيّة. ولذلك فإنّ معظم حركات التمرّد تحدث في الأراضي المتنازع عليها سياسيّاً والتي تتّسم ببنية تحتيّة ماديّة ضعيفة وقدرة محدودة على إختراق منصات تقنية الإتصالات، مثل الهواتف الذكيّة. ولكن، وعلى الرغم من أنّ النقاش الدائر بشأن استخدام العملة الافتراضيّة مصدراً لتنمية رأس المال في المناطق التي تعاني تنمية اقتصاديّة منخفضة قد أثار إهتمام الأوساط الإنمائيّة، فإنّ الحاجة إلى هواتف خلويّة متقدّمة، أيّ هواتف ذكيّة، للعملات الافتراضيّة قد أعاق التنفيذ. في المقابل، فإنّ نظام أم- بيسا M-PESA، وهو نظام

---

[19] ولكن، تجدر الإشارة إلى أنّ التردّد في ما يتعلّق بعملات جديدة يمكن التغلّب عليه من خلال بدء طرح عملة جديدة بشكل دقيق وسليم. المثال الأشهر هو طرح البرازيل للريال كعملة ورقيّة ($R) في العام 1994، حيث تمّت إدارتها بعناية لتحلّ محلّ العملة القديمة للتغلّب على التضخّم الشديد.

[20] بدلاً من ذلك، يمكن للمجموعة أن تعلن أنّ العملة ليست قابلة للتحويل. وفي هذه الحالة، فإنّ بيان سعر الصرف الثابت يمكن ببساطة أن يخدم غرضاً رمزياً.

لتحويل الأموال بواسطة الهاتف المحمول (مع آليّة مناسبة بدلاً من عملة افتراضيّة) يعمل بشكل جيّد في نيجيريا، إذ إنّه يحظى بدعم فعّال من الحكومة النيجيرية ومتطلّبات تقنيّة منخفضة. سنناقش الإحتياجات التقنية للعملة الافتراضيّة وتحدّياتها بمزيد من التفصيل في الفصل التاليّ.

والسبب الثاني هو أنّ القوانين النقديّة التي تقوم عليها العملة الافتراضيّة تحتاج إلى تحديد وتطبيق مستمر. وبذلك، فإنّ هذه القوانين تحدّد خصائص تلك العملة والكيفيّة التي سيتمّ بها تحفيز الجهات الفاعلة لخلق وتأمين العملة، سواء ما إذا كان سيتمّ وضع سقف محدّد للعرض النقديّ أم سيواصل نموّه، وما إذا كان المال سيكون مقيّداً جغرافيّاً أو يمكن استخدامه على نطاق عالميّ. ففي نظام مركزيّ، يتمّ وضع هذه القوانين وتنفيذها من قبل السلطة المركزيّة. أما النظام اللامركزيّ، فيحتاج إلى شكل من أشكال عمليّة اعتماد القوانين. كما أنّ أنظمة العملات المجتمعيّة غالباً ما أخفقت لأنّ المجتمعات المدرجة ضمن نظام العملة نمت بنسبة كبيرة جداً بحيث لم يعد ممكناً لها البتّ في عمليّة اعتماد المعايير والقوانين بفعاليّة[21]. لذا، تميل العملات الافتراضيّة مثل البتكوين إلى أن تعتمد نظماً لامركزيّة بحيث تحدّد القوانين التي تحكم العملة وتحفّز توسّعها وصيانتها من قبل مصمّميها، ولكنّها تخضع للإجماع في إتخاذ القرارات على مستوى البروتوكول، بين الخوادم الإلكترونية. وعلى هذا، فإنّ اللامركزيّة غالباً ما تكون السمة الرئيسة لمرونة العملة الافتراضيّة. لكنّ المحافظة على التحكّم بقواعد اللعبة، هو مصدر ضعف لعملة افتراضيّة لامركزيّة ذات تداول ضئيل نسبيّاً. فإنّ أيّ مجموعة من المتمرّدين تحاول أن تُنشئ عملة افتراضيّة ستُواجَه بالمفاضلة بين هيكل السلطة المركزيّة التي لا تتأثر بتغيّرات القوانين التي يحثّ عليها أغلبية مالكي العملات، لكنّها بذات الوقت قد تكون أكثر عرضة لخطر هجوم خارجيّ أو(حتى داخليّ). على نقيض ذلك، فإنّ هيكل سلطة لامركزيّة قد يكون هيكلاً أكثر مرونةً لهجمات خارجيّة، ولكن أقل تقبّلاً للتغيرات في القوانين.

والسبب الثالث هو، على الأقلّ في البداية، أنّ ثقة المستخدمين لعملات جديدة لا تزال ضعيفة[22]. لذا يحتاج المستخدمون لبعض الوقت لكي يعتادوا على تلك العملات ويطمئنّوا للنظام والإستقرار وسهولة استخدام العملة. وأخيراً نتوقّع أن تزداد الثقة بالعملات

---

[21] راجع جورجينا غوميز (Georgina Gomez) "إستدامة أنظمة العملات المتمّمة في الأرجنتين: أربع أنظمة حوكمة"، المجلّة الدوليّة للأبحاث حول العملات المجتمعيّة، المجلّد رقم 16، 2012، الصفحات D80 إلى 89.

[22] راجع ماتياس كيلبرر (Matthias Kaelberer)، "الثقة في اليورو: إكتشاف حوكمة عملة فوق وطنيّة"، المجتمعات الأوروبيّة، المجلّد رقم 9، العدد رقم 4، 2007، الصفحات 623 إلى 642.

الافتراضيّة مع الوقت. إنّ تطبيق استخدام عملة جديدة من أيّ نوع أمر صعب ويستتبع تحديّات تقنيّة واقتصاديّة ولوجستيّة ولا سيما بالنسبة للمجموعات المتمرّدة التي تختار نشر عملتها الورقيّة الخاصّة بها، إذ إنّ الثقة في العملة هي عنصر هامّ من عناصر نجاحها. وبناءً عليه، فإنّ إنخفاض نسبة إختراق العملات الافتراضيّة للحياة الاقتصاديّة اليوميّة سوف يزيد من شكوك مستخدمي العملات التي تنشر من خلال هذه التقنية. وعلى الرغم من أنّ العملة الورقيّة قد تتطلّب المزيد من البنية التحتيّة المادّيّة وبأن تكون أقلّ مرونة تجاه أيّ هجوم مادّيّ على المدى القريب، ستصبح العملات الورقيّة أكثر قبولاً وهي جديرة بطبيعتها بثقة السكّان أكثر من العملات الافتراضيّة. وجملة القول إنّ حذر السكّان من العملة الافتراضيّة سوف ينتفي بعد أن يصبحوا أكثر دراية بها. في المقابل، وفي منطقة حيث العملة الافتراضيّة هي الوسيلة الوحيدة للتبادل، سترغم الحاجة الاقتصادية الناس على القبول بالعملات الافتراضيّة والتي، لولا الحاجة، لكانوا رفضوا التعامل بها من الأساس. وحيث أنّ الخيارات متساوية، من المحتمل أن تقوم مجموعة متمرّدة بإختيار عملة ورقيّة، سواء كانت مدعومة من سلع أساسيّة تتحكّم بها الحكومة أم لا، بدلاً من عملة افتراضيّة من أجل زيادة ثقة السكّان في العملة، ولكن يمكن أن يحدث تحوّل في الموقف عندما تصبح التقنيّات التي تكمن وراء العملات الافتراضيّة أكثر انتشاراً وأكثر تمتّعاً بالثقة.

التحديّات التقنيّة التي يواجهها نشر العملة الافتراضيّة

في هذا الفصل، نبحث في التحديّات التقنيّة التي قد تواجهها جهات فاعلة غير حكوميّة عندما تنشر عملة افتراضيّة. وقد يستفيد الخصوم، كالولايات المتحدة الأمريكيّة، من هذه التحديّات لعرقلة نشر الجهات الفاعلة غير الحكوميّة للعملة الافتراضيّة. ويرتبط البعض من هذه التحديّات التقنيّة بتمكين نشر العملة الافتراضيّة بشكل واسع فضلاً عن إمكانية استخدامها بشكل كاف في العمليّات الماليّة اليوميّة (كشراء مشروب غازيّ من المتجر)، فيما يرتبط بعضها الآخر بأمانة نشر العملة الافتراضيّة لتكون موضع ثقة في الاستعمال اليوميّ. إضافةً إلى ذلك، يحتاج كل كيان ينشر عملة افتراضيّة إلى تأمين مرونة العملة في مواجهة الأخطار الإلكترونيّة التي يضعها الخصوم، بما فيها الأخطار الأكثر تطوراً التي تضعها الدول القوميّة المنافسة.

ونشدد على أنّ هذا الجزء سيركّز بشكل أساسيّ على مشاكل نشر العملة الافتراضيّة بدلاً من الإستثمار. غير أنّ بعض التحديّات التي نبحثها هنا، ولا سيما تلك المرتبطة بالمجهولية، تنطبق أيضاً على استثمار العملة الافتراضيّة.

تشمل التحديّات التقنيّة المحددة التي تواجه أيّ جهة فاعلة تحاول أن تنشر عملة افتراضيّة للاستعمال اليوميّ:

- الوصول إلى الإلمام التكنولوجي اللازم لتطوير العملة الافتراضيّة ونشرها والحفاظ عليها كخدمة إلكترونيّة. وفي سياق العملات الافتراضيّة، يشمل الإلمام التكنولوجي اللازم مهارات في مجالات ربط الشبكات والحوسبة وتقنيّات التشفير.
- التأكد من أن مستخدمي العملة يتمتعون بالوصول الثابت والأكيد إلى عملتهم بما يستلزم المستوى الأدنى الكافي من الإلمام التقنيّ للسماح باستعمالها في العمليّات اليوميّة.

- تأمين مستويات من مجهولية العمليّات التي يطالب بها المستخدمون، وتأمين سلامة العملية ليتأكد الشارون والبائعون من التبادل المناسب، وذلك كله من دون الحاجة إلى خبرة تقنية متقدّمة جداً.
- حماية سلامة العملة الافتراضيّة (وتوفرها) ضد الأخطار الإلكترونيّة المتقدّمة ولا سيما الدول القوميّة التي تعارض نشر جهات فاعلة غير حكوميّة للعملة الافتراضيّة.

ومن المهم أن نشير إلى أنّ التحديّات لا تقتصر على بتكوين أو غيرها من العملات الافتراضيّة اللامركزيّة (راجع الفصل الثاني لمناقشة أحدث التكنولوجيات الحاليّة). وبالفعل، ليس واضحاً ما إذا كانت جهة فاعلة غير حكوميّة ستفضّل غياب السلطة المركزيّة. وبالتالي، تشكّل كيفيّة هيكلة بنية السلطة التحتيّة، أي شبكة الحواسيب التي تنفّذ الخوارزميّات التي تؤدي الوظائف العامة نفسها التي تؤديها سلطة متموضعة مركزياً، إحدى نقاط القرار الأساسيّة لإنشاء عملة افتراضيّة.

وطوال هذا الفصل، سنتحدث عن نشر العملة الافتراضيّة كما لو كانت الجهات الفاعلة غير الحكوميّة تعمل وحدها بشكل أساسيّ. فإن مدّتها دولة قوميّة بالإمكانات الإلكترونيّة الملمّة، قد يغير ذلك حسابات القرار الذي تتخذه الجهة الفاعلة غير الحكوميّة بشأن احتمال نشر العملة الافتراضيّة (وكيفيّة نشرها)[1]. وفي الإجماع، سندعو معارضي الجهة الفاعلة غير الحكوميّة التي تنشر العملة الافتراضيّة "خصومهم".

تطوير عملة افتراضيّة ونشرها

تشكّل الخبرة والقدرة العامة الضروريّتان لتطوير العملة ووسائل التعامل بها على حدّ سواء ولنشرها أحد العوائق التقنيّة الرئيسة التي تواجه جهة فاعلة غير حكوميّة في نشرها للعملة الافتراضيّة. في المبدأ، يكون الإلمام التقني اللازم لتطوير العملة الافتراضيّة ونشرها عالي المستوى نسبياً، لكن في الممارسة، تتوافر تكنولوجيا حاليّة للاعتماد العام بهدف دعم نشر مماثل. إضافةً إلى ذلك، يكمن الهدف الأساسيّ في تحديد هذه المشاكل الرئيسة الآن

[1] تجدر الإشارة إلى أنّه تتوافر أدلّة كثيرة عن دعم جهات فاعلة حكومية لجهات فاعلة غير حكومية بشكل عام. لكن هذا الدعم الكبير، الذي يشكّل في الواقع تنسيقاً مباشراً ومستداماً، في نطاق عمليّات الفضاء الإلكترونيّ يبدو مختلفاً بطبيعته عن الأمثلة الحاضرة والقديمة عن الدعم الذي تقدّمه جهات فاعلة حكومية ولو أنّه ممكن.

والتي، متى تغلّبت عليها، ستؤثّر بشكل كبير على قدرة جهة فاعلة غير حكوميّة على نشر عملة افتراضيّة.

إنّ العناصر الرئيسة التي تستلزم التطور هي أولاً، العملة بحدّ ذاتها بما في ذلك خيارات التصميم المهمة والمتعددة وثانياً وسائل اكتساب العملة والحفاظ عليها وتحويلها كجزء من العمليّات الماليّة بما فيها الوسائل الماديّة التي تستطيع أن تدعم هذه التحويلات كالهواتف الذكيّة وثالثاً الخدمات المالية الكافية للدفع اللاحق وأنظمة عمليّات الدفع المباشر لدعم الخدمات جميعها بطريقة آمنة ومرنة.

تطوير برمجيّات لعملة افتراضيّة

تعود صعوبة تطوير برمجيّات على الحاسوب لعملة افتراضيّة جديدة إلى الدرجة التي ترغب فيها الجهة الفاعلة غير الحكوميّة الإبتعاد عن عملات افتراضيّة مستعملة و/أو عن برمجيّاتها ذات الصلة. من جهة، يمكن جهة فاعلة غير حكوميّة أن تعتبر بكل بساطة بتكوين أو أيّ عملة افتراضيّة أخرى عملة لها، لكن ذلك يثير السؤال عن المكسب السياسيّ أو الاقتصاديّ الذي ستجنيه من اعتماد بسيط مماثل. ومن جهة أخرى، يحق للجهة الفاعلة غير الحكوميّة أن تقرر خلق عملة جديدة تماماً من الصفر، ويستلزم ذلك الوصول إلى مطوري برمجيّات يتمتعون بمهارات بارزة. أما الحل الوسط، لربما الأكثر سهولة، فيقضي بخلق الجهة الفاعلة غير الحكوميّة لعملة افتراضيّة جديدة من خلال استعمال البرمجيّات عينها التي تستعملها عملة افتراضيّة مستعملة مسبقاً.

وسيضطر مطورو البرمجيّات أن يصمموا برنامجاً لتنظيم العملة (مثلاً منقّبون عن عملات لامركزيّة شبيهة ببتكوين)، فضلاً عن تطبيقات برمجيّات ليتمكّن المستخدمون اليوميّون من الحفاظ على العملة الافتراضيّة والتعامل بها. ويجب على هذا التطور أن يكون صالحاً للاستعمال بشكل كاف لتشجيع اعتماد العملة الافتراضيّة واستعمالها على نطاق واسع[2]. ونظراً للأمن الأساسي والمتأصل اللازم لتطبيقات مشابهة، يجب أن يكون التقدير التقريبي (الأصغر) لدرجة الإلمام الذي على المطور أن يتمتع به على مستوى إنشاء برمجيّات تشفير مخصصة تستعمل على نطاق واسع. وبالفعل، قليلة هي الأمثلة عن برمجيّات مماثلة في طور الاستعمال حالياً، ويتوفر مثال عام واحد عن برمجيّات

[2] راجع Open Hub، "تلخيص مشروع بتكوين"، غير مؤرّخ.

مماثلة لم تعد تستعمل فجأة[3]. تجدر الإشارة إلى أنّه إذا حظيت جهة فاعلة غير حكوميّة بدعم دولة قوميّة بما يشمل الوصول إلى خبرائها ومطوريها الإلكترونييّن، قد يمكن تنفيذ تتطور مماثل بشكل أكبر. وحتى في هذه الحالة الأقرب إلى المثاليّة، تتوافر أمثلة عن قدرات إلكترونيّة متطورة تواجه صعوبات في إنشاء خدمات إلكترونيّة منتشرة على نطاق واسع، حتى في الأمكنة الأكثر تساهلاً كتطوير الولايات المتحدة عمليّات التبادل على الإنترنت لدعم قانون الرعاية الصحيّة. وبشكل بديل، قد تعتمد الجهة الفاعلة غير الحكوميّة على "منظّمات القراصنة على شبكات الإنترنت" أو منظّمات الجرائم الإلكترونيّة أو المرتزقة[4] الإلكترونية التي تتحالف بعضها مع البعض الآخر أو يدفع لها. تجدر الإشارة إلى أنّ بعض الجهات الفاعلة غير الحكوميّة، ولا سيما المنظّمات الإرهابية، تبدو على الأقل ذات قدرة محدودة على إنشاء خدمات إلكترونية آمنة كمنصات التشفير[5].

أما الطريق الأقرب لتطوير عملة افتراضيّة جديدة فيقضي بتعديل عملة افتراضيّة مستعملة مسبقاً ويعني ذلك الحفاظ على النواحي التكنولوجيّة الأساسيّة للعملة المستعملة وتجديدها لتحمل اسماً جديداً. ونشير إلى أنّ هذا الإعداد مختلف عن استعمال البتكوين أو أيّ عملة افتراضيّة أخرى. فقد تكون البرمجيّات نفسها، لكنها تستخدم كخدمة إلكترونية منفصلة (أما لدى تعديل العملة الافتراضيّة، فقد تستخدم الجهة الفاعلة غير الحكوميّة بالفعل البتكوين أو أيّ عملة افتراضيّة مستعملة أخرى). الكثير من العملات الافتراضيّة الموجودة قد عدلت أو شكلت إمتدادات لبتكوين (راجع الفصل الثاني للمزيد من المعلومات). وفي بعض الحالات، يتطلب خلق عملة افتراضيّة جديدة قدرات إلكترونيّة بسيطة جداً بما أنّه تتوافر خدمات على الإنترنت تروّج لخدمات خلق عملة افتراضيّة. ويحتمل حصول مشكلة وهي أنّه قد يترتب عن استعمال برمجيّات قديمة وجود نقاط الضعف الإلكترونيّة التي تحتوي عليها تلك البرمجيّات.

---

[3] راجع براين كريبز، "الوداع الحقيقي: إستعمال تروكربت ليس آمناً"، Krebsonsecurity.com، 14 أيار 2014.

[4] راجع مثلاً كاسبرسكي لابز Kaspersky Labs، "الهجمات المستهدفة لصقور الصحراء"، النسخة الثانية، طبعة الشركة، موسكو: كاسبرسكي لابز، 2015.

[5] راجع مثلاً ريكوردد فيوتشر Recorded Future، "كيف تستخدم القاعدة التشفير بعد سنودن (الجزء الأول)"، دراسة من نشر المؤلّف، 8 أيار 2014a، "وكيف تستخدم القاعدة التشفير بعد سنودن (الجزء الثاني) – تحليل جديد بالتعاون مع ريفرسينغ لابز ReversingLabs"، دراسة من نشر المؤلّف، 1 آب 2014b.

نشر عملة افتراضيّة على المستوى الماديّ

يشكّل النشر الماديّ تحديّاً بارزاً آخر في نشر أيّ عملة افتراضيّة. ويعني النشر الماديّ تحديد الوسيلة التي يتعامل بها المواطن العاديّ مع البائع في حيه السكني. وفيما قد يكون الحاسوب كافياً للقيام ببعض عمليّات تحويل العملة الافتراضيّة، سيحتاج مستخدمو العملة الافتراضيّة، لإتاحة التحويلات اليوميّة، إلى عدد أكبر من الأجهزة المحمولة التي تتمّ من خلالها عمليّات التحويل. وعلى عكس عمليّات تحويل العملة الورقيّة، تشكّل تركيبة هذه التحويلات المعقّدة الحاسوبيّة عائقاً بارزاً أمام النشر لأنّ المستخدم العاديّ قد لا يملك الوسائل الماديّة المستعملة التي تخوّله أن يقوم بعمليّات التحويل اليوميّة.

