

مسؤولو البنوك المركزية

والتحدي الجديد للأمن السيبراني

العملات الرقمية الصادرة عن البنوك المركزية قد تفرض مخاطر أمنية، وإن كان تصميمها بشكل مسؤول يمكن أن يحول هذه المخاطر إلى فرص.

جوليا فانتي، وجوش ليبسكي، وأولي مور

ولكن مع إطلاق مزيد من البلدان مشروعات تجريبية لإصدار بنوكها المركزية لعملة رقمية، نشأت مخاوف كبيرة تتعلق بالأمن الإلكتروني والخصوصية. وذكر مؤخرا جيروم باول، رئيس الاحتياطي الفيدرالي، أن "المخاطر السيبرانية" هي المصدر الرئيسي لقلقه المتعلق بالاستقرار المالي، كما وصف تقرير أخير صدر عن مجلس اللوردات البريطاني الأمن السيبراني ومخاطر الخصوصية بأنهما من الأسباب المحتملة لعدم إصدار البنك المركزي لعملة رقمية.

وليس هذه المخاوف بلا مبرر. فمواطن الضعف في العملة الرقمية التي يصدرها البنك المركزي يمكن استغلالها للتأثير على النظام المالي لبلد ما. وستتمكن هذه العملة الرقمية من مراكمة بيانات حساسة عن المدفوعات والمستخدمين بحجم غير مسبوق. وإذا وقعت هذه البيانات في أيدي غير آمنة، سوف تستخدم في التجسس على المعاملات الخاصة للمواطنين، والحصول على

عالم البنوك المركزية الذي عادة ما يتسم بالحرص، نجد فكرة إصدار البنك المركزي لعملة رقمية تتحرك بسرعة البرق. فيتبين من بحث أجراه مركز الاقتصاد الجغرافي التابع للمجلس الأطلسي (Atlantic Council GeoEconomics Center) أن هناك حاليا ١٠٥ من البلدان واتحادات العملة تستكشف إمكانية إطلاق عملة البنك المركزي الرقمية، إما لمدفوعات التجزئة — تصدر للجمهور العام — أو الجملة، وتستخدم بصفة أساسية في المعاملات بين البنوك. وهكذا يكون عددها قد ارتفع من ٣٥ الذي أشارت إليه التقديرات مؤخرا في ٢٠٢٠. وليس الاقتصادات الأصغر هي وحدها المهتمة بهذا الأمر، فهناك ١٩ بلدا من أعضاء مجموعة العشرين تنظر في إصدار بنوكها المركزية لعملة رقمية، حقق معظمها بالفعل تقدما تجاوز مجرد مرحلة البحث.

التكنولوجيا تُمكن البنوك المركزية من ضمان تصميم أي عملة يصدرها بنك مركزي بحيث تنطوي ضمنا على خصائص الأمن السيبراني وحماية الخصوصية على حد سواء.

