كيف ستحمي سلسلة الكتل الكمومية معاملاتك الإلكترونية المستقبلية

اجتاحت العالم تقنية سلسلة الكتل blockchain كوسيلة لتسجيل المعاملات بشكلٍ خفي بين الأفراد. قد تبدو آمنة الآن، ولكنها مسألة وقت قبل أن يتمكن أحدهم من إيجاد طريقة ما للوصول إلى تلك الرسائل المشفرة.

في حين تفتح الحوسبة الكمومية المجال أمام المخترقين وتعطيهم بعض القوى التي تجعل نشاطاتهم خفيةً وغير قابلةٍ للاكتشاف، فإن الطبيعة الحساسة للتشابك **entanglement** قد توفر الفرصة لإبقاء البيانات آمنة من خلال الوصول إلى الماضي ومسح سجلها الخاص.

طور باحثان من جامعة فيكتوريا **Victoria** في ويلينغتون **Wellington** في نيوزيلاندا **New Zealand** مفهومها الخاص لسلسلة الكتل الكمومية والذي من شأنه ـ نظريًا ـ منع أي شخص من تزوير دفاتر حساباتك الإلكتروني دون علمك.

تشتهر تقنية سلسلة الكتل بسبب دورها في الأنظمة الاقتصادية المتعارف عليها بالعملة المشفرة **cryptocurrency**، فبينما ترتبط جنيهاتك ودولاراتك التقليدية بنظام مصرفي تمتلكه الدولة، فإن طرق الدفع بالبتكوين **Bitcoin** تعتمد على شبكة لامركزية من المعاملات المشفرة.

أهم ميزات "دفتر الشيكات" هذا، والذي يستطيع الجميع رؤيته، هي التخلص من أي نوع من أنواع الوساطة البشرية باستخدام مجموعة من الخوارزميات التي تختم المعاملات ختمًا زمنيًا وتقيّم كل عملية تبادل قائمةٍ على العملة عبر سلسلة من الحواسيب المرتبطة بالإنترنت.

تجعل طريقة اتخاذ القرار الموزعة هذه من سلسلة الكتل تقنيةً مثاليةً تمامًا لأي عملية ديمقراطية، بدأً من بناء نظام بنكي يملكه القطاع العام وليس انتهاءً ببناء شركة ليس لها مدير تنفيذي. يعتمد هذا النظام، في المقابل، على شفافية نسبية للكثير من الناس، ما قد يجعله عرضة للاستغلال والاختراق.

تعد هذه المعاملات، حتى اللحظة، مؤمّنة بمستويات تشفير عالية بحيث ستواجه أسرع الحواسيب العملاقة صعوبة بالغة في فكها وستستغرق وقتًا طويلًا لفعل لذلك. المشكلة هي أن الحوسبة الكمومية قد تقلب الموازين، فقد تتمكن الحواسيب الكمومية من اختراق أنظمة التشفير التقليدية قريبًا بوقتٍ قصير باستخدام خوارزمياتٍ معتمدةً على طريقة التخمين الضبابي للحالة الكمومية غير المحددة (بسبب طبيعة البتات الكمومية ـ كيوبت ـ التي تأخذ قيمتي 0 و 1 بنفس الوقت)

تحرز عمالقة التكنولوجيا من مثل غوغل وآي بي ام **IBM** تقدمًا كبيرًا في هذه الأنواع من الحواسيب الكمومية. إنها مثيرة، ولكنها تفتح في الوقت نفسه مستوًا جديدًا للمخاطر. لكن لحسن الحظ، فإن الظاهرة نفسها التي تعطينا القدرة على فك أقوى طرق التشفير، تقدم بدورها طريقة جديدة لتأمين الرسائل والمعلومات من الاختراق.

ما هو التشابك الكمومي؟

في الحقيقة، لا يمكن تحديد الخصائص الكمومية لجسيم ما إذا قمنا بدراستها أو قياسها بشكل مفرد، بل يجب أن تُقاس بطريقة أخرى. الأمر شبيه بقفاز داخل الصندوق، لن تتمكن من تحديد ما إذا كان لليد اليمنى أو اليسرى حتى تنظر إليه.

الأغرب من هذا كله، أنه إذا كان هذا الجسيم مرتبطًا بجسيم آخر في مرحلة زمنية ما، فمراقبة أحد هذين الزوجين تخبرك مباشرةً عن حالة الشريك الآخر (تخيل زوجًا من القفازات يتم سحبها من العلبة نفسها، فمعرفة حالة القفاز الأول ـ وليكن لليد اليمنى ـ ترشدك فوريًا لحالة

القفاز الثاني–يكون لليد اليسرى حتمًا)، بغض النظر عن المسافة بين هذين الجسمين سواء أكانت بضعة ملي مترات أم عدة أميال. وبتحقق هذه المشاهدة، يستقر الجسيم على حالة ما، ليأخذ شريكه شكلًا مكملًا له، وبالتالي يمكن الكشف عن أي اختراق في النظام.

يستخدم التشابك حاليًا في الاتصالات الكمومية لإضافة توقيعات خاصة إلى الاتصالات من شأنها تنبيه المستخدمين في حالة وجد من يتنصت على عملية الاتصال من الخارج.

سلسلة الكتل الكمومية

لم تكن هذه هي المرة الأولى التي تطبق فيها هذه العملية في سلسلة الكتل، حيث توصل باحثون خلال السنة الأخيرة من المركز الروسي الكمومي **Russian Quantum Centre** إلى إنشاء واختراع طريقة لاستبدال طرق التشفير التقليدية بأخرى كمومية.

كتب الباحثون: " من المريع معرفة أنه من الممكن تفسير إجرائية الترميز الخاص بنا كونها تؤثر على الماضي بطريقةٍ غير كلاسيكية. ومن هنا يمكن النظر إلى سلسلة الكتل الكمومية اللامركزية على أنها آلة سفر عبر الزمن مرتبطةٌ كموميًا".

تجعل عملية الختم الزمني الكمومي **quantum time-stamping** من تقنية سلسلة الكتل تقنيةً قويّةً بذاتها عوضًا عن استخدام تقنيات التشفير لحمايتها. فتؤثر محاولة التطفل بأي طريقةٍ على سجلاتٍ موجودةٍ ضمن دفتر حساباتٍ رقمي داخل تقنية سلسلة الكتل الكمومية على تاريخ السجلّ، وبالتالي تغيير جميع السجلات المدخلة في الماضي، وهذا ما يلغي بدوره جميع السجلات المرتبطة كإجرائية حَجزٍ احترازيٍّ رقمية.

يتوفر المقترح للمراجعة على موقع arciv.org لمن يرغب بالاطلاع عليه، الجدير بالذكر أنه لم يخضع للاختبار بعد.

ختامًا، من الذكاء الاستفادة من الكمومية غير المألوفة بعد، وهذا سيضمن بقاء تقنية سلسلة الكتل آمنة في المستقبل.

- التاريخ: 2018-09-21
- التصنيف: تكنولوجيا

#تكنولوجيا #الذكاء الاصطناعي #علوم الحاسوب #البيتكوين

المصطلحات

- **سلسلة الكتل (Blockchain)**: هي لائحة متنامية ومستمرة من الكتل Blocks، مرتبطة مع بعضها ومحمية بمستويات عالية من التشفير، وهي التقنية الأساسية التي تقوم عليها العملات الرقمية.

المصادر

- sciencealert

المساهمون

- ترجمة
  - بنان محمود جوابره

- مُراجعة
  - شريف دويكات
- تحرير
  - ليلاس قزيز
- تصميم
  - أحمد أزميزم
- نشر
  - يقين الدبعي