من جهة، إنّ الحل الأسهل لهذه المشكلة يكمن في استخدام الهواتف الذكيّة، بما أنّها تتمتع أصلاً بقدرات بارزة للحوسبة والتواصل. فعلى سبيل المثال، تملك البتكوين تطبيقات محتملة كثيرة على الهواتف الذكيّة يمكن استعمالها لإتمام عمليّات التحويل[6]. إن استعمال الهواتف الذكيّة لإتمام عمليّات تحويل العملة الافتراضيّة ليس تماماً بجديد، وبالفعل، يستخدم الكثير من البائعين في البلدان المتقدّمة هواتفهم الذكيّة (أو ألواحهم) من ذي قبل في عمليّات تحويل العملة إلى البطاقة الإئتمانيّة من خلال تطبيقات مثل سكوير[7].

يشكّل الاعتماد على نظام عملات قائم على الهواتف الذكيّة دون سواها أو بشكل أساسيّ تحديّاً لأسباب عدة. فتكمن المشكلة الكبرى في أنّ إنشاء عملة مستعملة على الهاتف الذكيّ يتطلّب هاتفاً ذكيّاً أو ما يعادله لكل شخص يقوم بعمليّة تحويل، وهي فرضيّة غير واقعيّة حالياً في أيّ بلد فكيف بالأجدى في البلدان النامية. أما المشكلة الأخرى فهي أنّه إذا كان تصميم العملة يقوم على الهواتف الذكيّة دون سواها أو على أيّ جهاز منفرد، يصبح المستخدم عرضة لسرقة العملة إذا سرق الجهاز. وفي حالة العملات الافتراضيّة التي خلقت حاليّاً، تسمح سرقة كلمة السرّ التي تسهّل الوصول إلى المحفظة الإلكترونيّة أو التطبيق بسرقة كل العملة المرتبطة بكلمة السرّ هذه. وعلى خلاف ذلك، في حالة العملة الماديّة، تقتصر السرقة بشكل عام على المال النقديّ المتوفر في اليد أو على الحدّ المسموح به لسحب المال من الصرّاف الآليّ أو على انحصارات أخرى كإلغاء الشيك الشخصي قبل استعماله[8]. وبالتالي، ستستفيد كثيراً أيّ عملة افتراضيّة يصل إليها

---

[6] راجع مثلاً بتكوين، "إختر محفظتك من بتكوين"، غير مؤرّخ.

[7] راجع Square، الصفحة الرئيسة، غير مؤرّخ.

[8] نفترض هنا أنّ عمليّات تحويل العملات الإفتراضيّة "لا يمكن إلغاؤها"، أي أنّه عندما تتمّ العمليّات، لا يمكن إبطالها. في الحقيقة، عدم القدرة على الإلغاء هي نموذجيّاً الحال للعملات الإفتراضيّة اللامركزية (ولا سيما لبتكوين). ويمكن الإلغاء تقنياً إذ كانت العملة الإفتراضيّة لامركزيّة أو نصف مركزيّة. قد لا تصبح السرقة مشكلة مصيريّة مع تطبيق القانون المنظم، على الرغم من أنّه قد يكون غير مناسب إلى حدّ كبير.

عدد محدود من الأجهزة من آليات الأمن المتطورة، كالتحقق من البيانات البيومتريّة (الذي تستخدمه آبل باي[9] (Apple Pay) أو أيّ تصديق آخر متعدد العوامل (كتطلّب صلة بلوتوث بين هاتف وجهاز إضافي مطلوب كلازمة للعملة الرقمية الإلكترونيّة)[10] حيث يتيح مستوى أعلى من الأمان أو من قدرات إلغاء الاعتماد.

لا يشكّل استعمال الهواتف الذكيّة الوسيلة الوحيدة للقيام بعمليّات تحويل رقميّة. وبالفعل، كان نظام تحويل العملة الأفريقي (المعياري) M–PESA يستخدم هواتف غير ذكيّة (أي "حمقاء") لسنوات عدة[11]. ومن الممكن القيام بعمليّات تحويل العملة الافتراضيّة المستعملة عبر هواتف مماثلة من خلال استعمال الرسائل النصيّة[12]، لكنّ هذه الأنظمة تستخدم بشكل أساسيّ خادماً مركزيّاً موثوقاً به للحفاظ على المحفظة. ونظراً لدرجة الثقة العالية المطلوبة في موفّر الخدمة، من غير الواضح ما إذا كان اعتماد عملة افتراضيّة مع إعداد ممثال سيعود لمسائل ثقة على الأرجح. في المبدأ، يمكن إنشاء تطبيق محفظة للهواتف غير الذكيّة، على الرغم من أنّه يصعب تثبيت تطبيق مماثل بطريقة واسعة، بما أن الهواتف المماثلة ليست عادة مجهّزة لعمليّات تثبيت مماثلة عن بعد (تشكّل تطبيقات المحفظة تحدي أمن للهواتف الذكيّة نظراً لخصائصها؛ راجع القسم الذي يتناول التهديدات الإلكترونيّة التي تواجهها العملات الافتراضيّة لاحقاً في هذا الفصل).

وفي الوقت عينه، تتوافر أدلّة عن ازدياد استعمال الهواتف النقّالة (وليس الهواتف الذكيّة فحسب) للقيام بالعمليّات الماليّة، ولا سيما في أفريقيا (راجع الشكل 1–4). ويعود جزء كبير من هذه الشعبية، ولا سيما في كينيا، إلى اعتماد خطة تحويل المال الخاصّة بخدمة M–PESA، كما ذكر أعلاه.

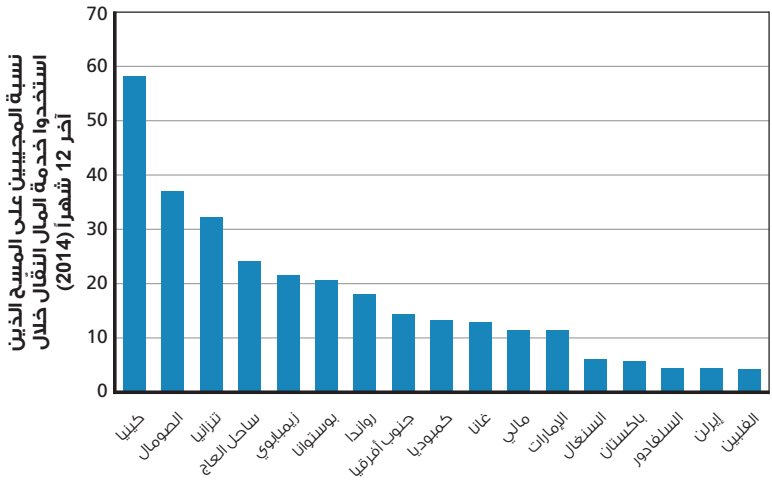
---

[9] راجع آبل، نظام حماية iOS و iOS 9 وما بعده، أيلول 2015.

[10] راجع Only Coin الصفحة الرئيسة، غير مؤرّخ.

[11] راجع وليام جاك وتفنيت سوري، إقتصاديّات أم بيسا The Economics of M–PESA، النسخة الثانية، دراسة من نشر المؤلّف، آب 2010/ واغناسيو ماس ودان رادكليف "إنتشار الدفع عبر الإنترنت أم بيسا في كينيا"، الموقع الإلكترونيّ للبنك الدولي أذار 2010. أم بيسا مختلفة كليّاً عن العملات الإفتراضية المعنيّة هنا إذ إنّها وسيلة للتحويل أكثر مما هي عملة. يشتري المستخدم العملة من بائعين طبيعيين ويحولون العملة من خلال رسائل نصيّة. ويكون الهاتف الخلوي للمزود موضع ثقة لإتمام العملية. في حال كان جهة غير حكومية تحاول نشر عملة إفتراضيّة في بيئة محظورة، قد لا تنجح هذه البنية لأنّها عرضة لعدة نقاط هجوم (مزوّد خدمة الخلويّ الوحيد، التجار التقليديون).

الشكل 1–4
استعمال الهواتف النقّالة لتسديد المدفوعات



RAND RR4.1-1231

المصدر: البنك الدولي، قاعدة بيانات التضمين المالي

يبيّن الشكل 1–4 أن استعمال الهواتف النقّالة لتسديد المدفوعات لا يقتصر على أفريقيا: فإن نسبة 13 في المئة من الكمبوديين ونسبة 12 في المئة من الإماراتيين ونسبة 6 في المئة من الباكستانيين ونسبة 4 في المئة من الإيرانيين أنها استعملت خدمات تحويل المال على الهواتف النقّالة في غضون 12 شهراً في العام 2014. تجدر الإشارة إلى أنّ البيانات في الشكل 1–4 تقتصر على عمليّات الدفع على الهاتف النقّال التي تتمّ عبر خدمات ماليّة على الهاتف النقّال؛ وتختلف عمليّات الدفع هذه عن عمليّات الدفع النقّال التي تتمّ بواسطة مؤسسات ماليّة قائمة (كالمصارف)، وبالتالي يجب النظر إليها على أنّها الحدود الدنيا لاستعمال الهواتف النقّالة للقيام بالعمليّات المالية. ونتيجة لذلك، يجب اعتبار أنّ استعمال الهواتف النقّالة للقيام بعمليّات تحويل العملات الافتراضيّة اليوميّة قابل للتنفيذ، في المستقبل بصورة خاصّة.

[12] راجع سلسلة الكتل، "إرسال من خلال: أرسل بتكوين مستخدماً البريد الإلكتروني والرسائل النصيّة" غير مؤرّخ (c).

تتوافر وسائل أخرى للقيام بعمليّات تحويل العملة الافتراضيّة تتخطّى الهواتف النقّالة، لكنّها تتطلّب أجهزة إضافيّة، مثل أجهزة اليو. أس. بي. (USB) أو البطاقات الذكيّة[13]. وهذا يتطلّب توزيعاً واسع النطاق لهذه الأجهزة من قبل جهة غير حكوميّة، مما يشكّل زيادة كبيرة في صعوبة نشر العملة الافتراضيّة من ناحية تمرين الفضاء الإلكترونيّ البحت[14]. بالإضافة إلى ذلك، قد تكون هذه الأجهزة عرضة لهجمات سلسلة التوريد التي تستهدف أمن شبكات الإمداد من قبل خصم ملمّ إلكترونياً (والذي نشير إليه بالمستوى الخامس أو المستوى السادس على النحو المبيّن في تقرير فرقة العمل: الأنظمة العسكريّة المرنة والتهديد الإلكترونيّ المتقدّم، الصادر عن مجلس علوم الدفاع في 2013؛ راجع "التهديدات الإلكترونيّة للعملة الافتراضيّة" أدناه، وكذلك الملحق (أ) لمزيد من المعلومات.

تحديّات النشر التي تواجهها العملات الافتراضيّة اللامركزيّة

في هذا الإطار، ستواجه جهة فاعلة غير حكوميّة تحدياً آخر تجاه نشر عملة افتراضيّة لامركزيّة يتمثّل بكيفيّة تحفيز عمليّات التنقيب التي تضمّ العنصر الأمنيّ الرئيس لجميع العملات الافتراضيّة اللامركزيّة الموجودة[15]. وعليه، إذا كان لدى الجهة الفاعلة غير الحكوميّة سمعة عالميّة سيّئة كالدولة الاسلاميّة في العراق والشام، سيقوم أفراد من جميع أنحاء العالم بتجنّب عمليّة التنقيب عن عملتها (إذا افترضنا مثلاً أنّ ايسلكوين (ISIL–Coin) هي العملة الافتراضيّة للدولة الإسلاميّة في بلاد الشام). في الواقع، قد يكون مثل هذا التنقيب غير قانونيّ في العديد من البلدان في ظلّ قوانين مكافحة الإرهاب. بذلك إذا كان المنقبون أقلّ تنوعاً من الناحية الجغرافيّة، من المحتمل أن يشكّل هذا تحدياً من منظور أمني لأنّه سيكون من السهل إستهدافهم. من ناحية أخرى، فإنّ التنوّع الجغرافيّ في مجتمعات الشتات قد يخفف من حدّة هذه المسألة. وكذلك إذا كان يتمّ التعامل مع العملة فقط في موقع جغرافيّ ثابت (على سبيل المثال، العراق وسوريا لأيسلكوين) ومنقّبين غير متقاربين جغرافياً، سيتمّ منعهم من التنقيب بسبب قلّة استخدامهم للعملة. باختصار، إن أحد الحلول لهذه المسألة هو التأكد من أنّ العملات الافتراضيّة تستحقّ الجهد لاستخدامها في

---

[13] راجع بتكوين، غير مؤرّخ (a)، وبتكوين ويكي، "محفظة الأجهزة"، 15 آب 2015.

[14] وهناك بعض الأدلّة على أنّ الدولة الإسلاميّة في العراق والشام قد نشرت بطاقة هويّة مع شريحة، على الرغم من أنّ هذه البطاقة ستكون أقلّ تطوراً من البطاقة الذكيّة التي تتضمن قدرات حوسبة تشفيريّة. راجع، على سبيل المثال، آرييتا لآيكا، "الدولة الإسلاميّة تتلقّى طعنة في الشرعيّة مع بطاقات الهويّة المزعومة بينما تفقد قواتها الأراضي التي كانت تسيطر عليها في العراق"، شبكة أخبار (Vice News) على الإنترنت، نيسان 2015.

[15] إذا كانت العملة لامركزيّة ولكن ليست مسكوكة، يجب ايجاد وسائل بديلة لتحفيز الأمن.

العمليّات عبر الإنترنت، ولكنّ هذا يثير تحديّات إضافيّة، ليس أقلّها هو أنّ بعض العملات الافتراضيّة المستعملة أصلاً يمكن أن يكون لها عذرها لمهاجمة العملات الافتراضيّة الحديثة (ولمزيد من الشرح لهذه الفكرة، راجع المقطع أدناه بشأن التهديدات الإلكترونية للعملات الافتراضيّة).

هناك وسائل أخرى لحوافز التنقيب. وأحدها هو أن يكون أداء عمليّة التنقيب للصالح العام، مما قد يشجع على نطاق واسع مجموعة من المستخدمين للتنقيب حتى لو لم يتعاملوا بالعملة. ومثال على ذلك العملة الرقميّة المشفّرة الجديدة برايم كوين (PrimeCoin)، حيث يتمّ التفتيش عن الأعداد الأوليّة في عمليّة التنقيب، على الرغم من عدم وضوح ما إذا كان المستخدمون يشعرون بأنّ المصلحة العامة تفوق الدعم المقدم من الكيان الراعي[16]. هناك تقنية أخرى لتحفيز التنقيب هي دمج التنقيب التي تضمّن أساساً التنقيب عن العملة الافتراضيّة الجديدة ضمن عملية التنقيب عن البتكوين. ولكنّ المشكلة مع مثل هذه العملية هو إمكانية أن تختار إدارة بتكوين تغيير القواعد من أجل عدم السماح بحدوث هذا التضمين (إذ من المفترض أن المنقّبين عن بتكوين لا ينظرون إلى تمويل الإرهاب بشكل إيجابيّ، إذا كانت تلك النظرة هي التي يُنظر بها عموماً الى الجهة الفاعلة غير الحكوميّة). فتغيير القواعد من بتكوين من شأنه أن يسبب إنهيار العملة.[17]

العملات الافتراضية، تبنّيها وقيمتها

في هذا الشأن، يتمثّل التحدي الرئيس لنشر عملة افتراضيّة في كيفيّة إنشاء مثيل للعملة الافتراضيّة، أي الإنتقال من صفر مستخدمين إلى المجتمع بأكمله داخل المنطقة الجغرافيّة التي تهمّ الجهة الفاعلة غير الحكوميّة. في الواقع، عملت بتكوين لأربع سنوات لكسب أيّ

---

[16] وكمثال آخر، راجع صني كينغ (Sunny King)، "برايمكوين (Primecoin): عملة مشفّرة برقم أوّلي مع إثبات العمل"، دراسة من نشر المؤلّف، 7 تموز 2013.

[17] راجع بونو وغيره، العام 2015، لمزيد من المناقشة. بما أنّ عمليّة تبني قوانين بتكوين هي عمليّة غير مركزيّة إلى حدّ كبير، يستحق إنفاذ مثل هذا التضمين المحظور المزيد من الدراسة.

[18] راجع سلسلة الكتل، "الرسملة السوقية"، غير مؤرخ (b).

[19] على سبيل المثال، اعتباراً من حزيران 2015، 41 فقط من أصل 514 عملة إفتراضيّة مدرجة حصلت على رسملة سوقيّة بقيمة أكثر من مليون دولار أمريكي؛ ثماني عملات إفتراضيّة حصلت على رسملة سوقية بقيمة أكثر من 10 ملايين دولار أمريكي؛ وثلاث عملات إفتراضيّة حصلت على رسملة سوقيّة بقيمة أكثر من 100 مليون دولار أمريكي؛ تراجع تصنيفات القيمة السوقيّة للعملات المشفّرة (CoinMarketCap)، 2015 (a).

قيمة بارزة كعملة[18]، ومن الواضح أنّ الغالبيّة العظمى من عمليّات نشر العملة الافتراضيّة تفشل في كسب القبول[19].

في الواقع، إنّ أفضل وقت لإستهداف عملة افتراضيّة ما هو في فترة إنطلاقتها الأولى حيث تكون الثقة في العملة في حدّها الأدنى بالإضافة إلى أنّ مهارة المدافعين الإلكترونييّن قد تكون أيضاً في أدنى مستوى على الإطلاق وأنّ الحساسية العامة لجهة إستقرار ونجاح العملة قد تكون مرتفعة جداً. ونتيجة لذلك، قد يكون هذا الوقت الأفضل لمحاولة عرقلة تداول العملة و/أو الحطّ من ثقة مستخدم العملة الافتراضيّة من أجل منع نجاح نشرها.

ويُضاف إلى ما سبق وجود إستراتيجيّة محتملة للتخفيف من هذه المسألة وهي دعم العملة الافتراضيّة الجديدة بعملة افتراضيّة موجودة من قبل[20] أو عملة ورقيّة أو سلعة أساسيّة لترسيخ قيمة العملة الافتراضيّة. وعلى وجه الخصوص، إذا حصلت الجهة الفاعلة غير الحكوميّة على دعم من الدولة القوميّة، يمكن تحديد قيمة العملة الافتراضيّة بسعر صرف ثابت بعملة الدولة القوميّة (أو بسلع أساسيّة تملكها الدولة القوميّة). لكن تستلزم هذه الإستراتيجيّة التخلّي عن السيطرة الاقتصاديّة على العملة الافتراضيّة، وبالتالي مقايضة السرعة التي يتمّ بها قبول العملة الافتراضيّة بمنافع النشر السياسيّة و/أو الاقتصاديّة.

ضمان المجهولية في استخدام العملة

يبحث هذا القسم في الدرجة التي يمكن بها للعملات الافتراضيّة توفير مجهولية كافية لمستخدميها، وأيضاً كم هو صعب إزالة مجهولية بعض عمليّات العملة الافتراضيّة، وأيّ مستوى من الإلمام لدى المستخدم قد يكون مطلوباً من أجل ضمان مجهولية كافية. نركّز

---

[20] راجع بونو وغيره، 2015، لمزيد من المناقشة، وخاصة في ما يتعلّق بتقنيّة ربط السلاسل (pegged side chains) وكذلك التفرُّع من بتكوين. هذا الربط بعملة إفتراضيّة سابقة قد يحلّ أيضاً مشكلة التنقيب لأن جميع عمليات التنقيب يمكن أن تتمّ بالعملة الإفتراضيّة المستعملة (مثلاً البتكوين)، ومن ثم تبدّل بالعملة الإفتراضيّة الجديدة. مثال واحد على العملة التي يتم تنقيبها واستخراجها بهذه الطريقة هو زيروكاش (Zerocash) ايلي بن ساسون (Eli Ben-Sasson)، اليساندرو كييزا (Alessandro Chiesa)، كريستينا غارمان (Christina Garman)، ماثيو غرين(Matthew Green)، إيان مايرز (Ian Miers)، إران ترومر (Eran Tromer)، ومادارز فيرزا (Madars Virza)، زيروكاش: دفعات مغفلة لامركزيّة من بتكوين" دراسة قدّمت في ندوة معهد مهندسي الكهرباء والإلكترونيّات 2014 بشأن الأمن والخصوصيّة، سان خوسيه، كاليفورنيا، 18-21 أيار 2014 a)، حيث أنّه يمكن الإعتماد على "معيار" ألتكوين الأساسي وبعد ذلك يبنى عليه.

