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. ■

L'AUTEUR

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

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.

HISTOIRE DES SCIENCES

Le monde givré de Bernardin de Saint-Pierre

En 1784, s'opposant à l'idée d'une mer libre au pôle Nord, l'écrivain Bernardin de Saint-Pierre imagina d'énormes masses de glaces polaires dont les cycles de fonte auraient régi la Terre. Il inspira tant les écrivains que les scientifiques.

Frédérique Rémy

À la fin du XVIII[e] siècle, les pôles terrestres et leurs glaces sont peu connus. On imagine le pôle Nord comme une mer libre entourée d'une épaisse barrière de glace, infranchissable. Le mythe s'est forgé à partir de vieilles croyances et de certains récits de voyage, étayés par les naturalistes et autres savants du XVIII[e] siècle. Par exemple, pour le naturaliste Georges-Louis Leclerc, comte de Buffon, qui n'imagine pas que la mer puisse geler, les glaces rencontrées par les marins ne peuvent venir que des continents, charriées par les grands fleuves de l'Arctique. Et à supposer que la mer puisse geler, le mathématicien et encyclopédiste Jean le Rond d'Alembert calcule que l'éclairage permanent du pôle Nord pendant l'été conduit à une température trop élevée pour que soit envisagée une formation de glace.

Le pôle Sud reste, quant à lui, totalement inconnu. Dans les années 1770, le marin anglais James Cook a réalisé la première circumnavigation australe et déclaré à son retour qu'il ne pouvait y avoir de continent vivable plus au Sud. Autant dire que l'on ne connaissait rien des régions polaires et que l'on avait peu d'idées sur la quantité de glace qui s'y trouvait.

En 1784, Jacques-Henri Bernardin de Saint-Pierre a 47 ans. Ingénieur de formation, il a été militaire, a voyagé et fréquenté les salons. Depuis quelques années, il essaie d'écrire, sans grand succès. Toutefois, le vent tourne lorsqu'il publie ses *Études de la nature*, mélange de raisonnement scientifique, d'anecdotes et de souvenirs personnels. Il y bâtit un système cosmogonique extravagant, mais étonnamment cohérent, dont le rôle principal, poussé à l'extrême, est tenu par les glaces polaires.

Les *Études de la nature* ont un succès indéniable. La première édition parue en décembre 1784 est épuisée dès l'année suivante et le livre est réédité plusieurs fois, assurant une notoriété durable à l'auteur. Son roman *Paul et Virginie* est publié quatre ans plus tard. Le système complexe imaginé par Bernardin est fortement critiqué par les scientifiques. Néanmoins, il porte, plus ou moins bien agencés, tous les ingrédients pour influencer durant de nombreuses décennies tant les écrivains que les scientifiques.

Les glaces de Bernardin

Pourquoi tant de glace chez Bernardin ? L'écrivain a sans doute été influencé par Buffon, pour qui la Terre se refroidissait. Selon le naturaliste, les glaces polaires donnaient une image de ce que serait le monde une fois refroidi. Il avait demandé aux géographes, marins et cartographes de l'époque de noter la position de toutes les glaces polaires rencontrées afin d'en suivre l'évolution et d'estimer la vitesse d'englacement de la Terre. Sa vision a beaucoup marqué l'époque, en particulier l'écrivain.

Bernardin est probablement le premier à imaginer une masse considérable de glace autour des pôles, dont « l'effusion » – ainsi nomme-t-il la fonte – contrôle au fil des jours et des saisons tout le système terrestre. Au cours de la journée et de l'année, un pôle est alternativement plus éclairé que l'autre. Ses glaces fondent alors, entraînant une importante masse d'eau vers l'équateur. La fonte diurne entraîne les marées, la fonte annuelle les courants océaniques.

Le système est complexe : ainsi, ce n'est pas l'effusion du jour qui entraîne la marée sur les côtes, mais la succession des effusions, qui, comme « une file de billes placées sur un billard », se propage. Au cours de la saison, la « coupole glaciale du pôle en fusion diminue chaque jour de diamètre », affaiblissant ainsi la puissance du courant, ce qui explique le déphasage de 24 minutes entre deux marées. Les grands courants océaniques sont aussi contrôlés par les glaces : « Les pôles me paraissent être les sources de la mer comme les montagnes à glaces sont les sources des fleuves. »

À partir du chemin parcouru par des épaves de bateaux échoués lors d'un mois de juin en mer du Nord, Bernardin déduit que la vitesse des courants d'été atteint plus de 30 lieues (120 kilomètres) par jour. Un tel courant ne peut qu'être engendré par l'effusion des glaces polaires. Six mois plus tard, les courants sont inversés et remontent vers le Nord en provoquant, entre autres, la mousson. Depuis les travaux d'Isaac Newton (1643-1727), on connaît la cause des marées (l'attraction gravitationnelle exer-