الخصوصية، يمكن أن تُستخدم هذه البيانات لمراقبة نشاط المدفوعات التي يؤديها الأفراد. وتراكم بيانات شديدة الحساسية في مكان واحد يزيد كذلك من المخاطر الأمنية بجعل المردود الذي يعود على الدخلاء المحتملين أعلى بقدر أكبر بكثير. ومع هذا، يمكن تخفيف المخاطر المقترنة بالجمع المركزي للبيانات إما بعدم جمعها على الإطلاق أو باختيار نظام للتحقق منها بحيث لا يرى كل عنصر فيه إلا مقدار المعلومات اللازمة لأداء وظيفته. ويمكن دعم هذا المنهج الأخير بأدوات تشفيرية مثل الأدلة صفرية المعرفة (zero-knowledge proofs)، والتي تصادق على المعلومات الخاصة دون الكشف عنها ولا تسمح بالتلاعب بها، أو أساليب التشفير التشفيري (cryptographic hashing techniques). فعلى سبيل المثال، مشروع هاميلتون (وهو عمل مشترك بين الاحتياطي الفيدرالي في بوسطن ومعهد ماساتشوستس للتكنولوجيا لاستكشاف إمكانية إصدار عملة رقمية من البنك المركزي في الولايات المتحدة) صمم نظاما يقسم عملية التحقق من المعاملة إلى مراحل، تقتضي كل مرحلة منها الوصول إلى أجزاء مختلفة من بيانات المعاملة. ويمكن زيادة التوسع في التقنيات التشفيرية هذه لبناء نظم تتحقق من صحة المعاملة من مجرد الاطلاع المُشَفَّر (encrypted access) على تفاصيل المعاملة مثل المرسل أو المتلقي أو مقدارها. وبينما تبدو هذه الأدوات جيدة إلى حد لا يكاد يصدق عقل، فقد خضعت لاختبارات مكثفة من خلال عملات مُشَفَّرة تحافظ على الخصوصية مثل "Zcash" وتقوم على تقديم كبير حققه مجتمع التشفير. وخلاصة القول إن التكنولوجيا تُمكن البنوك المركزية من ضمان تصميم أي عملة يصدرها بنك مركزي بحيث تنطوي ضمنا على خصائص الأمن السيبراني وحماية الخصوصية على حد سواء.

الشفافية مقابل الخصوصية

من المخاوف الشائعة بشأن التصميم التي تحافظ على الخصوصية (بما فيها تلك التي تستخدم تقنيات تشفير متخصصة) انخفاض مستوى الشفافية المتاحة للأجهزة التنظيمية. فيقتضي عمل الأجهزة التنظيمية عموما تكوين رؤية كافية لتحديد المعاملات المشتبه بها، مما يمكنها من الكشف عن جرائم غسل الأموال وتمويل الإرهاب وغيرها من الأنشطة غير المشروعة.

تفاصيل حساسة من الناحية الأمنية عن الأفراد والمؤسسات، وحتى في سرقة الأموال. وإذا طُبِّقت بدون وضع بروتوكولات أمنية سليمة، يمكن للعملة الرقمية أن توسع كثيرا من نطاق وحجم العديد من المخاوف الأمنية والمتعلقة بالخصوصية الموجودة بالفعل في النظام المالي اليوم.

وحتى وقت قريب، لم يبذل سوى جهد يسير بشكل علني في عالم الأمن السيبراني والبنوك المركزية لتكوين فهم حقيقي للمخاطر التي تهدد الأمن السيبراني والخصوصية والمصاحبة لإصدار البنوك المركزية لعملات رقمية. ونظر عدد قليل منها فيما إذا كانت تصاميم العملة الرقمية التي يصدرها البنك المركزي يمكنها تخفيف المخاطر أو ربما تحسين الأمن السيبراني في النظام المالي. وبحثنا الجديد، الذي نُشر في تقرير صدر مؤخرا عن المجلس الأطلسي بعنوان "المفتاح المفقود — تحدي الأمن السيبراني والعملات الرقمية الصادرة عن البنوك المركزية" ("Missing Key: The Challenge of Cybersecurity and CBDCs")، يحلل مخاطر الأمن السيبراني الجديدة التي قد تشكلها العملات الرقمية التي تصدرها البنوك المركزية على النظم المالية وتجد من الأسباب ما يبهر وضع خيارات كثيرة أمام صناعات السياسات لإطلاق هذه العملة الرقمية بأمان. وهناك الكثير من الأشكال المتنوعة لتصميم هذه العملة، ما بين قواعد بيانات مركزية وحتى دفاتر الحسابات الرقمية الموزعة والنظم القائمة على رموز. ويتعين النظر في كل نظام على حدة قبل استخلاص نتائج عن مخاطر الأمن السيبراني والخصوصية. ويتعين كذلك المقارنة بين هذه التصميمات والنظم المالية الحالية — تلك التي تقض مضجع باول بصفة مستمرة — لتحديد ما إذا كانت التكنولوجيا الجديدة يمكن أن توفر خيارات أكثر أمانا.