على البتكوين ومسائل المجهولية المتعلّقة بها، ولكن أيضاً سنقوم ببحث كيف أنّ العملات الافتراضيّة الجديدة والتقنيّة المرتبطة بها قد تكون قادرة على زيادة مجهولية المستخدم بشكل كبير.

إنّ التحقق من مجهولية عملة افتراضيّة أمر بالغ الأهمية لأنّ المجهولية هي إحدى أهم خصائص أيّ عملة، ما يعني تحديداً أنّ لا المشتري ولا البائع يحتاج الى معرفة تاريخها[21]. وبينما ينصبّ معظم التركيز على العملة الافتراضيّة على مجهولية بعض التحويلات غير المشروعة (مما يجعلها غير قابلة للتعقّب من قبل المؤسسات العسكريّة أو المنظّمات المكلّفة بإنفاذ القانون و/أو المنظّمات الاستخباريّة) تنشأ مسائل أخرى من استخدام عملة افتراضيّة باعتبارها وسيلة يوميّة للتحويل. لذا، من دون مجهولية كافية، يحجم المستخدمون اليوميّون بشدّة عن استخدامهم أيّ عملة افتراضيّة في العمليّات الاقتصاديّة اليوميّة نظراً للإنتهاكات الخطيرة المحتملة للخصوصيّة. تجدر الملاحظة هنا إلى أنّ "المجهولية" مفهوم واسع، وأنّ هجمات إزالة المجهولية تتراوح بين هجمات ذات إلمام عال لإزالة مجهولية مستخدم واحد وهجمات قراصنة تتطلّب القليل من الجهد والإلمام لإزالة مجهولية مجموعات واسعة من الأفراد.

تتضمّن الأقسام التالية أولاً بحثاً عن المفاضلة في مجهولية عملة افتراضيّة مقابل مركزيّة سلطة عملة افتراضيّة. ثم نبحث الحالة الخاصّة للبتكوين بصفتها العملة الافتراضيّة الأكثر نشراً والتي كانت موضع معظم الأبحاث. وأخيراً، نبحث في تقنيّات أخرى لبتكوين وفي عملات افتراضيّة أجدّ يمكن أن توفّر مستويات كافية للمجهولية.

المجهولية مقابل مركزيّة العملات الافتراضيّة

وكما أشرنا أعلاه، إنّ تأكيد مجهولية مستخدم يوميّ هي مسألة مختلفة عن ضمان المجهولية من الحكومة بواسطة مجموعات متمكّنة وملمّة تقنيّاً. ولكن من الناحية العمليّة، لا تقوم كل العملات الافتراضيّة بهذا التمييز. بالنسبة إلى العملات الافتراضيّة اللامركزيّة،

---

[21] راجع كينيث روجوف (Kenneth Rogoff)، "تكاليف وفوائد التخلص التدريجي من العملة الورقيّة"، المكتب الوطني للبحوث الاقتصادية (NBER) مؤتمر الإقتصاد الكلّي السنويّ 2014، المجلّد. 29، 2015، ص. 456–445. وتواصل الدراسة: "لا يوجد شيء في النظريّات القياسيّة عن الأموال التي تتطلب معاملات مغفلة من سلطات الضرائب أو إنفاذ القانون. ولكن مع ذلك يوجد مجموعة مهمة من الأدلّة تشير إلى أنّ نسبة كبيرة من العملات في معظم البلدان، وعموماً أكثر من 50 في المئة، تستخدم على وجه التحديد لإخفاء المعاملات".

المسألتان متلازمتان حاليّاً لأنّ تمييز مصدر الهجوم والإلمام ليس موجود كمعيار تصميميّ ضمن البنية التحتيّة المركزيّة. في إطار السلطة المركزيّة للعملة الافتراضيّة جرى عمل الكثير لمناقشة كيفيّة القيام بهذا التمييز[22]، ولكن من الناحية العمليّة، فإنّ العديد من العملات الافتراضيّة المركزيّة، مثل نظام دفع الأموال وتحويلها ونظام الدفع عبر الإنترنت ونظام تأمين إرسال الدفعات الماليّة واستقبالها[23] يقوم أيضاً بحماية هويّات المستخدمين من التحقيقات الحكوميّة مثلاً (على الرغم من أنّ سلطات العملات الافتراضيّة المركزيّة يجب أن تكون محلّ ثقة للقيام بذلك، وحيث أنّ العملات الافتراضيّة المشفّرة تحاول أن تبني أمنها على البراهين الرياضيّة). ولا بدّ من الملاحظة هنا أنّ هذه العملات الافتراضيّة هي بالضبط المستهدفة من قِبل الحكومات لأنّها تحاول توفير هذه المجهولية ولكنّها في ذات الوقت عرضة للهجوم بسبب تصميمها المركزيّ (محفِّزة بذلك حالة العملات الافتراضيّة اللامركزيّة) [24]. وبما أنّ العملات الافتراضيّة شبه المركزيّة غير شائعة، من الصعب تقييمها. إنّ أفضل عملة افتراضيّة شبه مركزيّة معروفة هي ريبل (Ripple) إذ إنّها ليست مصممة لتكون ذات استعمال خاص لأنّ توجهها هو نحو المؤسسات الماليّة بدلاً من الأفراد[25]. وفي الوقت عينه، جرى نقاش في دراسات التشفير عن كون العملات الافتراضيّة شبه المركزيّة أفضل وسيلة للمضيّ قدماً في الحفاظ على الأمن والخصوصيّة

---

[22] وقد بدأت هيئة العمل من قبل تشوم (Chaum، 1983) وهي مستمرّة بعملها حتى اليوم. هذه المخططات تعتمد عادة على بعض الأفكار من طرف ثالث موثوق به، تسعى العملات الإفتراضيّة إلى تجنّبه.

[23] راجع Perfect Money، الصفحة الرئيسة، غير مؤرّخ، ونظام WebMoney، الصفحة الرئيسة، غير مؤرّخ. راجع أيضاً براين كريبس (Brian Kerbs)، "حكومة الولايات المتحدة الأمريكية تستولي على موقع LibertyReserve.com،" موقع KrebsonSecurity.com، 13 أيار 2013.

[24] راجع، على سبيل المثال، الولايات المتحدة الأمريكية ضد نظام 13 ،Liberty reserve القانون الجنائي 368 (CRIM368) المحكمة المحليّة لجنوبي نيويورك 2013 (2013 .S.D.N.Y)، ووزارة العدل، مكتب المدعي العام الأمريكي، المنطقة الجنوبية من نيويورك، "لائحة الإتهام والوثائق الداعمة: الولايات المتحدة ضدّ Liberty reserve وغيرها" 28 أيار 2013.

[25] كما جاء في موقع Ripple فقرة الأسئلة المتكرّرة: "إنّ المجهولية ليست هدفاً تصميميّاً لريبل. ومع ذلك، ينبغي على ريبل أن توفر حماية للخصوصيّة كافية بالنسبة لمعظم الناس." راجع ريبل، غير مؤرخ (a).

[26] راجع الدفراوي ولامبكنز (Lampkins and Defrawy)، 2014. العملة الرقمية البديلة التكوين داش alt–coin Dash (سابقاً Darkcoin) قد يُنظر إليها على أنّها شبه مركزيّة في بعض النواحي بسبب تركيب ماسترنود (Masternode)، ولكنّ هذا أساساً هو لأغراض المجهولية ويتم تنفيذ المهام الأخرى للعملة قياساً بالعملة الرقميّة الإلكترونيّة. راجع أيضاً داش (Dash)، غير مؤرّخ (b).

للأفراد بينما تتيح المجال في الوقت عينه للحكومة لوضع أنظمتها، ولكن لم يتمّ بعد نشر مثل تلك العملة الافتراضيّة[26].

"المجهولية": دراسة حالة بتكوين

من أجل البحث في مدى مجهولية عملة افتراضيّة ما، سنأخذ في الإعتبار حالة البتكوين. يمكن مراجعة الفصل الثاني للإطلاع على الأساسيّات الفنيّة لبتكوين. ومن حيث المبدأ، إنّ بتكوين هو اسم مستعار لأنّ كل مستخدِم يتمثل بسلسلة أرقام عشوائيّة متولّدة بالتشفير، تدعى عنوان، بحيث لا تتكشف الهويّة الحقيقيّة للمستخدم. على أية حال، إذا لم يغيّر المستخدم عنوانه عند الإنتقال من عمليّة إلى أخرى، حينها يصبح تاريخ العمليّات بأكمله علنيّاً لأيّ شخص يعرف عنوان بتكوين المستخدم. وذلك لأنّ سلسلة كتل البتكوين، أي دفتر الحسابات العام، هو السجل العام لكل العمليّات التي تمّت في أيّ وقت مضى. لذلك، إنّ تكرار عمليّات البتكوين باستخدام العنوان عينه يشكّل خطراً جديّاً على المجهولية. تجدر الإشارة هنا إلى أنّ عنوان البتكوين يمكن أن يصبح معروفاً من قبل الكثيرين في سياق عمليّات عاديّة من قبل أيّ شخص يتعامل مع المستخدم، مثل أصحاب المحلات وشركات تمّ التسديد لها، وأصدقاء حُوِّلت أموال إليهم، وما الى ذلك[27]. وبعبارة أخرى، إنّ البتكوين مغفلة بمعنى أنّ كل عمليّة مصرفيّة وكل رصيد حساب مصرفيّ معروف لأيّ شخص لديه إتصال بالإنترنت، والمعلومات الوحيدة التي تبقى مجهولة هي هويّة مالك كل حساب مصرفيّ، وهو ما يمكن الإستدلال عليه من تفاعلات المستخدم.

ومن الواضح أنّ المجهولية هذه غير مقبولة في الحياة الاقتصاديّة اليوميّة، وبالتالي يجب تكوين ضمانات إضافيّة [28]. بالنسبة إلى الكثير من العملات الافتراضيّة الحاليّة (إن لم يكن معظمها) بما في ذلك بتكوين، تتطلب العمليّات الحاليّة للحفاظ على المجهولية

---

[27] على وجه الخصوص، إذا قامت منظّمة غير مشروعة في محاولة لجمع التبرّعات عبر بتكوين بنشر عنوانها من أجل الإستحصال على الأموال، ستصبح سلسلة الكتل سجلّاً عامّاً دائماً للاسم المستعار لأيّ مستخدم أعطى المال لتلك المنظّمة، إلّا إذا استخدم المتبرّعون نوعاً من الأجهزة المتقدمة؛ راجع الفقرات الآتية لمعرفة المزيد عن هذا الموضوع.

[28] في الواقع، تقول مؤسّسة بتكوين (بتكوين، "بعض الأشياء التي تحتاج إلى معرفتها"، غير مؤرّخ [ج]) تقول ما يلي:

> بتكوين ليست مغفلة. المطلوب هو بعض الجهد لحماية خصوصيّتك مع بتكوين ويتمّ تخزين كافة العمليّات الخاصّة بتكوين علناً وبشكل دائم على الشبكة، ممّا يعني أنّه يمكن لأيّ شخص أن يرى الرصيد والعمليات من أيّ عنوان للبتكوين. ومع ذلك، فإنّ هويّة المستخدم وراء أيّ عنوان تبقى مجهولة حتى يتمّ كشف المعلومات في خلال عمليّة شراء أو في ظروف أخرى. وهذا هو أحد الأسباب التي تتطلّب إستخدام عناوين بتكوين مرّة واحدة فحسب. نذكّر دائماً أنه من مسؤوليتك إعتماد ممارسات جيّدة من أجل حماية خصوصيّتك.

إلى تعلّم التشغيليّ الإلكترونيّ أو "التقنيّات" للوصول إلى درجة الأمان المطلوبة والتي تبدو غير ممكنة واقعيّاً بالنسبة إلى الشخص العاديّ. وفي الأقسام التالية سوف نبحث في وسائل إحقاق مجهولية بتكوين كممثلة للعملات الافتراضيّة الأخرى لسببين: أولاً، إنّ بتكوين هي أكثر العملات الافتراضيّة شعبيّة وبذلاً للجهود لحماية المعلومات. ثانياً، تم بناء الكثير من العملات الافتراضيّة باستخدام بتكوين أساساً لها، وبالتالي يمكن تطبيق العديد من الجهود المبذولة لتحقيق مجهولية البتكوين على عملات افتراضيّة أخرى.

تضمّ مجهولية بتكوين جانبين هما مجهولية العمليّات الفرديّة ومجهولية أنماط العمليّات. يتمّ ضمان مجهولية العمليّات الفرديّة في الغالب عن طريق تعيين اسم مستعار عشوائيّ لكل فرد. ولكن حتى مع هذا الاسم المستعار، يمكن تحديد العمليّة الفرديّة عن طريق فحص عناوين بروتوكول الإنترنت للمستخدمين، مما يكشف تاريخ صفقة المستخدم بالكامل. وفقاً لذلك، يمكن استخدام تقنيّات لإخفاء بروتوكول الإنترنت إذا كانت المجهولية الهدف المنشود. لذلك توصي مؤسسة بتكوين باستخدام هذه التقنيّات، وتذكر بالتحديد مشروع تور لحماية الخصوصيّة[29]. إنّ إحقاق المجهولية باستخدام بتكوين مع تور هو موضوع نقاش، فالأبحاث الحديثة تشير إلى أنّ إزالة المجهولية عن مستخدمي بتكوين مع تور ممكنة نظراً إلى الطريقة الحاليّة التي صيغت بها بتكوين[30].

إنّ عمليّة الاسم المستعار، كما ذكر آنفاً، لا تحفظ في حدّ ذاتها المجهولية وعندما تتاح الفرصة للوصول إلى اسم مستعار لمستخدم آخر، يمكن لأيّ شخص رؤية جميع العمليّات والأرصدة المرتبطة بذلك الاسم المستعار. وفقاً لذلك، توصي بتكوين بتغيير الاسم المستعار بعد كل استخدام، على الرغم من أنها في الأصل لا تفرض هذه الممارسة[31]. وبالنسبة إلى عملة افتراضيّة منشورة للاستخدام اليوميّ من قبل أشخاص عاديين، على مثل هذه الإجراءات أن تكون مُدمجة (جزء من النظام ذاته).

بالإضافة إلى ذلك، أظهر مجتمع الأبحاث الأمنيّة القدرة على أداء تحليلات الحدّ من الخصوصيّة على مجمل سلسلة الكتل الخاصّة ببتكوين في محاولة للتعرّف على

---

[29] راجع بتكوين "إحمِ خصوصيّتك،" غير مؤرّخ (b). وبالنسبة لمشروع تور، تراجع الصفحة الرئيسة لمشروع تور، غير مؤرخ (c). أمن تور هو خارج نطاق هذا التقرير.

[30] لمزيد من التفاصيل، راجع أليكس بيريوكوف (Alex Biryukov) وإيفان بوستوغاروف (Ivan Pustogarov) "بتكوين عبر شبكة تور ليست فكرة سديدة"، دراسة قدّمت من خلال الندوة العالميّة التاسعة عشرة حول التشفير الماليّ وأمن البيانات لعام 2015، سان خوسيه، كاليفورنيا، 21–17 أيار 2015a.

[31] راجع بيريوكوف و بوستوغاروف، 2015a.

الأفراد فقط من نمط عمليّاتهم[32]. من أجل حلّ هذه المشكلة، وجد ما يسمّى بخلط الخدمات للتعتيم على هذه العمليّات؛ هذه الخدمات تكدّس العمليّات بحيث لا يمكن إقتفاء أثرها بسهولة لجهات فاعلة فرديّة. تشمل هذه الخدمات

تقنيّة المجهولية في عمليّات العملات الرقميّة "كوين جوين"[33] (CoinJoin) وبروتوكول تسهيل دفعات مغفلة من البتكوين وغيرها من العملات المشفّرة "ميكس كوين"[34] (Mixcoin) والمحفظة المظلمة [35] (Dark Wallet) والتي يبدو أنّها توفّر جميعاً مستوى كاف لتأمين مجهولية المستخدم. على الرغم من هذا، يبقى دائماً احتمال التهديد من التطورات المستقبليّة تجاه إزالة المجهولية وكشف العمليّات الماضية، حتى تلك التي تمّت سابقاً بإجراءات ملائمة لضمان المجهولية.

بعد أن بحثنا في مجهولية بتكوين، نركّز الآن على المجهولية المتزايدة التي وفّرتها ألتكوين المستعملة حالياً والمقترحة.

استخدام بعض عملات ألتكوين الجديدة في عمليّات مغفلة

تمّ تكوين بعض الألتكوين بهدف أساسيّ وهو أن تكون أكثر مجهولية من البتكوين. وقد تمّ تصميم عملة مشفّرة مفتوحة المصدر لإضافة خصوصيّة للعمليّات تدعى دارك

---

[32] راجع، على سبيل المثال، سارة مايكلجون (Sarah Meiklejohn)، مارجوري بومارول (Mar–jori Pomarole)، غرانت جوردان (Grant Jordan)، كيريل لفتشنكو (Kirill Levchenko)، دايمون ماكوي (Damon McCoy)، جيفري م. فولكر (Geoffrey M.Voelker)، وستيفان سافاج (Stefan Savage)، "حفنة من بتكوين: تحديد خصائص الدفعات بين أشخاص مجهولي الهويّة، "نتائج مؤتمر قياس الإنترنت لعام 2013، تشرين الأول 2013، الصفحات 140–127".

[33] راجع المنتدى حول بتكوين، "كوين جوين: خصوصيّة بتكوين للعالم الحقيقيّ"، خطّ نقاش بدأ في 22 آب b2013؛ موقع كوين جوين الإلكتروني، "مكامن الضعف في شيرد كوين"، غير مؤرّخ. لكنّ هناك إدّعاءات على أنّ كوين جوين ليست مغفلة كما كان يعتقد، راجع على سبيل المثال –http://www.coin joinsudoku.com ويظهر هذا البحث الحاجة الى تحليلات أكثر حذراً لتقنيّات جديدة تم الإعلان عنها على أنّها "معزّزة الخصوصيّة".

[34] راجع جوزيف بونو(Joseph Bonneau)، أرفيند نارايانان (Arvind Narayanan)، أندرو ميلر (Andrew Miller)، جيريمي كلارك (Jeremy Clark) وجوشوا أ. كرول (Joshua A. Kroll)، "ميكس كوين: مجهولية بتكوين مع خلط ذات مساءلة"، التشفير الماليّ وأمن البيانات: المؤتمر الدولي الثامن عشر، برلين: سبرينغر هايدلبرغ، 2014، الصفحات 504–486.

[35] راجع المحفظة المظلمة، غير مؤرّخ. هناك أدلّة على أن الإرهابيّن أو محبّيهم، هم على علم بالمحفظة المظلمة. راجع المنذر، 2014.

كوين (Darkcoin) مع خدمة خلط مدمجة تدعى داركسند (Darksend) والتي بدورها تعتمد على تقنيّة كوين جوين كونها التقنية الأساسيّة التي تستند إليها[36]. وبذلك يجب على جميع المستخدمين أن يشاركوا في الخلط حتى تصبح عمليّة إزالة المجهولية أكثر صعوبة، وهذه ميزة تتقدم بها على البتكوين[37]. إنّ زيروكاش[38] (Zerocash) والمتابع له زيروكوين[39] (Zerocoin) بُنيا باستخدام أدوات تشفير أكثر تقدماً[40]. على وجه الخصوص، زيروكاش الذي يعتمد على ما يسمى صفر معرفة– حجج مقتضبة للمعرفة (ZK–SNARKs)[41] وهي خوارزميات تشفير متقدّمة تغني عن الحاجة إلى بعض آليات توزيع التوافق على قيمة بتكوين وبالتالي فهي قادرة على إخفاء العمليّات الفعليّة لزيادة المجهولية [42]. وبعبارة أخرى، فإن نهج زيروكاش هو استخدام تقنيّات تشفير متقدّمة من

---

[36] راجع موقع Dash الإلكترونيّ، غير مؤرّخ (a).

[37] تدعى أحدث نسخة من دارك ساند هي دارك ساند+. لتقويم أمن دارك ساند+، راجع كريستوف أطلس (Kristov Atlas)، "دراسة تحليلية حول خصوصيّة سلسلة الكتل الخاصّة بدارك كوين عبر دارك ساند+"، مقال من نشر المؤلّف، 10 ايلول 2014، للإستجابة لهذا العمل، راجع نقاش Dash، "رد على بحث Kristov "، مقالة منشورة ذاتياً، 11 ايلول 2014.

