L'AUTEUR

J.-P. DELAHAYE est professeur à l'Université de Lille et chercheur au Laboratoire d'informatique fondamentale de Lille (LIFL).

vrait aider à découvrir comment se replient diverses protéines, ce qui, pour certaines d'entre elles, serait utile en médecine.

Les preuves de travail sont, on le voit, au cœur d'une petite révolution dont le succès, s'il se confirme, conduira à faire que les calculs réalisés pour la gestion des monnaies cryptographiques serviront la recherche mathématique ou médicale… ce qui n'est bien sûr pas le cas du transport des billets de banque, ni de la fabrication des coffres-forts.

Des jeux « prouvablement équitables »

Le monde des cryptomonnaies, avec ses preuves de travail à base de fonctions à sens unique, a amené la mise en place de casinos en ligne qui ne peuvent pas tricher, chose que le joueur lui-même vérifie sans intervention d'aucune autorité centrale.

Puisque le minage détermine un gagnant parmi les machines participantes et qu'on ne peut pas tricher (sous réserve que la fonction f utilisée possède bien les propriétés requises), on pourrait concevoir des jeux de hasard fondés directement sur le protocole de désignation d'un gagnant de 25 *bitcoins* toutes les dix minutes. Cependant, les chances de gagner d'un joueur dépendraient de la puissance de calcul de sa machine, ce qui ne serait pas juste.

Il existe des méthodes plus directes conduisant à des tirages au hasard parfaitement équitables et contrôlables pour, par exemple, lancer des dés en ligne sans qu'aucune tricherie ne soit possible, ni pour le casino ni pour le joueur. Ces protocoles sont connus depuis longtemps en cryptographie (Manuel Blum a proposé une méthode de tirage à pile ou face par téléphone en 1981), mais c'est seulement depuis peu que des casinos en ligne proposent aux joueurs des jeux « prouvablement équitables ». On peut donc aujourd'hui jouer en ligne à des jeux de hasard dont l'honnêteté est garantie par la cryptographie mathématique, et cela sans faire intervenir aucune autorité de contrôle des casinos auxquels on se connecte. Le paiement des taxes dues par le casino et son honnêteté commerciale (le casino paye-t-il toujours ce qu'il doit aux joueurs ?) ne sont pas garantis par ces protocoles, qui ne concernent que le hasard des tirages aléatoires.

Voici, ci-dessous, un protocole réalisant un tirage au sort ayant une chance sur k de réussir (k étant un entier supérieur ou égal à 2). Pour jouer, vous engagerez la somme S ; si le tirage vous est défavorable, le casino gardera votre mise ; si vous gagnez, le casino vous rendra votre mise, y ajoutera $(k-1)S$, et enlèvera par exemple un pour cent du total pour ses frais.

Protocole prouvablement équitable pour effectuer un tirage ayant une chance sur k de réussir (on prendra k = 2 pour simuler un lancer de pièce à pile ou face).

1) Le casino choisit un nombre x, et envoie le résultat du calcul de $f(x) = y$ au joueur. La fonction f est une fonction à sens unique produisant des résultats assimilables à du hasard, comme c'est le cas de la fonction SHA-256 utilisée par *Bitcoin*.

2) Le joueur envoie au casino un nombre z qu'il choisit comme il veut, éventuellement avec l'aide de son ordinateur.

3) Le casino calcule $t = x + z$, puis $u = f(t) \bmod k$ (le reste de la division de $f(t)$ par k).

4) Si $u = 0$, le joueur a gagné, sinon il a perdu.

5) Après le tirage, le casino fait parvenir x au joueur. Le joueur contrôle que le casino n'a pas triché en vérifiant que le y qu'il avait reçu avant de choisir z est bien $f(x)$; il contrôle aussi les calculs de $t = x + z$ et de $u = f(t) \bmod k$.

Le casino n'a pas pu manipuler le résultat, car, quand il a choisi x, il ne connaissait pas z. Le joueur n'a lui non plus pas pu manipuler le résultat, car, quand il a choisi z, il ne connaissait pas x. Le protocole est donc équitable et il n'existe aucune possibilité de tricherie, ni pour le casino ni pour le joueur.

Les outils de la cryptographie mathématique semblent concerner de plus en plus d'aspects de la vie économique et numérique. Les protocoles à base de preuves de travail et de fonctions à sens unique non seulement conduisent à mieux contrôler ce qui se passe sur les réseaux, mais ouvrent aussi des perspectives nouvelles, comme celles des cryptomonnaies et des jeux prouvablement équitables. ■

BIBLIOGRAPHIE

S. King, **Primecoin : Cryptocurrency with prime number proof-of-work**, 2013 : http://primecoin.org/static/primecoin-paper.pdf

R. Alexander, **Determining electrical cost of Bitcoin mining**, *Bitcoin Magazine*, 18 déc. 2013 : http://bitcoinmagazine.com/8994/determining-electrical-cost-bitcoin-mining/

N. Popper, **Into the bitcoin mines**, *New York Times*, 12 décembre 2013 : http://dealbook.nytimes.com/2013/12/21/into-the-bitcoin-mines/

J.-P. Delahaye, ***Bitcoin*, la cryptomonnaie**, *Pour la Science* n° 434, décembre 2013.

Wikibooks, **Les fonctions de hachage cryptographiques**, http://fr.wikibooks.org/wiki/Les_fonctions_de_hachage_cryptographiques

A. Back, ***Hashcash*, a Denial of Service Counter-Measure**, 2002 ftp://sunsite.icm.edu.pl/site/replay.old/programs/hashcash/hashcash.pdf

C. Dwork et M. Naor, **Pricing via processing or combatting junk mail**, *Advances in Cryptology*, CRYPTO' 92, Lecture Notes in Computer Science, vol. 740, pp. 139-147, 1993.