إذن ماهي بعض المخاطر الرئيسية الجديدة التي تهدد الأمن السيبراني والتي يمكن أن تنشأ من إصدار بنك مركزي لعملة رقمية؟ والأهم من ذلك، ما الذي يمكن عمله لتخفيف هذه المخاطر؟

مركزية جمع البيانات

كثير من الأشكال المتنوعة المقترحة لتصميم عملات البنوك المركزية الرقمية (وخاصة العملة لمدفوعات التجزئة) ينطوي على جمع بيانات المعاملات على أساس مركزي، وهو ما يفرض مخاطر كبيرة على الخصوصية والمسألة الأمنية. فمن منظور

الحاجة إلى وضع معايير دولية وزيادة تبادل المعرفة بين البنوك مسألة بالغة الأهمية في هذا الوقت الذي يتسم بسرعة تطور العملة واعتمادها.

الحكومات العديد من الخيارات المتاحة لتصميم العملة الرقمية التي يصدرها البنك المركزي، بما فيها بعض الأشكال المتنوعة الجديدة التي لم تخضع للاختبار بصورة كاملة في العمليات التجريبية التي تنفذها البنوك المركزية حالياً. وتتيح هذه الأشكال المتنوعة مفاضلات مختلفة من حيث الأداء والأمن والخصوصية. وينبغي للحكومات اختيار تصميم يقوم على احتياجات البلد المعنى وأولويات سياساته. وبناء على تقييمنا لهذه المفاضلات، فإن مستوى الأمن الذي تنطوي عليه العملة الرقمية التي يصدرها البنك المركزي لا يختلف كثيراً عن النظم القائمة. وبينما التصاميم التي تتسم بالمسؤولية يجب أن تأخذ الأمن السيبراني في اعتبارها، فلا ينبغي أن يحول ذلك دون النظر فيما إذا كان سيتم تصميم واختبار عملة يصدرها البنك المركزي في المقام الأول.

وهناك أمر واضح جلي في بحثنا. إن تشتت الجهود الدولية لإنشاء عملة رقمية يصدرها البنك المركزي من المرجح أن يتمخض عن تحديات أمام إمكانية التشغيل البيئي وبشكل مخاطر على الأمن السيبراني عبر الحدود. وتركز البلدان بشكل مفهوم على استخدام العملة على المستوى المحلي، ولا تكاد تفكر في تنظيمها عبر الحدود، وإمكانية التشغيل البيئي ووضع المعايير. وبصرف النظر عما إذا كانت الولايات المتحدة ستقرر إطلاق عملة رقمية يصدرها البنك المركزي، كـمصدر لعملة رئيسية للاحتياجات العالمية، فينبغي للاحتياطي الفيدرالي أن يبذل جهوداً كبيرة في قيادة عملية وضع قواعد تنظيمية عالمية داخل أجهزة وضع المعايير للعمليات الرقمية التي تصدرها البنوك المركزية. وللمنتديات المالية الدولية، ومنها بنك التسويات الدولية وصندوق النقد الدولي ومجموعة العشرين دور على نفس الدرجة من الأهمية.

إن المخاطر التي تهدد الأمن السيبراني والخصوصية من إطلاق عملات رقمية تصدرها البنوك المركزية حقيقة واقعة. ولكن الحلول لتجاوز هذه التحديات في متناول التكنولوجيا وصناع السياسات. وسيكون سوء الحظ حليفنا إذا تقرر بشكل مسبق أن المخاطر كبيرة للغاية قبل وضع حلول من شأنها بالفعل المساعدة على الوصول إلى نظام مالي عالمي أحدث وأكثر استقراراً. ¹⁰

جوليا فانتي زميل أول في مركز الاقتصاد الجغرافي التابع للمعهد الأطلسي وأستاذ مساعد في هندسة الكهرباء والكمبيوتر في جامعة كارنيغي ميلون.
جون ليبسكي هو مدير أقدم في مركز الاقتصاد الجغرافي التابع للمعهد الأطلسي وكان يعمل سابقاً في صندوق النقد الدولي.
أولي مور زميل مركز الاقتصاد الجغرافي في المجلس الأطلسي.