[38] راجع مشروع Zerocash، الصفحة الرئيسة، غير مؤرخ. بن ساسون وآخرون (.Ben Sasson et al)، 2014a؛ وبن ساسون وآخرون القاعدة و. "زيروكاش: دفعات لامركزيّة مغفلة من بتكوين"، دراسة قدّمت في خلال ندوة الأمن والخصوصيّة على الإنترنت لعام 2014 التي نظّمتها جمعيّة مهندسي الكهرباء والإلكترونيات، سان خوسيه، كاليفورنيا، من 18 إلى 21 أيار[39]. 2014b راجع موقع Zerocash Project الإلكترونيّ، غير مؤرّخ.

[40] طُرحت عملة ألتكوين أخرى تدعى بينوكيو كوين (PinocchioCoin) وهي نسخة جديدة من زيرو كوين (Zerocoin) ولكن تستخدم تقنيّات تشفير مختلفة. راجع جورج دانزيس (George Danezis) وسيدريك فرونيه (Cédric Fournet) وماركولف كولويس (Markulf Kohlweiss) وبراين بارنو (Bryan Parno)، "بينوكيو كوين: بناء زيروكوين على أساس نظام إثبات مقتضب يستند إلى الإقران"، بيتشوب 2013 (PETShop 2013): نتائج أول ورشة عمل نظّمتها رابطة مكائن الحوسبة حول دعم اللغة لتكنولوجيّات تعزيز الخصوصيّة، نيويورك: رابطة مكائن الحوسبة، 2013، الصفحات 27 إلى 30.

[41] راجع ألي بن–ساسون (Eli Ben–Sasson) وأليساندرو كييزا(Alessandro Chiesa) وكريستينا غارمن (Christina Garman) وماثيو غرين (Matthew Green) وإيان مايرز (Ian Miers) وإيران ترومر (Eran Tromer) ومادارز فيرزا(Madars Virza)، "حجج مقتضبة للمعرفة لبرامج سي: التحقّق بإقتضاب من تطبيق البرنامج وبمعرفة منعدمة"، في طبعات رام كانيتي وخوان أ. غاراي، أوجه التقدّم في علم التشفير CRYPTO 2013: المؤتمر السنويّ الثالث والثلاثين لعلم التشفير، سانتا باربرا، كاليفورنيا، آب 2013، الصفحات 90 إلى 108.

[42] في المقابل، تعتمد بتكوين فقط على تفهم وظائف هاش المفهومة والمقبولة في مجتمع أمن الحاسوب (SHA–256) وعلى خطط التوقيع الرقميّ (EC–DSA).

أجل تأمين مجهولية المستخدمين إنّما أيضاً تأمين مجهولية العمليّات وأنماطها. لذلك من غير الواضح ما إذا كان سيتمّ اعتماد زيروكاش إذ إنّه حتى تاريخ كتابة هذا التقرير، لم يتمّ نشره بعد.

وجملة القول إنه من الصعب تقييم الأمن المطلق وقابليّة استخدام زيروكاش، إذ إنه لم يتمّ اختباره في بوتقة الاستخدام والتقييم في العالم الحقيقيّ، على الرغم من أنّ آلياته النظريّة لديها براهين أمنيّة أكثر صرامة من كل العملات الافتراضيّة المستعملة. خلافاً لذلك، فإنّ داش كوين (Dashcoin) مستخدمة حالياً ويبدو أنّها مغفلة إلى حدّ معقول (وبالتأكيد أكثر من استخدام بتكوين من دون تقنيّة إضافيّة لتعزيز الخصوصيّة)، على الرغم من أنّه مضى على وجودها عام واحد فقط حتى تاريخ كتابة هذا التقرير. إنّ رسملتها السوقيّة الحاليّة هي أقلّ بكثير من قيمة بتكوين، وبالتالي من الصعب إجراء مقارنة متساوية بينهما[43].

حتّى الآن، قمنا ببحث مجهولية العملة الافتراضيّة، وتبيّن في الحقيقة أنّ التهديدات التقنيّة التي تناولناها حتى الآن لا تتّسم نسبياً بالإلمام. في القسم التالي، سوف نبحث في التهديدات الإلكترونيّة على نطاق أوسع ونركّز بشكل خاصّ على كيفيّة تأثير مستوى الإلمام الإلكترونيّ لخصم ما على نجاح جهة فاعلة غير حكوميّة في نشر عملة افتراضيّة.

التهديدات الإلكترونية للعملات الافتراضيّة

إن أحد العناصر الأساسيّة في بحث إحتمال نجاح جهة غير حكوميّة في نشر عملة افتراضيّة هو مقدار الإلمام الإلكترونيّ المطلوب لإحباط مثل هذا النشر. في الواقع، إذا كانت الجهة الفاعلة دولة مثل الولايات المتحدة واستطاعت أن تقنع الجهة غير الحكوميّة بإمكانيّة منع نشر عملتها الافتراضيّة عبر الوسائل الإلكترونيّة، قد يتغيّر قرار حساب التفاضل والتكامل للجهة الفاعلة غير الحكوميّة لتبتعد بعيداً عن النشر. هناك نوعان من المخاوف ذات الصلة عند التفكير في كيفيّة التأثير على عمليّة إتخاذ القرار من قِبل جهات فاعلة غير حكوميّة لتحقيق هدفها بنشر عملة افتراضيّة. الأول، يمكن أن تتدهور ثقة العامة في العملة،

[43] إبتداءً من 22 شباط 2015، بلغت قيمة رسملة بتكوين السوقية $3,274,674,231، في حين بلغت القيمة السوقية لعملة داش (Darkcoin سابقاً) $12,885,950. راجع CoinMarket-Cap "رأسمال أسواق العملات المشفّرة،" 30 أيلول 2015 a.

وكذلك قيمة العملة، تدهوراً بالغاً إذا تمّ إختراق وكشف هوية عملة افتراضيّة بواسطة هجوم إلكترونيّ[44]. الثاني، قد تكون العملة الافتراضيّة هدفاً محتملاً ولا سيما بالنسبة للدولة القوميّة المتضررة وحلفائها، بما في ذلك الولايات المتحدة، وذلك لأنّه يُنظر إلى العملة الافتراضيّة على أنّها تهديد للأمن القوميّ، كما هو الحال عندما تقوّض عملة افتراضيّة العملات الرسميّة للدولة أو عندما تستخدم وسيلة لدعم المجرمين أو المجموعات الإرهابيّة. وبناءً على هذا الدافع، فإنّ هذا القسم سيُعنى بالبحث في التهديدات الإلكترونيّة للعملات الافتراضيّة بوصفها عملاً يحتاج إلمام بالتهديد الإلكترونيّ.

في النهاية، فإنّ جهة فاعلة غير حكوميّة، (وفي الواقع حتى جهة فاعلة حكوميّة) من شأنها مواجهة تحديّات كبيرة في حماية عملة افتراضيّة من هجمات إلكترونيّة مدمّرة ضد خصم عنيد وملمّ إلكترونياً. وعلى ذلك فإنّ حساب التفاضل والتكامل الرئيس من جانب الخصم هو في كمّ القدرات التي يريد الكشف عنها ومقدار الإستثمار المكرس من الوقت ومن العاملين من أجل ضمان هجوم ناجح.

قد تتراوح الهجمات المحتملة من مستوى منخفض (مثل قطع الخدمات الموزّعة (DDoS) إلى هجمات مصممة ببراعة (على سبيل المثال، هجمات ضدّ البنية التحتيّة الأساسية أو من خلال استغلال نقاط الضعف لشن هجوم فوريّ مباغت[45]. وينبغي أيضاً أن يلاحظ أنّ الهجمات قد تُشنّ من جانب معارضين من غير الدول القوميّة. لذا، إنّ سرقة العملة، كما حدث في هجوم البتكوين في العام 2014 ضد بورصة ماونت جوكس (Mt. Gox) [46] هو دافع واضح. وعند مناقشة التهديدات الإلكترونية، من المفيد أن يكون هناك

---

[44] على سبيل المثال، راجع تيموثي ب. لي (Timothy B. Lee)، "خلل كبير في شبكة بتكوين يحفّز المبيعات المكثّفة بأسعار زهيدة"؛ تنخفض الأسعار موقّتاً بنسبة 23 في المئة"، موقع أرس تكنيكا الإلكترونيّ، 11 آذار 2013.

[45] الهجوم الفوريّ المباغت هو الهجوم الذي يستفيد من نقاط ضعف البرامج التي يجهلها المطوّر والتي لا يوجد لها تصحيح. وفي حين أنّ هذا القسم سيناقش بعض الهجمات، راجع أيضاً بونو وغيره، 2015؛ أطلس، 2014. وبتكوين ويكي، "نقاط الضعف"، 8 تمّوز d2015، لإجراء مناقشات تفصيليّة أخرى عن هجمات معيّنة فضلاً عن التدابير المضادّة المحتملة.

[46] تفاصيل بشأن سرقة ما يقرب 400 مليون دولار أمريكي من بورصة ماونت جوكس لا تزال مستجدّة، وهناك خلاف حول أسباب الخسارة. وعلى الرغم من أنّ إدارة الشركة كانت على ما يبدو إدارة سيّئة، يبدو واضحاً أنّ مزيجاً من الدعم الداخليّ لهجمات القراصنة أدّى الى الخسائر. راجع روبرت مكميلان (Robert McMillan)، "القصّة الخفيّة لشركة أم.تي جوكس (Mt. Gox)، للكارثة التي أصابت عملة بتكوين والتي تسبّبت بخسائر قيمتها 460 مليون دولار أمريكي"، موقع مجلّة وايرد الإلكترونيّ، 3 آذار 2014.

إطار لمناقشة الإلمام وسنستخدم نظام المستويات الستة لتصنيف تطور جهة فاعلة في تنفيذ عمليّات الفضاء الإلكترونيّ كما حددها مجلس علوم الدفاع[47]. وبخاصّة إنّ المستوَييْن الأول والثاني من الخصوم هما على مستوى تطور سيناريو القراصنة الأحداث (script kiddies) أي الأفراد أو المجموعات الذين يستخدمون البرامج النصيّة المتاحة عموماً. على أنّ خصوم المستوَييْن الثالث والرابع هم أكثر إلماماً ويقومون بتطوير شيفرات خبيثة مخصصة مثل تلك المُعدَّة على أساس نقاط ضعف لشن هجوم مباغت والتي يمكن أن يكون قد تمّ اكتشافها من قبل الخصوم أنفسهم، أو من جرّاء تراكم ناقلات الهجمات المتعددة واستغلال الثغرات[48]. أما خصوم المستويين الخامس والسادس، وفي حين أنهم قادرين على هجمات متطورة مستندة إلى الإنترنت، إلا أنهم سيعملون على خلق مواطن الضعف والفرص المتاحة للهجوم. وعليه، فإن خصوم المستويين الخامس والسادس سيقومون باستخدام ليس فقط التقنيات الإلكترونية المتطورة ولكن أيضاً قدرات الاستخبارات البشرية المتطورة (HUMINT). وفي هذا المعنى، إنهم حقاً جهات فاعلة شاملة. للمزيد من التفاصيل حول المستويات، بما في ذلك مزيد من الأمثلة، راجع الفصل الثاني من تقرير فرقة العمل لدى مجلس علوم الدفاع: النظم العسكرية المرنة والتهديد الإلكترونيّ المتقدم. راجع ملحق هذا التقرير للاطلاع على جدول وصف المستويات.

والمهم، أنّه يمكن لخصوم من مستويات أعلى أن يعتمدوا على تقنيّات من مستوى أدنى، وغالباً ما يفعلون ذلك للتشويش على هويّاتهم وقدراتهم. على وجه الخصوص، قد يكون الخصم المهاجم غير راغب في استخدام تقنيّات عالية المستوى، ليس بسبب نقص في الإلمام، إنما بالأحرى بسبب عدم الرغبة في أن يعزى الهجوم إليهم[49]. ويضاف إلى ذلك مسألة أخرى ذات الصلة وهي تحليل الكلفة بالنسبة إلى المنفعة لمعرفة ما إذا كان الإستثمار في الوقت والمال لمساندة القدرة الإلكترونية الجديدة يستحقّ الحطّ من قيمة عملة افتراضيّة أو تدميرها باستخدام الوسائل الإلكترونيّة[50]. في هذا القسم، سندعو أعداء الجهة الفاعلة غير

---

[47] مجلس العلوم الدفاعيّة، وزارة الدفاع، تقرير فرقة العمل: الأنظمة العسكريّة المرنة والتهديد الإلكترونيّ المتقدّم، كانون الثاني 2013.

[48] على سبيل المثال، كانت الشعلة الخبيثة من عمل الخصوم من الفئة الرابعة، وفقاً لمجلس علوم الدفاع، 2013.

[49] يتخطّى قرار جهة فاعلة حكوميّة لإستخدام قدرة إلكترونيّة معيّنة، أو الكشف عن وجود نهج تكنولوجي متقدّم لعمليات الفضاء الإلكترونيّ، نطاق هذا التقرير.

[50] قد يكون إعتبار آخر للدولة القومية قد يكون ردّ فعل سياسيّاً ناجماً عن حرمان السكان من الوصول إلى عملتهم، وبالتالي تحقيق الهدف التقنيّ لتدمير العملة الإفتراضيّة أو إفسادها بالكلفة المحتملة لفقدان القلب والعقل. وهذه وسيلة مثيرة للاهتمام للدراسة المستقبليّة.

الحكوميّة التي تنشر عملة افتراضيّة خصوماً. وكما ذكر آنفاً، يمكن أن يشمل هؤلاء الخصوم على حدّ سواء دولة أو دولاً قوميّة حيث يتمّ نشر العملة الافتراضيّة وحلفاء تلك الدولة القوميّة "الضحية" الذين قد يكون لديهم قدرات إلكترونية أكثر تطوّراً.

وتجدر الإشارة في البداية إلى أن أسهل الهجمات وأكثرها فعاليّة التي يمكن للدولة القوميّة التي نُشرت فيها العملة الافتراضيّة أن تقوم بها هي إما بقطع الإنترنت أو برشحه رشحاً دقيقاً في الدولة التي تصدر عنها عمليّات العملة الافتراضيّة. تتميّز هذه الهجمات بفعاليّة خاصّة لقطع الوصول إلى خدمات المحفظة الرقميّة وخدمات التنقيب. في المقابل، إنّ قطع الإنترنت بالكامل يترتّب عنه تكاليف بالغة، في حين أنّ رشحه بطريقة فعّالة في دولة لا تقوم بذلك أصلاً يمكن أن يتطلّب موارد إضافيّة كبيرة. بالإضافة الى ذلك، إنّ أيّ جدار حماية يمكن أن يُهزم بواسطة تقنيّات فعّالة بما فيه الكفاية لإخفاء بروتوكول الإنترنت مثل تور، مع أنّ هذه التقنيّات عمليّاً يجب أن تدمج في برمجيّات عملة افتراضيّة[51]. أخيراً، هذا الرشح لن يمنع كليّاً استخدام العملات الافتراضيّة محليّاً، شرط أن تدعم بنية الإنترنت التحتيّة وقوّة الحوسبة إستمراريّة العملة.

وأخيراً، علينا أن نميّز مسار الهجوم عن استغلال الثغرات والهجوم بحدّ ذاته. يمكن اعتبار مسارات الهجوم على أنّها المدخل، سواء من خلال البريد الإلكترونيّ المخادع (spear fishing)، أو تجاوز الآليات الأمنية للوصول إلى بيانات الحواسيب (back–doors)، أو الزرع المتعمّد من فعل بشريّ (deliberate implant) أي قيام شخص بإدخال برمجيّات خبيثة من خلال محرك أقراص (USB)، أو من خلال نشر الفيروسات عن طريق الأجهزة النقّالة. بينما استغلال نقاط الضعف (الثغرات) هو استخدام حاسوب أو ميزات الشبكة لأغراض إضافيّة، سواء من خلال هجمات القطع الموزّع للخدمة (باستغلال

---

[51] من غير الواضح ما إذا كان ممكناً لشبكة تور أن تعمل في وجود جدار حماية منفّذ بشكل جيد. على سبيل المثال، واجه تور التحديات مع سور الصين العظيم. راجع، على سبيل المثال، رويا إنصافي (Roya Ensafi)، فيليب وينتر (Philipp Winter)، عبد الله معين (Abdullah Mueen)، وجديديا ر. كراندال (Jedidiah R. Crandall)، "تصنيف واسع النطاق للتناقضات الزمانية المكانية في أكبر جدار حماية في العالم"، دراسة من نشر المؤلّف، 3 تشرين الأوّل 2014، وفيليب ونتر (Philipp Winter) وستيفان ليندسكوغ (Stefan Lindskog)، "كيف يقوم جدار الحماية العظيم الذي تستعمله الصين بصدّ شبكة تور"، دراسة قدّمت في ورشة العمل الثانية لجمعيّة أنظمة الحوسبة المتقدّمة حول التواصل الحرّ والمفتوح عبر الإنترنت (التواصل الحرّ والمفتوح عبر الإنترنت)، بالفيو، واشنطن، آب 2012.

خصائص الشبكات الرقميّة) أو فيضان الثغرات الأمنية في البرمجيّات (أي استبدال الذاكرة لزرع رمز) أو بالتلاعب[52].

هجمات يستخدمها الخصوم من المستويين الأول والثاني

إنّ لدى خصوم المستويين الأول والثاني مجموعة متنوّعة من الهجمات المحتملة يستطيعون أداءها إنما أكثر الهجمات مباشرةً هو الهجوم الذي يعتمد على القوّة الحسابيّة المستقيمة أو عرض النطاق الترددي[53]. في الواقع، إنّ إحدى أقوى الهجمات التي يمكن أن يقوموا بها ضدّ العملات الافتراضيّة اللامركزية مثل البتكوين هي تجاوز القوّة الحسابيّة التي من شأنها، في حالة أخرى، ضمان أمن النظام (عادةً 51 في المئة من إجمالي القوّة الحسابيّة، وتسمى أيضاً في كثير من الأحيان قوّة التنقيب) [54]. إنّ الهجوم الأقوى لتدمير عملة ما هو ما يعرف

---

[52] ومن الأمثلة الحديثة على التلاعب ما حدث مع بيع حواسيب لينوفو (Lenovo) الشخصيّة، التي قامت الشركة بالتثبيت عليها برمجيات حرّة مدعومة من الإعلانات تُضمّن نفسها في سجلّ الحاسوب شهادات وتزوّد مواقع شبكة الإنترنت بشهادات أمنيّة مزوّرة. وبما أنّ العملات الإفتراضية تعتمد على الشهادات والتحقّق من الملكيّة، يمكن هذا الضعف أن يستخدم لخرق النظام وكشف مفاتيح التشفير المخزّنة فيه.

[53] تجدر الإشارة الى أنّه في حين أنّ الهجمات على القوة الحسابية تستهدف بتكوين ليست معرضة، نماذج بديلة مثل إثبات صحة ملكية رصيد ومشتقاتها بنفس الطريقة، لأنّها لا تعتمد على القوّة الحسابيّة لتوليد سلسلة الكتل. وبالإضافة إلى ذلك، فإنّ المصاريف النقديّة لهذه الهجمات قد تكون كبيرة عندما تنفّذ من قبل فاعل واحد.

[54] يحكى عن نسبة 51 في المئة في الممارسة العمليّة، على الرغم من أنّ هناك نتائج نظرية تظهر أنّ الحدّ قد يكون أقرب الى 25 في المئة. راجع إتاي أيال (Ittay Eyal) وأمين غن سيرير (Emin Gun Sirer)، "الأكثريّة ليست كافية: التنقيب عن بتكوين ضعيف"، في طبعات نيكولاس كريستن ورياني سافافي–ناييني (Reihaneh Safavi–Naini)، علم التشفير الماليّ وأمن البيانات: المؤتمر الدوليّ الثامن عشر، علم التشفير الماليّ 2014، آذار 2014، الصفحات 436 إلى 454. وبالإضافة إلى ذلك، إنّ خوان غاراي (Juan Garay) وأغلوس كياياس (Aggelos Kiayias) ونيكوس ليوناردوس(Nikos Leon–ardos)، "بروتوكول بتكوين الأساسي: تحليل وتطبيقات"، في طبعات إليزابيث (Elisabeth Oswald) أوسوالد ومارك فيشلين (Marc Fischlin)، تطوّرات في علم التشفير – مؤتمر يوروكريبت 2015 (EUROCRYPT 2015): المؤتمر الدوليّ الرابع والثلاثين حول نظريّة التقنيّات التشفيريّة وتطبيقاتها، نيسان 2015، الصفحات 281 إلى 310، يثبتون أنّ نسبة 51 في المئة تنخفض أيضاً في وجود كمون الشبكة المتنامي.

بهجوم الإصبع الذهبيّ [55]. في الواقع، كما يشير إليه بونو والمؤلفون المشاركون:

> إذا كان هدف أغلبيّة المنقّبين هو صراحة تقويض إستقرار البتكوين وبالتالي تقويض فائدتها كعملة، فَهُم حتماً يستطيعون فعل ذلك عن طريق إدخال تشعّبات عميقة عمداً أو رفض كتل منقّب آخر... وقد يرغب في محاولة القيام بهكذا هجوم دولة تودّ الإضرار ببتكوين تجنّباً للمنافسة مع عملتها الخاصّة (مع إضافة التشديد)، أو فرد مستثمر بشكل كبير في عملة منافسة[56].

بعبارة أخرى، يتطلّب هجوم الإصبع الذهبيّ تشكيل إتحاد إحتكاريّ يستطيع من خلال قوّته الحسابيّة المهيمنة أن يغيّر قواعد السوق (لتقويض الثقة في العملة) ومنع مستخدمين معيّنين من التداول بالعملة (لطرد مجموعة فرعيّة من المستخدمين من سوق العملات) أو خنق إمدادات العملة الجديدة (لدفع الأسعار إلى الإرتفاع). لذا، ما لم تكن العملة جديدة أو ما لم يكن مقدار القوّة الحسابيّة المرتبطة باللامركزية منخفضاً، من غير الواضح كيف سيكون الخصم قادراً على الوصول المستمر إلى 51 في المئة من إجمالي القوّة الحسابيّة للعملة[57].

وبصورة خاصّة بالنسبة إلى بتكوين، هناك وسيلة أخرى لشنّ هجوم الإصبع الذهبيّ، من خلال إفساد مجامع التنقيب. فالتنقيب يتمّ نموذجياً من قبل مجامع حسابيّة تعمل بتجميع جهود تنقيب المنقّبين الفرديّين. وبذلك يمكن بعض من مجامع التنقيب هذه الإقتراب من عتبة 51 في المئة، بما في ذلك حالة (GHash.io) التي تجاوزت هذه العتبة بشكل بسيط ثمّ وعدت بألاّ يتكرر ذلك[58]. إنّ المسألة هنا ليست أنّ مجمع تنقيب قد يقرر تعطيل بتكوين،

---

[55] راجع جوشوا أ. كرول وإيان س. دايفي (Ian C. Davey) وأدوارد و. فلتن، "إقتصاديّات التنقيب عن بتكوين أو بتكوين بوجود الخصوم"، دراسة قدّمت في ورشة العمل الثانية عشرة حول إقتصاديّات أمن المعلومات (ورشة عمل حول إقتصاديّات أمن المعلومات لعام 2013)، واشنطن، 11 و12 حزيران 2013.

[56] بونو (Bonneau) وغيره، 2015، يتابعون: "تمّت بالفعل مراقبة هذه الهجمات من خلال وأد ألتكوين، بحيث شنت هجمات عميقة ضدّ عملات منافسة جديدة ذات قدرة تنقيب منخفضة وتمّ تركيبها بنجاح من قبل المنقبين عن بتكوين".

[57] إنّ الطريقة الوحيدة لإلتقاط 51 في المئة من القوّة الحسابية هي إمّا عن طريق إختراقات التشفير (على سبيل المثال، طرق خوارزميّة لاختراق SHA–2 أسرع في حالة بتكوين) أو من خلال أجهزة حوسبة جديدة، من دوائر لأغراض خاصة إلى ربّما حواسيب كموميّة (quantum computers). تخرج إمكانية هذه الاحداث عن نطاق هذا التقرير.

[58] راجع بونو وغيره، 2015، ومجمعات التنقيب GHash.io، "مجمع تنقيب عن بتكوين (GHash.IO) يمنع تراكم نسبة 51 في المئة من طاقة الهاش كلّها"، غير مؤرّخ.

إنّما هي أنّ أحد المهاجمين قد يحاول إختراق عدة مجامع تنقيب بحيث تقابل ما يزيد عن 51 في المئة من القوّة الحسابيّة. وبهذه الطريقة، يمكن لمهاجم مع موارد أوليّة صغيرة نسبيّاً أن يشنّ هجوم من 51 في المئة على بتكوين. في الواقع، قد يتطلّب مثل هذا الهجوم خصماً عالي المستوى.

وتجدر الإشارة إلى أنّ مثل هذا الهجوم يتطلّب إستثمار رأسمال خارج سوق بتكوين (للحواسيب والكهرباء مثلاً)، لذلك قد يكون من الصعب إحتساب العائد على الإستثمار لهجوم مماثل. ومع ذلك، إذا كانت الكلفة ضمن الحدود التي كان الخصم سينفقها على الأسلحة في هجوم حركيّ مباشر ضدّ رعاة العملة، ينبغي النظر إلى هجوم من نوع الإصبع الذهبيّ على أنّه واقعيّ[59].

وفي حالة العملات الافتراضيّة المركزيّة أو شبه المركزيّة، إنّ هجمات قطع الخدمة الموزّع والبريد الإلكتروني المخادع المعدّ لمهاجمة نقاط الضعف في الشبكات والبنى التحتيّة الحاسوبيّة تعتبر فعّالة في الحطّ من نظام عملة افتراضيّة، ولا سيما في خدمات أكثر مركزيّة مثل محافظ الإنترنت أو خدمات التنقيب. وكذلك هناك مجموعة من هجمات قطع الخدمة الموزّع ذات الصلة موجودة وتشمل تخريب العمليّات بواسطة البريد الإلكتروني غير المرغوب به وهجمات النص لإضاعة القدرة الحاسوبيّة من خلال خلق عمليّات تحتاج إلى حسابات كبيرة للتأكد من صحّتها[60].

وهذه هي طرق أخرى يمكن للمهاجم فيها فرض تكاليف على الشبكة، حتى لو لم يكن هناك سلطة مركزيّة. إنّ مهاجمة مراكز التبادل أو غيرها من الخدمات الإلكترونية المركزيّة يمكن أن تبرهن انّها فعّالة، حتى لو كانت العملة الافتراضيّة غير مركزيّة. وبدلاً من ذلك قد تستخدم أساليب تقنيّة منخفضّة لمهاجمة مستخدمي بتكوين الذين يستعملون تور[61] (Tor). ويمكن استخدام هجمات قطع الخدمة الموزّع (DDoS attacks) للحطّ من الوصل الشبكي للعمليّات الاقتصاديّة المحليّة واليوميّة بحيث تبطئ عمليّات العملة الافتراضيّة لتصبح غير

---

[59] قد يكون اعتبار آخر هو تكلفة الإجراءات القانونيّة مثل الإعتقالات لإحباط العملة، والتي كانت ناجحة ضدّ العملات الإفتراضيّة مثل (ليبرتي ريزرف) تراجع الولايات المتحدة ضدّ ليبرتي ريزرف، 2013، وزارة العدل، 2013.

[60] راجع، على سبيل المثال، المنتدى حول بتكوين، "ضعف بتكوين الجديد: عمليّة تحتاج على الأقل 3 دقائق ليتمّ التحقق منها من قبل النظير"، خطّ نقاش بدأ في 30 كانون الثاني 2013a.

[61] راجع بيريوكوف (Biryukov) و بوستوغاروف (Pustogarov)، 2015a.

عمليّة وغير مريحة. وبالتالي إنّ أيّ هجوم يخترق نظم الوصول إلى مفاتيح حسابات المستخدمين أو يكشف نظم المستخدمين[62] يمكن استخدامه لسرقة العملة.

وتجدر الإشارة إلى أنّ الغالبيّة العظمى من الدراسات الموجودة المخصصة لأمن العملة الافتراضيّة تتعلق بتهديدات المستويين الأول والثاني، وهذا الأمر مفهوم لأنّ هذه التهديدات وبمستواها المنخفض تعطي نتائج فعّالة إلى حدّ ما. وسوف ننظر الآن في تهديدات أكثر تقدّماً.

هجمات يستخدمها الخصوم من المستويين الثالث والرابع

سيستخدم الخصوم من المستويين الثالث الرابع هجمات أكثر إلماماً بما في ذلك إكتشاف واستغلال ثغرات الهجوم المباغت أو التلاعب بالبنى التحتيّة الكامنة للعملة الافتراضيّة. بالنسبة إلى بتكوين مثلاً "كيف يمكن للمشاركين في النظام البيئي للبتكوين تحقيق الإجماع حول القواعد الافتراضية لعمليّات بتكوين إذا لم يتمّ تحليلها جيّداً"[63]. وبما أنّ نظام بتكوين يتطلّب إجماع المستخدمين على قواعد توليد العملة وحالة العمليّة والتحقق من صحّتها، لذلك ستكون القواعد عرضة للتلاعب أو لإستغلال ثغرات أو عيوب في تطبيق تلك القواعد. في الواقع، يمكن لخصوم من مستويات عالية النظر في مهاجمة القواعد الكامنة للعملات الافتراضيّة اللامركزيّة من أجل تغييرها.

لخصوم المستويين الثالث والرابع أيضاً القدرة على اكتشاف واستغلال هجمات الهجوم المباغت وقد يستخدمونها لإحداث تأثير كبير. وبخاصّة قد يستخدمونها لمهاجمة جماعات التنقيب، كما نوقش في المقطع السابق أعلاه، من أجل السيطرة على 51 في المئة من إجمالي القوّة الحسابيّة. وفي حالات السلطة المركزيّة وشبه المركزيّة، قد تستغل هذه الجهات الفاعلة بنجاح خوادم السلطة وتتسبب بإنهيار العملة جوهريّاً، ربما من خلال هجوم مدبر بمشاركة أفراد من الداخل. حتى في حالة اللامركزيّة، يمكن للخصوم استغلال أهداف محددة بنجاح على الأرجح ويمكنهم إستهداف الأفراد أصحاب الثروات المرتفعة علناً للحدّ من الثقة في العملة (أو إستهداف المواطنين العاديين بشكل عشوائيّ لزرع الشك).

ومن المرجّح أن يكون لدى خصوم المستوى الرابع القدرة على بناء واستخدام الهجوم المباغت ضدّ خدمات العملة الافتراضيّة الهامة مثل التبادلات والمَحافظ فضلاً عن تطبيقات

---

[62] وجود مجموعة واسعة من الثغرات التي يمكن استغلالها من قبل قراصنة يتمتّعون بالحد الأدنى من المهارات يتطلب تأمين حماية كلّ حاسوب شخصي أو هاتف ذكيّ بشكل أساسي. فالفيروسات التي تسرق البتكوين موجودة وتمّت ملاحظة ذلك علناً. راجع أدريان كوفرت (Adrian Covert)، "ثمّة فيروس سيسرق كلّ عملاتكم من البتكوين"، Gizmodo.com، 17 حزيران 2011. ويشير ذلك مرّة أخرى إلى أهميّة المهارات المكتسبة لمستخدمي العملات المشفّرة.

[63] بونو (Bonneau) وغيره، 2015.

الهاتف الخلوي المستخدمة لإجراء العمليّات اليوميّة. في الواقع، قد يقومون باستخدام أذونات وشهادات مزيّفة لتثبيت التطبيقات التي تخرب (أو تتجسس) على تطبيقات مستخدمي العملة الافتراضيّة. وبعد ذلك يقومون إما بتعطيل هذه التطبيقات أو بنشر نقاط الضعف فيها للحطّ من الثقة في العملة الافتراضيّة. وقد يحاول خصوم المستوى الرابع أيضاً أن يحطّوا من قدرة العملة الافتراضيّة على بناء بروتوكولات تشفير موثوق بها (مثل خلق مفتاح وتخزينه كما هي الحال في تطبيقات المحفظة) عن طريق تغيير تطبيقات برمجيّات وظائف التشفير الرئيسة بمهارة. وقد يحاول الخصوم أيضاً تغيير الرمز الفعلي المستخدم من قبل خوادم العملة الافتراضيّة أو مستخدميها من أجل الحطّ من الفعاليّة أو السماح بمسار هجوم أسهل لكي يقطعوا الخدمة لاحقاً وفي الوقت عينه عن فئات واسعة من الخوادم و/أو المستخدمين.

هجمات يستخدمها الخصوم من المستويين الخامس والسادس

كما يمكن لجهات فاعلة من المستويين الخامس والسادس أن تستخدم الهجمات الضارة بشكل خاصّ من خلال هجمات سلسلة التوريد ضدّ البنية التحتيّة الأساسيّة أو من خلال تقويض تنفيذ البرمجيّات المستخدمة من قبل مشتركي العملة الافتراضيّة. قد تصيب هذه الجهات الفاعلة فئات واسعة من البرمجيّات والمعدات بالفيروسات لأنها قد تستهدف الهواتف الخلويّة أو الأجهزة الأخرى، بما في ذلك أجهزة الحاسوب المستخدمة كخوادم للخدمات الحرجة للعملة الافتراضيّة أو الأجهزة المخصصة لأغراض خاصّة والمستخدمة في التنقيب، وإفسادها قبل التسليم. وبذلك يمكنها الإستفادة من هذا الوصول لتمكينها من إجراء العمليّات المذكورة في المقطع أعلاه على المستويين الثالث والرابع مع وجود إحتمال أكبر للنجاح. وبتلويث الأجهزة خاصّة الأجهزة ذات الأغراض الخاصّة التي تقوم بمهام التشفير، ستكون الجهات الفاعلة من المستويين الخامس والسادس قادرة أيضاً على كسر معايير التشفير التي تكمن وراء العملة الافتراضيّة، والذي يمكنه بدوره كسر أمن العملة الافتراضيّة. وإذا كشفت علناً (أو جرى الكشف على نتائج هذا الكسر دون الكشف عن الكسر نفسه) فإنّ هذه الإستراتيجيّة يمكن أن تؤدي إلى إحباط الثقة في العملة الافتراضيّة بشدّة.

علاوة على ذلك، يمكن للجهات الفاعلة من المستويين الخامس والسادس استخدام وسائل المعلومات الاستخباراتية، أي من خلال توظيف عملاء لتولّي أدوار وظيفيّة رئيسة في العملة الافتراضيّة، مثل مطوري البرمجيّات، أو من خلال رشوة هؤلاء الموظفين أو استمالتهم، سواء داخل منظّمة العملة الافتراضيّة أو في غيرها من المنظّمات التي توفّر خدمات أساسيّة للعملة الافتراضيّة.

إمكانية الدفاع الناجح

في ضوء المناقشة السابقة بشأن مهاجمة العملة الافتراضيّة، فإن الأمر يستحق بحثاً وجيزاً بشأن ما إذا كان من الممكن على الإطلاق نشر عملة افتراضيّة تتحمل هجوماً إلكترونيّاً. وإلاّ، سيكون بحث نشر جهة غير حكوميّة لعملة افتراضيّة مثير للجدل.

في نهاية المطاف، يبدو واضحاً أن الجهة الفاعلة غير الحكوميّة (وفي الواقع، حتى الجهة الفاعلة الحكوميّة) ستواجه تحديّات كبيرة ضدّ خصم عنيد من مستوى عال في ظلّ الافتراضات والتطبيقات الأساسية للعملات الافتراضيّة. كقاعدة عامة، قد ينجح خصم عالي المستوى في مهاجمة أيّ هدف جدير بالإهتمام في الفضاء الإلكترونيّ إذا ما استثمرت موارد كافية. في حالة العملة الافتراضيّة، التي تتطلّب الثقة والمجهولية وتوافر الخدمات الإلكترونيّة المنتشرة على نطاق واسع (مثل المحفظة وتطبيقات التنقيب)، يبدو غير ممكن قيام دفاع إلكتروني ناجح على الدوام. قد يكون الأمل الوحيد هو في دعم الجهة الفاعلة غير الحكوميّة من قبل خصم في دولة قوميّة ملمّة يكون قادراً على مواجهة مثل هذه التهديدات. وحتى في هذا السيناريو ليس من الواضح ما إذا كان هذا التنسيق سوف ينجح، لا سيما في حالة خصم من المستويين الخامس والسادس.

قد تكون جهة فاعلة غير حكوميّة ملمّة قادرة على شن دفاع ضدّ خصم من المستويين الأول والثاني، على الرغم من أنّ الحماية من هجمات قطع الخدمة الموزّع أو هجمات التنقيب قد تكون مرتبطة بالطريقة التي أصبحت فيها الخدمات المختلفة مركزيّة وبقوّة التنقيب التي تدعم حالياً العمليّات اللامركزيّة.

ومن الجدير بالذكر مرّة أخرى أن خصوماً من مستويات عالية لا يرغبون في شن هجمات تكشف عن مستوى إلمامهم. في الواقع، إنّ الحسابات السياسيّة قد تمنع خصماً عالي المستوى من شنّ هجومه الأكثر إلماماً، لا سيما في ظروف أظهرت فيها جهة فاعلة غير حكوميّة القدرة على الردّ أو عندما تحظى جهة فاعلة غير حكوميّة بدعم من قبل دولة قوميّة ترى أنّ مثل هذا الهجوم الملمّ كاف للتهديد بالإنتقام. وخلاصة القول، إنّ السؤال الكبير المجهول الإجابة هو ليس بالضرورة ما إذا كان الخصم الملمّ قادراً على إسقاط عملة افتراضيّة، ولكن ما إذا كانوا على استعداد من الناحية السياسيّة لتكريس موارد العملة الافتراضيّة أو لديه القدرة على ذلك كهدف من الأولويات.

مع ذلك، قد يكون ممكناً إبتكار عملة افتراضيّة مستقرة ومرنة نسبيّاً وذلك بإعادة النظر في بعض الافتراضات والبُنى الأساسيّة، لا سيما بعد الإعلان عن هذه الافتراضات والبُنى من قبل قوّة إلكترونيّة ملمّة (مثل خبراء الدولة القوميّة في الموضوع الإلكترونيّ). على وجه الخصوص، من الأهميّة بمكان أن تتخذ التدابير المناسبة لحماية تصميم برمجيّات العملة الافتراضيّة الأساسيّة وكذلك الخدمات الخارجيّة، مثل خدمات المحفظة الآمنة (وتطبيقات الهاتف الذكي) وخدمات التنقيب، إلى جانب الحماية المرتبطة بالخوادم التي من شأنها أن تقوم بهذه الخدمات. إنّ الدولة القوميّة الملمّة هي الجهة الفاعلة الأكثر قدرة على ضمان هذا الأمن ما يشكّل سبباً آخر يزيد من فرص بقاء العملة الافتراضيّة على قيد الحياة إلكترونيّاً عندما تلقى جهة فاعلة غير حكوميّة الدعم من دولة قوميّة ملمّة إلكترونيّاً. على أقل تقدير، سيتمّ طرح مستوى الإلمام والإستثمار لمهاجمة عملة افتراضيّة بنجاح مما يجعل حساب التفاضل والتكامل أي قرار الخصم لمهاجمة عملة افتراضيّة أكثر تعقيداً.

تداعيات تتخطّى العملة

بحثت الفصول السابقة من هذا التقرير في التحدّيات المحتملة المرتبطة بنشر الجهات الفاعلة غير الحكوميّة العملات الافتراضيّة كعملة عاديّة. أمّا الآن فسنبحث في التداعيات التكنولوجيّة الأوسع نطاقاً لنشر العملة الافتراضيّة، ولا سيما في سياق الأمن القوميّ. وفيما كثرت النقاشات العامة حول تطبيقات تكنولوجيا سلسلة الكتل التابعة لبتكوين التي تعنى بالتقدّم التكنولوجيّ المستقبليّ المرتبط بالتمويل[1]، تجذب إهتمامنا في هذا الموضوع نقاطٌ أوسع تشمل: أوّلاً التداعيات المباشرة لتكنولوجيا سلسلة الكتل التابعة لبتكوين وأمثالها، وثانياً كيف قد يؤدّي نشر العملة الافتراضيّة إلى زيادة الإلمام بالتشفير لدى الجهات الفاعلة السابقة التي لم تكن ملمّة به وثالثاً كيف قد تبدأ العملات الافتراضيّة حقبة يسهل فيها وصول الجهات الفاعلة القليلة الإلمام بالمجال الإلكترونيّ إلى خدمات إلكترونيّة مرنة.