ولكن حتى هذه المسألة ليست قراراً اختيارياً. فيمكن استخدام التقنيات التشفيرية في تصميم عملة رقمية يصدرها بنك مركزي تتيح الخصوصية على نحو مشابه للمعاملات النقدية حتى مستوى محدد (١٠ آلاف دولار مثلاً) بينما تسمح للسلطات الحكومية بممارسة قدر كافٍ من الإشراف التنظيمي. ولا يختلف هذا المستوى الحدي عن النظام الحالي المتبع في الولايات المتحدة، والذي يسمح برفض حجم التقارير عن المعاملات التي يقل حجمها عن ١٠ آلاف دولار. والحقيقة هي أن أي نظام جديد لعملة رقمية يصدرها بنك مركزي لا يتعين عليه أن يعيد اختراع بروتوكولات أمنية وإنما يمكنه بدلاً من ذلك تحسين البروتوكولات الموجودة.

وقد تعهد العديد من البلدان بإصدار عملة رقمية من خلال بنوكها المركزية أو ربما أطلق هذه العملة لمدفوعات التجزئة والتي تقوم بنيتها التحتية الأساسية على تكنولوجيا الدفاتر الرقمية الموزعة. ومن الأمثلة الجيدة على ذلك عملة نيجيريا "eNaira" التي أطلقتها في أكتوبر ٢٠٢١. ويقتضي هذا النوع من التصاميم إشراك أطراف أخرى كجهات تتحقق من صحة المعاملات، مما يعني استحداث دور جديد للأطراف الأخرى (مثل المؤسسات المالية وغير المالية) في العمليات النقدية للبنوك المركزية. والأهم من ذلك أن ضمانات أمن الدفتر الرقمي ستتوقف على نزاهة الأطراف الأخرى التي تتحقق من صحة المعاملات وعلى مدى توفرها، والتي قد لا يكون للبنك المركزي سيطرة مباشرة عليها. (برغم إمكانية تطبيق تكنولوجيا الدفاتر الرقمية الموزعة مع سيطرة البنك المركزي على جميع جهات التحقق من صحة المعاملات، الأمر الذي لا يحقق الهدف من استخدام التكنولوجيا إلى حد كبير). ويمكن تخفيف المخاطر المصاحبة باعتماد آليات تنظيمية مثل شروط التدقيق وصرامة شروط الإفصاح عن حالات خرق النظام. ومع هذا، لا توجد وثيقة واضحة لصياغة هذه القواعد التنظيمية ضمن نظام بنفس قدر الحساسية الزمنية والترابط الوثيق اللذين تتسم بهما عملة رقمية صادرة عن بنك مركزي وتقوم على تكنولوجيا الدفاتر الرقمية الموزعة. وهذا هو السبب وراء أهمية الحاجة إلى وضع معايير دولية وزيادة تبادل المعرفة بين البنوك في هذا الوقت الذي يتسم بسرعة تطور العملة واعتمادها.

هل هي مصدر تهديد أم فرص متاحة؟

على مدار الثمانية عشر شهراً الماضية قررت بعض البنوك المركزية في وقت سابق لأوانه أن العملة الرقمية التي يصدرها البنك المركزي تفرض الكثير من المخاطر على الأمن السيبراني والخصوصية. وكنا نرغب في تحديد حقيقة الأمر الذي يشكل تهديداً وذلك الذي يتيح الفرص. وخلصنا إلى نتيجة مفادها أن أمام