كما سنرى في هذا الفصل، إنّ حرص سياسة الأمن القوميّ الأكبر يكمن في توفّر القدرات الإلكترونيّة التي تزداد إلماماً لدى الجهات الفاعلة القليلة الإلمام بالمجال الإلكترونيّ. وفيما قد يفيد ذلك الولايات المتّحدة من خلال تزويد الجهات الفاعلة غير الحكوميّة التي تدعمها الولايات المتّحدة بالوصول إلى خدمات إلكترونيّة أكبر في بيئات إلكترونيّة قد تكون مرفوضة أو متداعية، قد يلحق الضرر بمصالح الولايات المتّحدة من خلال السماح للمجموعات الإرهابيّة بالوصول إلى خدمات إلكترونيّة قد يصعب على الدولة بشكل متزايد من أن تمنع حصوله.

[1] راجع، على سبيل المثال، مارك أندرسن (Marc Andreessen)، "لمَ بتكوين مهمّة"، صحيفة نيويورك تايمز الإلكترونيّة، 21 كانون الثاني 2014.

تكنولوجيا سلسلة الكتل والإجماع الموزّع

في نهاية المطاف، وفّرت العملات الافتراضيّة اللامركزيّة كبتكوين وسائل مرنة لتخزين البيانات وتحديثها بطريقة عالية التوزيع يصعب جدّاً إفسادها. وفي حالة بتكوين، تشكّل بياناتها سجلّاً عامّاً للعمليات المالية، لكن في المبدأ، يمكن تخزين بيانات أخرى بطريقة مشابهة. ويشكّل أيضاً الوقت اللازم لتوزيع البيانات والإتّفاق عليها عاملاً معرقلاً. وحتى في حالة العملات الافتراضيّة الأخرى التي تفوق بتكوين فاعليّةً، يستغرق وقت الإجماع عدة دقائق. ويبدو أنّ الثغرة الزمنيّة هذه متأصّلة في الأنظمة اللامركزيّة التي يجب أن تتّفق فيها عدّة عقد تنظيمية على حالة تشغيليّة مشتركة. ويشكّل عرض حزمة التواصل اللازم مشكلة كبيرة أخرى. فزيادة البيانات يحتاج مزيد من متطلّبات الخدمة الإلكترونيّة، تزداد أيضاً كمّيّة التواصل على طول الشبكة اللامركزيّة. وسيكون بالتالي السؤال الذي سيُطرح في أبحاث مستقبليّة حول كيفيّة تقديم خدمات مماثلة بطريقة فعّالة من حيث التواصل.

بشكل عامّ، ينتج الاستعمال المحتمل لتكنولوجيا مماثلة عن حالات يكون فيها نشر البيانات والحفاظ عليها في مواجهة تحديّات أو في حالة قمع، لكنّ الوصول إلى البيانات ليس بعدد وحدة زمنيّة قدرها واحد على ألف من الثانية. وتشمل الأمثلة إستراتيجيّات وتقنيّات وإجراءات مصمّمة لتمكين الإنشقاقيّين السياسيّين من استعمالها ونشر المنشورات الإرهابيّة كمجلّة "إنسباير" لتنظيم القاعدة في شبه الجزيرة العربيّة أو مجلّة "دابق" لتنظيم الدولة الإسلاميّة في العراق والشام.

وستكون كيفيّة تحفيز أمن أيّ نظام لامركزيٍّ تحديّاً من التحديّات الرئيسة في تكييف تكنولوجيا سلسلة الكتل مع التطبيقات غير الماليّة الأخرى. ومن أحد إبتكارات بتكوين الرئيسة هو كيف تتداخل الحوافز الاقتصاديّة مع عمليّة الأمن اللامركزيّ بشكل جيّد. فعلى سبيل المثال، جرى العمل على زيادة أمن خدمة شبكة تور اللامركزيّة، لكن من خلال استعمال حوافز ماليّة[2]. ولا يبدو واضحاً كيف ستحرز تكنولوجيا سلسلة الكتل على طراز بتكوين تقدّماً في الإعدادات من دون حوافز مماثلة[3].

---

[2] راجع ألكس بيريوكوف (Alex Biryukov) وإيفان بوستوغاروف (Ivan Pustogarov)، "إثبات العمل بمثابة تسديد صغير مغفل: مكافأة مرحّل شبكة تور"، دراسة قدّمت في خلال الندوة العالميّة التاسعة عشرة حول التشفير الماليّ وأمن البيانات لعام 2015، سان خوسيه، بويرتو ريكو، من 26 إلى 30 كانون الثاني، 2015b.

[3] لحلّ واحد محتمل، راجع مايدسايف (Maidsafe)، غير مؤرّخ (a).

ويمكن أن تحدث مهمّات أكثر حساسيّة تجاه الوقت مع إزدياد فاعليّة الإجماع الموزّع المرن والآمن (ومع الحفاظ على قابليّة إدارة متطلّبات التواصل). وتشمل هذه المهمّات المنتديات المرنة على الإنترنت التي قد يصعب قطعها وخدمات الدردشة المرنة الفوريّة وخدمات المراسلة المغفلة الموجّهة في الشبكات اللامركزيّة على نطاق واسع، لتخلق المجهولية الحقيقيّة[4]. وقد تستخدم بروتوكولات الإجماع الموزّع عندما تكون في أقصى فعاليّتها لدردشات الصوت عبر بروتوكول الإنترنت المغفلة والمرنة، أي نسخة مرنة ومغفلة فعلاً عن تطبيق سكايب.

وفيما قد تكون تطبيقات مماثلة نافعة لمستخدمي الأمن القوميّ، ستكون نافعة بشكل خاصّ للخصوم القليلي الإلمام بالتكنولوجيا، بما أنّهم سيتمكّنون من الوصول إلى خدمات أكثر مرونة، نظراً لمهاراتهم المحدودة.

العملات الافتراضيّة تزيد الإلمام بالتشفير

أدّى إزدياد إدراك تكنولوجيا سلسلة الكتل إلى ازدياد إدراك تقنيّات التشفير الملمة بآخر التطورات للإجماع الموزّع والحوسبة. وأصبح أصحاب مشاريع رأس المال يتكلّمون على مفاهيم مرتبطة بعلم الحاسوب كمسألة الجنرال البيزنطي[5] (Byzantine Generals Problem)، وأصبح خبراء الأمن الإلكترونيّ العام يتكلّمون على نتائج معمّقة في التشفير النظريّ كنظريّة معرفة منعدمة – حجج مقتضبة للمعرفة (ZK–SNARKs)[6]. وبالعادة، لا تشكّل هذه المسائل مواضيع نقاش تتداول خارج دوائر أكاديميّة نادرة.

ويشكّل التركيز الأكبر على تطبيقات تقنيّات التشفير المتقدّمة كالحوسبة الآمنة المتعدّدة الأطراف إحدى النتائج المحتملة: يسعى مجال التشفير إلى القيام بالحوسبة الموزّعة بطريقة تحافظ على سرّيّة مدخلات الحوسبة ومخرجاتها وعلى سلامتها، حتّى لدى وجود نشاط خبيث ضمن النظام الموزّع. ويشكّل بروتوكول بتكوين حول الإجماع الموزّع، بطريقة أو بأخرى، مجموعة مميّزة من الوظائف تحاول الحوسبة الآمنة المتعدّدة

---

[4] جوناثان وارن (Jonathan Warren)، "بيت مسج Bitmessage" نظام النظير للنظير لتصديق الرسائل وإيصالها"، دراسة من نشر المؤلّف، 27 تشرين الثاني 2012.

[5] راجع أندرسن (Andreessen)، 2014. لسوء الحظ، الإدّعاء حول العقد البيزنطيّ في المقالة خاطئ (راجع غاراي وكياياس وليوناردوس، 2015).

[6] راجع بن–ساسون (Ben–Sasson) وغيره، 2013.

الأطراف أن تحسبها[7]. وقد يؤدّي التركيز المتزايد على الحوسبة الآمنة المتعدّدة الأطراف إلى بروتوكولات موزّعة آمنة وكفوءة لدرجات وظيفيّة متزايدة؛ وعرضت وكالة مشاريع الأبحاث المتطوّرة الدفاعيّة DARPA مؤخّراً طريقة آمنة ببث الصوت عبر بروتوكول الإنترنت الآمن (VOIP) على بنية تحتيّة غير موثوق فيها من خلال استعمال الحوسبة الآمنة المتعدّدة الأطراف (MPC)[8].

أمّا الحصيلة الأخرى، فهي الإتاحة المتزايدة لبرمجيّات التشفير المصمّمة بحرفية – أو بصورة عامة – رمز التشفير– هذه البرمجيات مصمّمةٌ لدعم العملات الافتراضيّة، حيث يمكن لمطوّرو البرامج الأقلّ إلماماً أن يستخدموها لتوفير قدر أكبر من الأمن. وفي الممارسة، قد يسمح ذلك للمجرمين الإلكترونيّين والإرهابيّين، الذين يتمتّعون بمستوى أدنى من الإلمام التكنولوجيّ، بأن يصلوا إلى عمليّات تواصل أكثر أمناً وإلى خدمات إلكترونيّة أخرى، مما يصعّب على الولايات المتّحدة ملاحقتهم وهزيمتهم.

أخيراً، إنّ الاستعمال المتنامي للعملة الافتراضيّة القائم على التنقيب قد تترتّب عنه تداعيات على توافر جهاز ذي هدف خاصّ لإختراق أمن التشفير. فعلى سبيل المثال، تشبه عمليّة التنقيب عن بتكوين العمليّة المستخدمة لإختراق تشفير هاش الآمن 2 SHA–2 وهي دالة هاش التشفيريّة. أمّا الآن، يستطيع المنقّبون عن الأجهزة أن يقوموا بأكثر من 5 تريليون هاش في الثانية الواحدة؛ وبمعنى آخر، لم يشارك سوى 1,000 من هؤلاء المنقّبين في مجموع قوّة التنقيب في بتكوين في كانون الأول 2013، على مستوى الرسملة السوقيّة للعملة الافتراضيّة[9]. إنّ التحفيز الاقتصاديّ تجاه أجهزة تتزايد قوّة قد

---

[7] ليس الإجماع على بتكوين حالة مميّزة من حالات الحوسبة الآمنة متعددة الأطراف. إنّ لامركزيّة بتكوين مثيرة للإهتمام بصورة خاصّة لأنّها تحفّز الحوسبة الموزّعة. أمّا تأمين الحوسبة الآمنة لا يفترض عادةً تحفيزاً مماثلاً. وبإشارة إلى مدى إهتمام الذين يهمّهم تأمين الحوسبة الآمنة بالبتكوين (والعكس صحيح)، حملت جائزة أفضل مقالة في ندوة الأمن والخصوصيّة على الإنترنت لعام 2014 عنوان "الحوسبة المتعدّدة الأطراف الآمنة على بتكوين" (راجع مارسين أندريشويكز وستيفان دزيامبوسكي ودانييل مالينوسكي ولوكاس مازوريك، "الحسابات الآمنة المتعدّدة الأطراف على بتكوين"، دراسة مقدّمة في خلال ندوة الأمن والخصوصيّة على الإنترنت التي نظّمتها جمعيّة مهندسي الكهرباء والإلكترونيات، سان خوسيه، كاليفورنيا، من 18 إلى 21 أيار 2014).

[8] راجع وكالة مشاريع البحوث المتطوّرة الدفاعيّة داربا، "البرامج المقدّمة في اليوم التجريبي الذي نظّمه مكتب الإبتكار المعلوماتيّ التابع لوكالة داربا"، 21 أيار 2014.

[9] راجع بتكوين ويكي (Bitcoin Wiki)، "مقارنة التنقيب عن المعدّات الإلكترونيّة"، 16 أيلول 2015c، وسلسلة الكتل، "تمويل السوق"، غير مؤرّخ (b).

تخرق أمن التشفير يمكن أن يخاصم إستثمارات دولة قوميّة في أجهزة مماثلة مما قد ينتج تداعيات على أمن أدوات التشفير.

العملات الافتراضيّة والإتّجاه نحو خدمات إلكترونيّة لامركزّية ومرنة

يمكن إعتبار بتكوين والإبتكارات الحاليّة في العملات الافتراضيّة مجرّد خطوة أخيرة تمهّد للجهات الفاعلة القليلة الإلمام بالمجال الإلكترونيّ الوصول إلى خدمات إلكترونيّة لامركزيّة ومرنة. وقد يساعد فهم الإتّجاه التقليديّ هذا على تحديد وجهة الإتّجاه والتداعيات على وزارة الدفاع.

الخطوة الأولى نحو تطوير بتكوين كانت بتكنولوجيا النظير للنظير كخدمة نابستر Napster وشبكة جنوتيلا Gnutella (ولاحقاً بت تورنت BitTorrent). وسمحت هذه التكنولوجيا للمستخدمين بأن يصلوا إلى المعلومات من خلال التواصل مع الغرباء على الإنترنت، بالتالي توفير منتدى لتبادل البيانات[10]. وقلبت هذه الخدمات المقاييس في توفير البيانات وأثّرت كثيراً على الكيانات كصناعة الموسيقى. وكان أمن هذه الخدمات الكلّيّ بحده الأدنى. وبما أنّ العمليّات كانت ثنائيّة، يمكن قطع هذه الخدمات الإلكترونيّة الخاصّة المتاحة للجميع (البيانات في هذه الحال) ورصدها بسهولة نسبيّة. ويمكن إعتبار مرحلة التكنولوجيا هذه "مرحلة التوافر الإلكترونيّ من دون اللامركزيّة".

وأتت أوّل خطوة نحو اللامركزيّة من مشروع شبكة تور[11] (Tor). فتسمح شبكة تور للمستخدمين بالحفاظ على خصوصيّة هويّاتهم على الإنترنت من خلال توفير مجمع من

---

[10] راجع جوهان بووالسي (Johan Pouwelse) وباول غارباكي (Pawel Garbacki) وديك إيبيما (Dick Epema) وهنك سيبس (Henk Sips)، "نظام النظير للنظير بت تورينت لمشاركة الملفّات: القياسات والتحليل"، في طبعات ميغال كاسترو، إجراءات المؤتمر الدوليّ الرابع حول أنظمة النظير للنظير الدوليّة 2005، شباط 2005، ص. 216–205، وستيفان سارويو (Stefan Saroiu)، وب. كريشنا غومادي (P. Krishna Gummadi) وستيفن د. غريبل (Steven D. Gribble)، " دراسة قياسيّة حول أنظمة تبادل الملفّات عبر تقنيّة النظير للنظير"، مارتن ج. كينزل (Martin G. Kienzle) وطبعات براشانت ج. شينوي (Prashant J. Shenoy)، إجراءات منظّمة SPIE: الحوسبة وإقامة الشبكات المتعدّدة الوسائط (MMCN 2002)، المجلّد 4673، 2002، الصفحات 156 إلى 170.

[11] للمزيد من المعلومات حول تور، راجع مشروع تور، "لمحة عامّة"، غير مؤرّخ (d).

العقد المتاحة حول العالم التي تمّكن المستخدم من أن يصل إليها بشكل متسلسل. ومن وجهة نظر إشرافيّة، يبدو أنّ المستخدم يملك هويّة العقدة الأخيرة التي استخدمت في خدمة تور. ونجحت تور لأنّ المتطوّعين حول العالم يستضيفون العقد التي تمكن المستخدمين من استعمالها. إضافةً إلى ذلك، يمكن إنشاء مواقع بأكملها يمكن الوصول إليها عبر تور فحسب. ويدعى هذا النظام ككلّ الإنترنت المظلم[12]. ومن الصعب الهجوم على تور بما أنّ المستخدمين يتواصلون مباشرةً من عقدة تور إلى عقدة تور أخرى، لكنّ عدد الوصلات المباشرة قليلٌ (عادةً ثلاثة)، ويعتقد أنّ تور معرّضة لخصوم ملمّين[13]. ومن وجهة نظر مركزيّة، قد تكون تور لامركزيّة على نحو غير مضبوط. وينتهي المطاف بالمستخدم في الاعتماد على عدد قليل من العقد إنطلاقاً من مجموعة واسعة من عقد تور المتاحة، لكنّه يتمتّع بحرّيّة إختيار العُقَد التي يرغب في استعمالها.

وتتّجه بتكوين والعملات الافتراضيّة اللامركزيّة الأخرى نحو لامركزيّة تامّة، تعتمد فيها الخدمة الإلكترونيّة بالفعل – وهي الإجماع الموزّع – على أغلبيّة الشبكة اللامركزيّة بدلاً من عدد قليل من العقد (في حالة تور). ويمكن الهجوم على العملات الافتراضيّة بشكل ناجح كما سبق وعرضنا ذلك في الفصل الرابع. لكن من خلال التوجّه نحو عمليّات إلكترونيّة لامركزيّة، حيث يمكن للجهات الفاعلة القليلة الإلمام بالمجال الإلكترونيّ الوصول بشكل سهل إلى الخدمات الإلكترونيّة ذات التعقيد المتزايد. وسيضطرّ مجتمع الأمن القوميّ إلى مواجهة تحدي يقضي بمنع هذه الجهات الفاعلة في المجال الإلكترونيّ من الاستمرار عبر السنوات القادمة.

نحو أرضيّة أساسيّة إلكترونيّة عامّة ومرنة

مرّت حوالى عشر سنوات بين إنشاء نابستر وإنشاء بتكوين. وتطرح وتيرة التطوّر هذه السؤال الآتي: "ما هي التكنولوجيا التي نتوقّع أنّها ستنشأ في السنوات العشر أو العشرين القادمة؟" يطرح الإتّجاه التاريخيّ، الذي هو بمثابة إختبار فكريّ، فكرة الأرضيّة الأساسيّة الإلكترونيّة العامّة والمرنة: وهي قدرة الجهات الفاعلة القليلة الإلمام بالمجال الإلكترونيّ

---

[12] راجع مشروع تور، "بروتوكول الخدمة السرّيّ"، غير مؤرّخ (ب)، و"الغفليّة على الإنترنت"، غير مؤرّخ (a).

[13] مثالٌ على هجوم مماثل، راجع مشروع تور، "مسار مرحّل لإستشارة أمنيّة"، 30 تمّوز 2014، و"الفئات والوصمات والهجمات"، 19 كانون الأوّل 2014.

على الوصول الدائم والمؤمّن إلى خدمات إلكترونيّة بغض النظر عمّا إذا عارضت جهة فاعلة حكوميّة على قدر عالٍ من الإلمام استعمالها. ما هي التداعيات التقنيّة لإتاحة مماثلة؟

بشكل عامّ، يمكن للأرضيّة الأساسيّة الإلكترونيّة العامّة والمرنة أن تكون سيفاً ذا حدّين: حيث تأمن من جانب السماح لوزارة الدفاع بنشر القوّة، على مستوى المعلومات والعمليّات الإلكترونيّة، لكن من جانب آخر تؤمن السماح لأعداء الولايات المتّحدة بالقيام بالعمليّة نفسها مع حاجز لإدخال البيانات أضعف من ذي قبل.

وقد تسمح الأرضيّة الأساسيّة الإلكترونيّة العامّة والمرنة بالتدفّق المجانيّ للمعلومات على شكل إتّصالات عامّة، كالمواقع الإخباريّة غير المنقطعة والمنتديات الإلكترونيّة، تخترق جدران الحماية الوطنيّة كجدرا الحماية الصينيّ العظيم، لكن قد تسمح أيضاً بوصول أكبر إلى إستراتيجيّات المتشدّدين وبياناتهم. وقد تهزم إمكانيّة مماثلة للرقابة على الإنترنت وتتيح نشر نظرة أمريكا عن العالم في بلدان أنكرت معلومات مماثلة من قبل. وفي الوقت عينه، ستتوافر مواقع تتيح الجرائم والإرهاب بشكل دائم (بالفعل، في بيئة مماثلة، قد لا يزال موقع ليبرتي ريزرف Liberty Reserve العملة السابقة التي أبطلتها الحكومة الأمريكيّة، فاعلاً). وقد يكون ردّ فعل محتمل لبعض البلدان على تطوّرات مماثلة أن تنفصل بشكل أساسيّ من شبكة الإنترنت العالميّة. وستتمكّن وزارة الدفاع من القيام بعمليّات معلوماتية بحرّيّة أكبر، لكنّها قد تكون أيضاً أكثر عرضةً لعمليّات المعلوماتية الإرهابيّة.

وقد يسمح الوصول المباشر إلى خدمات إلكترونيّة مرنة بتوفير ببنية تحتيّة للاتّصالات مرنة وعالميّة وتتيح الإتّصالات الخاصّة: إتّصالات غير منقطعة ومغفلة ومشفّرة[14]. وقد تخدم مثل هذه الاتصالات المماثلة حاجات الإنشقاقيّين السياسيّين في التواصل من دون تدخّل حكومتهم. لكنّه قد يسمح للمجرمين أو الإرهابيّين أو الدول القوميّة حتّى بأن تبني بنية تحتيّة غير مسندة حيث يتم التخطيط من خلالها لهجمات إلكترونيّة أو للقيام بنشاط إجراميّ. وقد تكون التداعيات على وزارة الدفاع والمجتمع الاستخباراتيّ أنّه

[14] قد تستعمل، بشكل أكثر تقنيّةً، لإنشاء البنية الأساسيّة العالميّة للمفتاح العامّ. والبنية الأساسيّة للمفتاح العامّ هي وسيلة لإتاحة مصدر ثقة للاتّصالات والتصديق الآمنة للمستخدمين والأجهزة. للمزيد من المعلومات عن البنيّة الأساسيّة للمفتاح العامّ، راجع، على سبيل المثال، ريتشارد د. كون وفينسنت ك. هيو، وو. تيموثي بولك وشو–جن تشانغ، مدخل إلى تقنيّة المفتاح العامّ والبنية الأساسيّة والفدراليّة للمفتاح العامّ، غايثرسبيرغ، ميريلاند: المعهد الوطنيّ للمعايير والتقنيّة، الولايات المتّحدة الأمريكيّة، وزارة التجارة، 26 شباط 2001.

يجب تطوير الإستراتيجيّات والتقنيّات والإجراءات الجديدة التابعة لاستخبارات الإشارات من أجل التصدّي لهذا التهديد.

وقد يستعمل خصوم الولايات المتّحدة تكنولوجيا مماثلة، عدا عن استخدام الأرضيّة الأساسيّة الإلكترونيّة المرنة للإتّصالات، من أجل السماح بوصلات مباشرة غير مسندة وغير قابلة للإختراق لمهاجمة الدول القوميّة إلكترونيّاً. وقد تستطيع الجهات الفاعلة، الحكوميّة وغير الحكوميّة، أن تنشر قوّة إلكترونيّة بطرق لم تكن ممكنة من ذي قبل بمستويات إلمام إلكترونيّ أدنى بكثير من تلك التي كانت مطلوبة في السابق. من ناحية أخرى، قد تستخدم وزارة الدفاع البنية التحتيّة المرنة ذاتها لتكتسب الوصول ولتقوم بهجمات إلكترونيّة أيضاً. إنّه من المحتمل أن يكون هذا تقدماً نحو دفاعات إلكترونيّة أكثر فعاليّة من الدفاعات الحاليّة.

الخاتمة والأبحاث المستقبليّة

بحث هذا التقرير في إمكانيّة المجموعات الإرهابيّة أو المتمرّدة أو الإجراميّة من تعزيز نفوذها السياسيّ و/أو الاقتصاديّ، من خلال نشر عملة افتراضيّة تستعمل كما تستعمل أيّ عملة في العمليّات الاقتصاديّة المنتظمة. ولإبعاد تهديد استعمال عملة افتراضيّة غير حكوميّة، ينبغي على مجتمع الأمن القوميّ الأمريكيّ أن يفهم كيف تستطيع الجهات الفاعلة غير الحكوميّة أن تستثمر العملات الافتراضيّة. ويشكّل هذا البحث جزءاً صغيراً من حوار أوسع حول جدوى العملات الافتراضيّة من منظورين: الأول إجتماعيّ علميّ (أي العملة الافتراضيّة بمثابة عملة) والثاني تكنولوجيّ (أي العملة الافتراضيّة بمثابة خدمة إلكترونيّة آمنة ومغفلة ومرنة).

من منظور اقتصاديّ، قد يواجه التشجيع على اعتماد العملات الافتراضيّة (بدلاً من اعتماد عملات مستعملة) تحديّات بارزة من حيث قبول المجتمع بها كعملة جديدة لا تتمتّع بخلفيّة تاريخيّة، وبالتالي قد تفتقر إلى الشرعيّة كونها عملة لا تتمتّع بتمثيل ملموس على شكل ورقة أو نقود في المجتمعات التي اعتادت أن يكون المال فيها ماديّاً. ونتوقّع أن يخفّ حذر المجتمعات حيال العملات الافتراضيّة بالتعود على استعمال هذه العملة. فقد يتم التغيّير في المواقف عندما تصبح التكنولوجيا التي تقوم عليها العملات الافتراضيّة أكثر شيوعاً وجدارةً بالثقة. إضافةً إلى ذلك، في المكان الذي تكون فيه العملة الافتراضيّة الوسيلة الوحيدة للقيام بعمليّات التحويل، قد ترغم الحاجة الاقتصاديّة الناس على القبول بالعملات الافتراضيّة، التي كانوا سيرفضونها في حالة أخرى.

لذلك، قد تكون الإستراتيجيّة الفضلى التي ينبغي أن تعتمدها الولايات المتّحدة وحلفاؤها لمنع نشر عملة افتراضيّة هي إستهداف خصائصها الأكثر زيادةً لقبولها، وبالتحديد مجهولية عمليّة التحويل وأمانها وتوافرها.

ومن منظور تكنولوجيّ، يشكّل اليوم نشر عملة افتراضيّة تحلّ مكان العملة العاديّة في العمليّات التجاريّة اليوميّة تحدياً كبيراً. وتشمل التحديّات الوصول إلى الإلمام التكنولوجيّ اللازم لتطوير عملة افتراضيّة كخدمة إلكترونيّة ونشرها والحفاظ عليها وتأمين مستويات عالية من مجهولية عمليّات التحويل التي يطلبها المستخدمون لتأمين سلامة التحويل، حتّى يتأكّد البائعون والشارون من أنّ التبادل صحيح، وذلك من دون الحاجة إلى إلمام تكنولوجيّ متقدّم جدّاً، وأخيراً حماية سلامة العملة الافتراضيّة الإجماليّة (وتوافرها) من أخطار إلكترونيّة متقدّمة، ولا سيما الدول القوميّة التي قد تعارض نشر الجهات الفاعلة غير الحكوميّة لعملة افتراضيّة. وقد يؤدّي توافر التكنولوجيّات للحدّ من هذه المسائل في المستقبل إلى تسهيل عمليّة نشر الجهة الفاعلة غير الحكوميّة للعملة الافتراضيّة.

وفي الوقت عينه، تتّخذ الولايات المتّحدة أو غيرها من البلدان التي تسعى إلى إبعاد عملة افتراضيّة ما قراراً مهمّاً يقضي بتحديد أيّ مستوى من الإلمام الإلكتروني (أو القدرات) لازم لهذه المهمة وأيّ نوع من الاستثمار في القدرات البشرية والوقت والأبحاث سيكون مفيداً لإبعاد أيّ عملة افتراضيّة.

وعندما تدعم دولة قوميّة ما تتمتّع بإلمام إلكترونيّ متقدّم جهةً فاعلة غير حكوميّة، يصبح نشر هذه الأخيرة للعملة الافتراضيّة أكثر قابليّة للتنفيذ. وقد تسمح الدولة القوميّة هذه للجهات الفاعلة غير الحكوميّة بالتغلّب على العقبات التقنيّة المهمّة التي ترتبط بنشر عملة افتراضيّة، ويشمل ذلك قدرة دولة قوميّة على الدفاع عن جهة فاعلة غير حكوميّة وحمايتها بهجوم إلكترونيّ بدرجة إلمام عالية من خصم آخر للدولة القوميّة كالولايات المتّحدة الأمريكيّة.

أخيراً، يتمتع نشر العملات الافتراضيّة بالقدرة على تطوير تكنولوجيات تعني مجتمع الأمن القوميّ، بما في ذلك الخدمات الإلكترونيّة التي تزداد مرونةً مما يسهل استعمالها من قبل جهات فاعلة قليلة الإلمام، كنشر المعلومات وتخزينها. وقد زاد أيضاً التركيز المتنامي على العملات الافتراضيّة الإلمام بالتشفير، مما قد يؤدّي إلى برمجيّات تزداد أمناً من جهة، وإلى معدّات إلكترونيّة تزداد فاعليّة لاختراق الأمن التشفيريّ من جهة أخرى. وأخيراً، يشير الإتّجاه التاريخيّ إلى تطوّر أرضيّة حيويّة إلكترونيّة عامّة ومقاومة، عرّف عنها هذا التقرير بأنّها قدرة الجهات الفاعلة القليلة الإلمام في المجال الإلكترونيّ على الوصول الدائم والآمن إلى الخدمات الإلكترونيّة، بغض النظر عمّا إذا عارضت جهة فاعلة حكوميّة ملمّة استعمالها. ويحمل ذلك تبعات على جدران الحماية التي تفرضها الحكومة لمراقبة محتوى الإنترنت؛ وعلى الوصول إلى الخطابات المتطرّفة؛ وعلى قابليّة شنّ الدولة القوميّة هجمات إلكترونيّة؛ وعلى القدرة على الحفاظ على عمليّة اتّصال آمنة وغير قابلة للإنقطاع ومغفلة.

للأبحاث المستقبليّة

تتعدّد التحديّات التي أظهرها هذا التقرير والتي تستحقّ أن تُدرَس في المستقبل. أمّا واحد منها، فهو كسب فهم أوضح حول المفاضلات بين العقبات التكنولوجيّة لولوج العملات الافتراضيّة وقبول المجتمع بأن يستخدمها في عمليّات التحويل اليوميّة. وقد تكون قابليّة الاستخدام موضوع دراسة مفيد بشكل خاصّ. ومن التحديّات ذات الصلة هو فهم إلى أيّ درجة يريد المواطن العاديّ أن يثق بالعملات الافتراضيّة القائمة على مبادئ تشفير متقدّمة لا يفهمها. وستترتّب عن ذلك تداعيات على العملات الجديدة، كعملة زيروكاش، التي توصف بأنّها خطوة مهمّة نحو المجهولية.

وسنحتاج بشكل ملحوظ إلى المزيد من العمل للبحث في إمكانيّة الجهات الفاعلة غير الحكوميّة استثمار عملة افتراضيّة بدلاً من نشرها. فمتى قد تختار جهة فاعلة غير حكوميّة أن تستخدم عملة افتراضيّة بدلاً من النقود للقيام بتحويلات أو جمع التبرّعات أو تبييض الأموال بطريقة غير شرعيّة؟ وماذا قد تكون نقاط القرار الرئيس؟ وما هي العملات الافتراضيّة التي تصلح للاستعمال في هذه الطريقة؟ وما هي كمّيّة العملات الإجماليّة التي يمكن استخدامها في عمليّات التحويل العاديّة أو شبه العاديّة فيما يتمّ الحفاظ على المجهولية؟ وبصورة خاصّة، متى قد تكون العملة الافتراضيّة أكثر نفعاً من الدولارات الأمريكيّة الورقيّة في عمليّات التحويل غير الشرعيّة؟ وقد يستعمل هذا التقرير لاستعراض هذا البحث، ولكن يجب القيام بالمزيد من العمل.

وسنحتاج إلى المزيد من البحث عن كثب للمناطق حول العالم وللجهات الفاعلة غير الحكوميّة التي ستكون المستفيد الأكبر من نشر عملة افتراضيّة تكون بمثابة وسيلة سياسيّة. وسنحتاج إلى تحليل إضافيّ لتحديد أيّ موشّرات وإنذارات ستكون أكثر فائدة لبرهنة أنّ الجهات الفاعلة غير الحكوميّة تعتمد بشكل متنام على العملات الافتراضيّة.

وسنحتاج إلى دراسة إضافيّة لفهم أيّ تكنولوجيّات مرنة تتيحها العملات الافتراضيّة أو العكس. ولا يبدو واضحاً ما إذا كانت الحوافز الاقتصاديّة التي تمكّن بتكوين ستعمل في خدمات إلكترونيّة أكثر شموليّةً. وأخيراً، سنحتاج إلى دراسة إضافيّة لاكتشاف الأفكار التي تكمن وراء الأرضيّة الحيويّة الإلكترونيّة العامّة والمرنة، لترقّب التداعيات السياسيّة على المديين القريب والبعيد، فيما تصبح الخدمات الإلكترونيّة التي تزداد مرونة منتشرة ومتاحة حتى للمستخدم الأقلّ إلماماً في المجال الإلكترونيّ.

ملحق

تصنيف مستويات الإلمام بالتهديدات الإلكترونيّة

يرد أدناه ملخّص عن إطار المستويات بحسب ما ذكر في الجدول الوارد في مستند صادر عن مجلس العلوم في وزارة الدفاع الأمريكية في العام 2013. راجع الفصل 2 لمزيد من التفاصيل.

الجدول رقم A.1
مستويات التهديد الإلكتروني

المستوى	الوصف
I	الممارسون الذين يعتمدون على الآخرين لتطوير الشيفرات الخبيثة، وآليات التسليم، واستراتيجية التنفيذ (باستعمال ثغرات معروفة)
II	الممارسون مع خبرة أعمق وقدرة على تطوير أدواتهم الخاصّة (من مواطن ضعف معروفة عامةً)
III	الممارسون الذين يركزون على اكتشاف الرمز الخبيث المجهول واستخدامه وهم ضليعون في تركيب المستخدم ومجموعات البرامج المستعملة لإخفاء عمليّات root kits ويستخدمون غالباً أدوات التنقيب عن البيانات ويستهدفون المسؤولين في الشركات والمستخدمين الرئيسين (من حكومة وصناعة). من أجل سرقة معلومات عن الأفراد والشركات بهدف معلن وهو بيع المعلومات إلى عناصر إجرامية أخرى
IV	جهات فاعلة تنتمي للدولة أو لعناصر إجراميّة منظّمة وضليعة في التقنيّة وجديرة ومحترفين ممولين جيداً يعملون ضمن مجموعات لاكتشاف مواطن الضعف والثغرات الجديدة
V	جهات فاعلة في الدولة تخلق مواطن ضعف من خلال برنامج نشيط للتأثير على خدمات ومنتجات تجارية خلال مراحل التصميم أو التطوير أو التصنيع أو مع القدرة على التأثير على منتجات في سلسلة التوريد للسماح باستثمار الشبكات وخلق أنظمة قابلة لخدمة المصلحة
VI	دول لها القدرة على أن تنفّذ بنجاح عمليّات تغطي شتّى التوجهات (قدرات إلكترونية مجموعة مع كل قدراتها العسكرية والإستخبارية) من أجل تحقيق نتيجة محددة في المجالات السياسيّة والعسكريّة والاقتصاديّة والتطبيق على نطاق واسع

المصدر: مجلس العلوم في وزارة الدفاع الأمريكية.

المراجع

al-Munthir, Taqi'ul-Deen, "Bitcoin wa Sadaqat al-Jihad: Bitcoin and the Charity of Violent Physical Struggle," self-published article, August 2014. As of February 26, 2015:
https://alkhilafaharidat.files.wordpress.com/2014/07/btcedit-21.pdf

Altcoins, homepage, undated. As of February 24, 2015:
http://altcoins.com

Andreessen, Marc, "Why Bitcoin Matters," *New York Times* online, January 21, 2014. As of February 23, 2015:
http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters

Andrychowicz, Marcin, Stefan Dziembowski, Daniel Malinowski, and Łukasz Mazurek, "Secure Multiparty Computations on Bitcoin," paper presented at the IEEE Symposium on Security and Privacy, San Jose, Calif., May 18–21, 2014.

Apple, "iOS Security, iOS 9.0 and Later," September 2015. As of October 7, 2015:
https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Atlas, Kristov, "An Analysis of Darkcoin's Blockchain Privacy via Darksend+," self-published article, September 10, 2014. As of February 22, 2014:
http://cdn.anonymousbitcoinbook.com/darkcoin/darksend-paper/Atlas_Darksend-Analysis-v001.pdf

Auroracoin, "AuroraSpjall" undated. As of November 6, 2015:
http://auroraspjall.is

Barotseland Free State, *Barotseland Mupu Currency Act of 2012*, February 28, 2012. As of April 16, 2015:
http://www.barotseland.info/Currency_Act.htm

Ben-Sasson, Eli, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza, "SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge," in Ram Canetti and Juan A. Garay, eds., *Advances in Cryptology—CRYPTO 2013: 33rd Annual Cryptology Conference*, Santa Barbara, Calif., August 2013, pp. 90–108.

———, “Zerocash: Decentralized Anonymous Payments from Bitcoin,” paper presented at the 2014 IEEE Symposium on Security and Privacy, San Jose, Calif., May 18–21, 2014a.

———, “Zerocash: Decentralized Anonymous Payments from Bitcoin,” extended version of the paper presented at the 2014 IEEE Symposium on Security and Privacy, San Jose, Calif., May 18–21, 2014b. As of February 20, 2015: http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf

Bernstein, Peter L., *The Power of Gold: The History of an Obsession*, Hoboken, N.J.: Wiley and Sons, Inc., 2004.

Biryukov, Alex, and Ivan Pustogarov, “Bitcoin over Tor Isn’t a Good Idea,” paper presented at the 2015 IEEE Symposium on Security and Privacy, San Jose, Calif., May 17–21, 2015a.

———, “Proof-of-Work as Anonymous Micropayment: Rewarding a Tor Relay,” paper presented at the 19th International Conference on Financial Cryptography and Data Security 2015, San Jose, Puerto Rico, January 26–30, 2015b.

Bitcoin, “Choose Your Bitcoin Wallet,” undated (a). As of February 19, 2015: https://bitcoin.org/en/choose-your-wallet

———, “Protect Your Privacy,” undated (b). As of February 22, 2015: https://bitcoin.org/en/protect-your-privacy

———, “Some Things You Need to Know,” undated (c). As of February 20, 2015: https://bitcoin.org/en/you-need-to-know

Bitcoin Forum, “[RELEASE] Liquidcoin (Speculation Based),” discussion thread began January 18, 2012. As of February 26, 2015: https://bitcointalk.org/index.php?topic=60026.0

———, “New Bitcoin Vulnerability: A Transaction That Takes at Least 3 Minutes to Be Verified by a Peer,” discussion thread began January 30, 2013a. As of October 13, 2015: https://bitcointalk.org/index.php?topic=140078.msg1491085#msg1491085

———, “CoinJoin: Bitcoin Privacy for the Real World,” discussion thread began August 22, 2013b. As of February 22, 2015: https://bitcointalk.org/index.php?topic=279249.0

Bitcoin Help, homepage, undated. As of February 25, 2015: https://bitcoinhelp.net

Bitcoin Wiki, “Comparison of Cryptocurrencies,” December 24, 2014. As of February 24, 2015: https://en.bitcoin.it/wiki/Comparison_of_cryptocurrencies

———, “Hardware Wallet,” August 15, 2015a. As of February 19, 2015: https://en.bitcoin.it/wiki/Hardware_wallet

———, homepage, August 13, 2015b. As of February 25, 2015: https://en.bitcoin.it/wiki/Main_Page

———, "Mining Hardware Comparison," September 16, 2015c. As June 25, 2015: https://en.bitcoin.it/wiki/Mining_hardware_comparison

———, "Weaknesses," July 8, 2015d. As of February 16, 2015: https://en.bitcoin.it/wiki/Weaknesses

Blanc, Jerome, "Thirty Years of Community and Complementary Currencies," *International Journal of Community Currency Research*, Vol. 16, 2012, pp. D1–4.

Blockchain, homepage, undated (a). As of June 25, 2015: https://blockchain.info

———, "Market Capitalization," undated (b). As of February 19, 2015: https://blockchain.info/charts/market-cap?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address

———, "Send Via: Send Bitcoins Using Email and SMS," undated (c). As of February 19, 2015: https://blockchain.info/wallet/send-via

Bonneau, Joseph, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten, "Research Perspectives on Bitcoin and Second-Generation Cryptocurrencies," *Proceedings of IEEE Security and Privacy 2015*, San Jose, Calif.: IEEE Computer Society, May 2015.

Bonneau, Joseph, Arvind Narayanan, Andrew Miller, Jeremy Clark, and Joshua A. Kroll, "Mixcoin: Anonymity for Bitcoin with Accountable Mixes," *Financial Cryptography and Data Security: 18th International Conference*, Berlin: Springer Heidelberg, 2014, pp. 486–504.

Brantly, Aaron, "Financing Terror Bit by Bit," *CTC Sentinel*, Vol. 7, No. 10, October 2014, pp. 1–5.

Chaum, David, "Blind Signatures for Untraceable Payments," in David Chaum, Ronald L. Rivest, and Alan T. Sherman, eds., *Advances in Cryptology: Proceedings of Crypto '82*, Berlin: Springer-Verlag, 1983, pp. 199–203.

Chaum, David, Amos Fiat, and Moni Naor, "Untraceable Electronic Cash," in Shafi Goldwasser, ed., *Advances in Cryptology: Proceedings of Crypto '88: Proceedings*, Berlin: Springer-Verlag, 1990, pp. 319–327.

Christin, Nicolas, "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace," *Proceedings of the 22nd International Conference on World Wide Web (WWW 2013)*, Rio de Janeiro: World Wide Web Conference, 2013, pp. 213–223.

Cohen, Benjamin J., *The Geography of Money*, Ithaca, N.Y.: Cornell University Press, 1998.

CoinJoin, "Weaknesses in SharedCoin," undated. As of February 22, 2015: http://www.coinjoinsudoku.com

CoinMarketCap, "Crypto-Currency Market Capitalizations," September 30, 2015a. As of June 25, 2015: http://coinmarketcap.com

Covert, Adrian, "There's a Virus That Will Steal All Your Bitcoins," *Gizmodo.com*, June 17, 2011. As of February 25, 2015: http://gizmodo.com/5813039/theres-a-virus-that-will-steal-all-your-bitcoins

Danezis, George, Cédric Fournet, Markulf Kohlweiss, and Bryan Parno, "Pinocchio Coin: Building Zerocoin from a Succinct Pairing-Based Proof System," *PETShop '13: Proceedings of the First ACM Workshop on Language Support for Privacy-Enhancing Technologies*, New York: Association for Computing Machinery, 2013, pp. 27–30.

Daragahi, Borzo, "ISIS Declares Its Own Currency," *Financial Times* online, November 13, 2014. As of February 24, 2015: http://www.ft.com/intl/cms/s/2/baf893e0-6b4f-11e4-9337-00144feabdc0.html#axzz3SgRLthZp

Dark Wallet, homepage, undated. As of February 22, 2015: https://www.darkwallet.is

Dash, homepage, undated (a). As of June 25, 2015: https://www.dashpay.io

———, "Masternodes and Proof of Service," undated (b). As of June 25, 2015: https://www.dashpay.io/masternodes2

Dash Talk, "Reply to Kristov's Paper," self-published article, September 11, 2014. As of February 22, 2015: https://dashcointalk.org/threads/reply-to-kristovs-paper.2325

Davies, Glyn, *A History of Money: From Ancient Times to the Present Day*, Chicago: University of Chicago Press, 2005.

Defense Advanced Research Projects Agency, "DARPA I2O Demo Day Featured Programs," May 21, 2014. As of October 7, 2015: http://www.darpa.mil/attachments/DARPAI2ODemoDay_ProgramDescriptions.pdf

Defense Science Board, Department of Defense, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat,* January 2013. As of September 30, 2015: http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

Department of Justice, U.S. Attorney's Office, Southern District of New York, "Indictment and Supporting Documents: U.S. v. Liberty Reserve et al.," May 28, 2013. As of February 22, 2015: http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReserveetalDocuments.php

Desan, Christine, *Making Money: Coin, Currency, and the Coming of Capitalism*, Oxford: Oxford University Press, 2014.

Dowd, Kevin, "Contemporary Private Monetary Systems," self-published paper, August 2013. As of February 26, 2015:
http://www.kevindowd.org/app/download/8477462997/Contemporary+Private+Monetary+Systems.pdf?t=1380159881

El Defrawy, Karim, and Joshua Lampkins, "Founding Digital Currency on Secure Computation," *CCS '14: Proceedings of ACM SIGSAC Conference on Computer and Communications Security*, March 2014, pp. 1–14.

Ensafi, Roya, Philipp Winter, Abdullah Mueen, and Jedidiah R. Crandall, "Large-Scale Spatiotemporal Characterization of Inconsistencies in the World's Largest Firewall," self-published paper, October 3, 2014. As of February 22, 2015:
http://arxiv.org/pdf/1410.0735.pdf

European Banking Authority, "EBA Opinion on 'Virtual Currencies,'" July 4, 2014. As of October 1, 2015:
https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

European Central Bank, *Virtual Currency Schemes*, October 2012. As of October 1, 2015:
https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

Eyal, Ittay, and Emin Gun Sirer, "Majority Is Not Enough: Bitcoin Mining Is Vulnerable," in Nicolas Christin and Reihaneh Safavi-Naini, eds., *Financial Cryptography and Data Security: 18th International Conference, FC 2014*, March 2014, pp. 436–454.

Federal Bureau of Investigation, "Ransomware on the Rise: FBI and Partners Working to Combat This Cyber Threat," January 20, 2015. As of February 13, 2015:
http://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise

Folding Coin, "Announcing Scotcoin," February 5, 2015. As of February 13, 2015:
http://foldingcoin.net/2015/01/announcing-scotcoin

Frieden, Jeffry A., *Global Capitalism: Its Fall and Rise in the Twentieth Century*, New York: W. W. Norton and Company, 2006.

Garay, Juan, Aggelos Kiayias, and Nikos Leonardos, "The Bitcoin Backbone Protocol: Analysis and Applications," in Elisabeth Oswald and Marc Fischlin, eds., *Advances in Cryptology—EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Crypotgraphic Techniques*, April 2015, pp. 281–310.

GHash.io, "Bitcoin Mining Pool GHash.IO Is Preventing Accumulation of 51 Percent of All Hashing Power," undated. As of February 23, 2015:
https://ghash.io/ghashio_press_release.pdf

Gill, Nathan, "Ecuador Turning to Virtual Currency After Oil Loans," *Bloomberg News* online, August 11, 2014. As of February 13, 2015:
http://www.bloomberg.com/news/articles/2014-08-11/
ecuador-turning-to-virtual-currency-after-oil-loans-correct-

GitHub, "Omni Protocol Specification (formerly Mastercoin)," undated. As of February 26, 2015:
https://github.com/OmniLayer/spec

Gomez, Georgina, "Sustainability of the Argentine Complementary Currency Systems: Four Governance Systems," *International Journal of Community Currency Research*, Vol. 16, 2012, pp. D80–89.

Helleiner, Eric, *The Making of National Money: Territorial Currencies in Historical Perspective*, Ithaca, N.Y.: Cornell University Press, 2003.

Hern, Alex, "Bitcoin Goes National with Scotcoin and Auroracoin," *Guardian* website, March 25, 2014. As of October 7, 2015:
http://www.theguardian.com/technology/2014/mar/25/
bitcoin-goes-national-with-scotcoin-auroracoin

Irish Coin, homepage, undated. As of February 24, 2015:
http://irishcoin.org

Ithaca Hours, homepage, undated. As of February 24, 2015:
http://www.ithacahours.com

Jack, William, and Tavneet Suri, "The Economics of M-Pesa," second version, self-published paper, August 2010. As of February 19, 2015:
http://www.mit.edu/~tavneet/M-PESA.pdf

Johnson, Marion, "The Cowrie Currencies of West Africa. Part I," *Journal of African History*, Vol. 11, No. 1, 1970, pp. 17–49.

Kaelberer, Matthias, "Trust in the Euro: Exploring the Governance of a Supra-National Currency," *European Societies*, Vol. 9, No. 4, 2007, pp. 623–642.

Kaspersky Labs, "The Desert Falcons Targeted Attacks," version 2.0, corporate publication, Moscow, 2015. As of October 1, 2015:
https://securelist.com/files/2015/02/The-Desert-Falcons-targeted-attacks.pdf

Kharif, Olga, "Bitcoin: Not Just for Libertarians and Anarchists Anymore," *BloombergBusiness.com*, October 9, 2014. As of February 20, 2015:
http://www.bloomberg.com/bw/articles/2014-10-09/
bitcoin-not-just-for-libertarians-and-anarchists-anymore

Kindleberger, Charles, *A Financial History of Western Europe*, Oxford: Oxford University Press, 1993.

King, Sunny, "Primecoin: Cryptocurrency with Prime Number Proof-of-Work," self-published paper, July 7, 2013. As of February 19, 2015:
http://primecoin.io/bin/primecoin-paper.pdf

King, Sunny, and Scott Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake," self-published paper, August 19, 2012. As of February 24, 2015: http://archive.org/stream/PPCoinPaper/ppcoin-paper_djvu.txt

Krebs, Brian, "True Goodbye: 'Using Truecrypt Is Not Secure,'" *KrebsonSecurity.com*, May 14, 2014. As of February 19, 2015: http://www.krebsonsecurity.com/2014/05/true-goodbye-using-truecrypt-is-not-secure/

———, "U.S. Government Seizes LibertyReserve.com," *KrebsonSecurity.com*, May 13, 2013. As of September 29, 2015: http://www.krebsonsecurity.com/2013/05/u-s-government-seizes-libertyreserve-com

Kroll, Joshua A., Ian C. Davey, and Edward W. Felten, "The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries," paper presented at the 12th Workshop on the Economics of Information Security (WEIS 2013), Washington, D.C., June 11–12, 2013.

Kuhn, Richard D., Vincent C. Hu, W. Timothy Polk, and Shu-Jen Chang, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, Gaithersburg, Md.: National Institute of Standards and Technology, U.S. Department of Commerce, February 26, 2001. As of February 16, 2015: http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf

Lajka, Arijeta, "Islamic State Takes a Stab at Legitimacy with Alleged Identification Cards as Forces Lose Ground in Iraq," *Vice News* online, April 16, 2015. As of June 25, 2015: https://news.vice.com/article/islamic-state-takes-a-stab-at-legitimacy-with-alleged-identification-cards-as-forces-lose-ground-in-iraq

Lee, Timothy B., "Major Glitch in Bitcoin Network Sparks Sell-Off; Price Temporarily Falls 23%," *Ars Technica*, March 11, 2013. As of April 16, 2015: http://arstechnica.com/business/2013/03/major-glitch-in-bitcoin-network-sparks-sell-off-price-temporarily-falls-23

Litecoin, homepage, undated. As of February 24, 2015: https://litecoin.org

Maidsafe, homepage, undated (a). As of on February 24, 2015: http://maidsafe.net

———, "SAFE Network System Docs," undated (b). As of February 24, 2015: http://systemdocs.maidsafe.net

Mas, Ignacio, and Dan Radcliffe, "Mobile Payments Go Viral: M-PESA in Kenya," World Bank website, March 2010. As of February 19, 2015: http://siteresources.worldbank.org/AFRICAEXT/Resources/258643-1271798012256/M-PESA_Kenya.pdf

Mazacoin, homepage, undated. As of February 24, 2015: https://mazacoin.org

McMillan, Robert, "The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster," *Wired* online, March 3, 2014. As of September 29, 2015: http://www.wired.com/2014/03/bitcoin-exchange

Meiklejohn, Sarah, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," *Proceedings of the 2013 Conference on Internet Measurement (IMC '13)*, October 2013, pp. 127–140.

Murphy, Edward V., M. Maureen Murphy, and Michael V. Seitzinger, *Bitcoin: Questions, Answers, and Analysis of Legal Issues*, Washington, D.C.: Congressional Research Service, August 14, 2015.

Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System," self-published paper, 2008. As of February 15, 2015: https://bitcoin.org/bitcoin.pdf

Namecoin, homepage, undated. As of February 24, 2015: http://namecoin.info/

Nxt Wiki, "Whitepaper:NXT," modified July 13, 2014. As of October 7, 2015: http://wiki.nxtcrypto.org/wiki/Whitepaper:Nxt

Only Coin, homepage, undated. As of February 19, 2015: https://onlycoin.com

Open Hub, "Bitcoin Project Summary," undated. As of February 26, 2015: https://www.openhub.net/p/bitcoin

Perfect Money, homepage, undated. As of April 16, 2015: https://perfectmoney.is

Pfajfar, Damjan, Giovanni Sgro, and Wolf Wagner, "Are Alternative Currencies a Substitute or a Complement to Fiat Money? Evidence from Cross-Country Data," *International Journal of Community Currency Research*, Vol. 16, 2012, pp. 45–56.

Pitta, Julie, "Requiem for a Bright Idea," *Forbes* online, November 1, 1999. As of February 26, 2015: http://www.forbes.com/forbes/1999/1101/6411390a.html

Pouwelse, Johan, Paweł Garbacki, Dick Epema, and Henk Sips, "The Bittorrent P2P File-Sharing System: Measurements and Analysis," in Miguel Castro, ed., *IPTPS 2005 Proceedings of the Fourth International Conference on Peer-to-Peer Systems*, February 2005, pp. 205–216.

Prisco, Giulio, "An Independent Scotland Powered by Bitcoin?" *CryptoCoinNews.com*, September 17, 2014. As of February 13, 2015: https://www.cryptocoinsnews.com/an-independent-scotland-powered-by-bitcoin

Recorded Future, "How Al-Qaeda Uses Encryption Post-Snowden (Part 1)," self-published paper, May 8, 2014a. As of February 17, 2015: https://www.recordedfuture.com/al-qaeda-encryption-technology-part-1

———, "How Al-Qaeda Uses Encryption Post-Snowden (Part 2)—New Analysis in Collaboration with ReversingLabs," self-published paper, August 1, 2014b. As of February 17, 2015:
https://www.recordedfuture.com/al-qaeda-encryption-technology-part-2

Ripple, "FAQ," undated (a). As of February 22, 2015:
http://wiki.ripple.com/FAQ

———, homepage, undated (b). As of February 24, 2015:
https://ripple.com

Rogoff, Kenneth, "Costs and Benefits to Phasing Out Paper Currency," *NBER Macroeconomics Annual 2014*, Vol. 29, 2015, pp. 445–456.

Salt Spring Dollars, homepage, undated. As of February 24, 2015:
http://www.saltspringdollars.com

Samani, Raj, "Cybercrime Exposed: Cybercrime-as-a-Service," corporate white paper, Santa Clara, Calif.: McAfee Labs, 2013a. As of September 29, 2015:
http://www.mcafee.com/us/resources/white-papers/wp-cybercrime-exposed.pdf

———, "Digital Laundry: An Analysis of Online Currencies, and Their Use in Cybercrime," corporate white paper, Santa Clara, Calif.: McAfee Labs, 2013b. As of September 29, 2015:
http://www.mcafee.com/us/resources/white-papers/wp-digital-laundry.pdf

Saroiu, Stefan, P. Krishna Gummadi, and Steven D. Gribble, "A Measurement Study of Peer-to-Peer File Sharing Systems," Martin G. Kienzle and Prashant J. Shenoy, eds., *Proceedings of SPIE: Multimedia Computing and Networking (MMCN) 2002,* Vol. 4673, 2002, pp. 156–170.

Scotcoin, homepage, undated. As of February 19, 2015:
http://scotcoin.org

Square, homepage, undated. As of February 19, 2015:
https://squareup.com

Taylor, Adam, "The Islamic State (or Someone Pretending to Be It) Is Trying to Raise Funds Using Bitcoin," *Washington Post* online, June 9, 2015. As of June 25, 2015:
http://www.washingtonpost.com/blogs/worldviews/wp/2015/06/09/the-islamic-state-or-someone-pretending-to-be-it-is-trying-to-raise-funds-using-bitcoin

Taylor, Michael Bedford, "Bitcoin and the Age of Bespoke Silicon," paper presented at the *International Conference on Compilers, Architecture, and Synthesis for Embedded Systems (CASES)*, Montreal, Quebec, September 29–October 4, 2013.

Tor Project, "Anonymity Online," undated (a). As of February 16, 2015:
https://www.torproject.org

———, “Category, Tags, Attacks,” December 19, 2014. As of February 24, 2015: https://blog.torproject.org/category/tags/attacks

———, “Hidden Service Protocol,” undated (b). As of February 24, 2015: https://www.torproject.org/docs/hidden-services.html.en

———, homepage, undated (c). As of February 22, 2015: https://www.torproject.org

———, “Overview,” undated (d). As of February 24, 2015: https://www.torproject.org/about/overview

———, “Security Advisory Relay Early Traffic,” July 30, 2014. As of February 24, 2015: https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack

Totnes Pound, homepage, undated. As of February 24, 2015: http://www.totnespound.org

Treisman, Daniel, “Russia’s ‘Ethical Revival’: The Separatist Activism of Regional Leaders in a Postcommunist Order,” *World Politics*, Vol. 49, No. 2, 1997, pp. 212–249.

United States v. Liberty Reserve, 13 CRIM368 (S.D.N.Y. 2013). As of February 22, 2015: http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR/Liberty%20Reserve,%20et%20al.%20Indictment%20-%20Redacted.pdf

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.

Warren, Jonathan, “Bitmessage: A Peer-to-Peer Message Authentication and Delivery System,” self-published paper, November 27, 2012. As of February 23, 2015: https://bitmessage.org/bitmessage.pdf

Weatherford, Jack McIver, *The History of Money*, New York: Crown Publishers, 1997.

WebMoney Transfer, homepage, undated. As of April 16, 2015: http://www.wmtransfer.com

Wikipedia, “Ora (Currency),” April 27, 2015. As of April 21, 2015: http://en.wikipedia.org/wiki/Ora_%28currency%29

Willett, J. R., *The Second Bitcoin White Paper*, vs. 0.5 (Draft for Public Comment), self-published paper, undated. As of October 1, 2015: https://sites.google.com/site/2ndbtcwpaper/2ndBitcoinWhitepaper.pdf

Winter, Philipp, and Stefan Lindskog, “How the Great Firewall of China is Blocking Tor,” paper presented at the Second USENIX Workshop on Free and Open Communication on the Internet (FOCI), Bellevue, Wash., August 2012.

World Bank, *Global Findex Database*, 2014. As of June 25, 2015: http://datatopics.worldbank.org/financialinclusion

Zerocash Project, homepage, undated. As of February 22, 2015: http://zerocash-project.org

Zerocoin Project, homepage, undated. As of February 22, 2015: http://zerocoin.org

يبحث هذا التقرير في الجدوى من قيام جهات فاعلة غير حكوميّة بزيادة نفوذها السياسيّ و/أو الإقتصاديّ عن طريق نشر عملة إفتراضيّة لاستخدامها في العمليّات الإقتصاديّة العاديّة. والعملة الرقميّة الإلكترونيّة بتكوين (Bitcoin) هي تمثيل رقميّ لعملة مقيّمة يمكن تحويلها أو تخزينها أو تداولها إلكترونيّاً، شأنها شأن العملة العاديّة. ولا تصدر العملات الإفتراضيّة لا عن البنك المركزيّ ولا عن السلطات العامّة، وليست بالضرورة متعلّقةً بعملةٍ ورقيّة (كالدولار واليورو...). إنّما يقبل الناس بها وسيلةً للدفع. وطرحنا الأسئلة البحثيّة الآتية من المنظورين التكنولوجيّ والسياسيّ الإقتصاديّ: (1) لماذا قد تقدم جهة فاعلة غير حكوميّة على نشر عملة إفتراضيّة؟ وبمعنى آخر، ما الفائدة السياسيّة و/أو الإقتصاديّة من نشرها؟ وكيف يمكن للجهة الفاعلة غير الحكوميّة هذه أن تقوم بعمليّة نشر مماثلة؟ وما هي التحدّيات التي سيتعيّن التغلّب عليها؟ (2) كيف يمكن لحكومة أو لمنظّمة أن تنجح تقنيّاً في تعطيل نشر عملة إفتراضيّة من قبل جهة فاعلة غير حكوميّة، وما هي درجة الإلمام الإلكترونيّ المطلوبة؟ (3) ما هي القدرات الإضافيّة التي تصبح ممكنة عندما تُستخدم التكنولوجيا المستعملة في تطوير العملات الإفتراضيّة وتطبيقها لأغراض أوسع نطاقاً من العملة؟ إنّ هذا التقرير معدٌّ ليكون ذا فائدة لصانعي السياسات المهتمّين بمسائل التكنولوجيا ومكافحة الإرهاب والإستخبارات ومسائل إنفاذ القانون وللباحثين في العملة الإفتراضيّة والأمن الإلكترونيّ.

معهد أبحاث RAND للدفاع الوطنيّ

www.rand.org

$17.50

ISBN2-9183-8330-0 10-
ISBN3-9183-8330-0-978 13-

9 780833 091833 51750

Arabic Translation
"National Security Implications of Virtual Currency"
RR-1231/1-OSD