

■ 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.

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 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 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. ■

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'éclairement 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 viable 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-

cée par la Lune et le Soleil sur les masses d'eau]. Et depuis quelques années, les principaux courants marins ont été cartographiés (dont le Gulf Stream, en 1770 par Benjamin Franklin), fournissant des tracés qui ne correspondent pas forcément aux idées de Bernardin. Mais Bernardin a une force de conviction exceptionnelle et l'on voit, avec son système, la Terre respirer et être périodiquement nettoyée et régénérée.

Une coupole large de 2 000 lieues

Afin d'appuyer son propos, Bernardin va jusqu'à évaluer le volume des glaces polaires – et ce à partir de trois méthodes. Pour lui, la forme en œuf de la Terre, déduite de son ombre sur la Lune pendant une éclipse, vient d'une excroissance polaire due à la présence d'immenses masses de glace, ce qui permet d'évaluer leur taille. Une autre méthode peut être appliquée aux glaces de l'hémisphère Nord : Bernardin extrapole l'épaisseur de la couche de neige pendant l'hiver en fonction de la latitude : quelques pouces en France, quelques pieds en Allemagne, quelques toises en Russie...soit quelques centaines de pieds au-delà du cercle polaire ! Pour l'hémisphère Sud, faute de pouvoir s'appuyer sur des relevés similaires, il fonde son évaluation sur la vitesse des courants. Par analogie avec la vitesse des fleuves à leur embouchure et leur dénivelé, il déduit la hauteur de glace de la vitesse des courants marins. Il propose aussi d'utiliser l'intensité des aurores boréales, causées, pense-t-il, par la réfraction de la glace polaire, pour calculer la surface des glaces.

Toujours est-il qu'en dépit d'un manque évident de culture scientifique et d'erreurs de raisonnement, il en arrive à envisager des coupoles de glace de 2 000 lieues de diamètre (8 000 kilomètres) pourvues de flèches de 10 lieues (40 kilomètres) de hauteur, centrées sur chacun des pôles et présentes en alternance. Même si ces chiffres paraissent démesurés à l'époque, ils ne sont pas complètement déraisonnables, sachant que l'Antarctique a un diamètre moyen de 2 000 kilomètres et une épaisseur de quelques kilomètres.

LC-USZ62-126744. Prints and Photographs Division, Library of Congress, USA



DANS SON OUVRAGE

Études de la nature (1784), Jacques-Henri Bernardin de Saint-Pierre (1737-1814), ci-contre, décrit la Terre comme un système complexe gouverné par les cycles de glaciation et de fonte de « coupoles » de glace aux pôles. Selon Bernardin, en fondant alternativement en fonction de leur exposition au soleil, les glaces des pôles seraient notamment responsables de l'apparition de courants océaniques (ci-dessous, représentés pour les mois de janvier et février, soit durant l'été austral).

J.-H. Bernardin de Saint-Pierre, *Études de la nature*, 1784



Dès 1822, le mathématicien Joseph Adhémar s'attaque lui aussi au problème du déluge. Il a lu Bernardin, reprend les mêmes références, raconte les mêmes anecdotes et, surtout, lui emprunte son hypothèse de la fonte puissante des glaces polaires entraînant un flux d'eau extraordinaire qui recouvre tous les continents. En revanche, pour Adhémar, la cause de la fonte est la précession des équinoxes, c'est-à-dire le décalage des équinoxes au fil des ans, connu depuis l'Antiquité. Autrement dit, ce n'est pas la fonte des glaces qui modifie l'axe de rotation de la Terre, mais le mouvement de la Terre qui modifie la fonte des glaces.

La précession des équinoxes est due au changement de direction de l'axe de rotation de la Terre et influe donc sur la durée des saisons. À l'époque de Bernardin (et toujours aujourd'hui), l'orientation de l'axe de rotation de la Terre est telle que la planète est au plus près du Soleil pendant l'été austral (et l'hiver boréal). Aussi l'été austral est-il plus long que l'été boréal, et le climat boréal, plus froid. Les observations des XVII^e et XVIII^e siècles suggèrent une période d'environ 25 000 ans. Adhémar refait le calcul et trouve une période de 21 000 ans : tous les 10 500 ans, un hémisphère donné connaîtra un hiver plus long que l'autre.

Ainsi, la calotte de l'hémisphère qui connaît le plus long hiver grossit lentement, mais sûrement, et 10 500 ans plus tard, l'orbite terrestre est telle que cette calotte fond. L'eau se répand sur toute la Terre et provoque le déluge, tandis que se forme une autre calotte dans l'autre hémisphère, et ainsi de suite. Adhémar pense que cette énorme calotte attire par gravité les eaux vers elle, ce qui explique la différence de profondeur des océans austral et boréal. Il peut ainsi, lui aussi, estimer le volume de la calotte australe. Il trouve une hauteur de 20 lieues, soit environ 90 kilomètres. Publié en 1842, son calcul ne sera réellement lu et repris qu'après réédition, en 1860.

En 1840, le géologue suisse Louis Agassiz publie son *Étude sur les glaciers*, où il montre que les blocs erratiques (ou moraines) retrouvés çà et là, ou que les stries sur certains rochers, sont la preuve de glaciations passées. Peu à peu, dans le

courant du siècle, l'hypothèse de glaciations répétées remplace celle du déluge. Le scénario est alors tout trouvé : la précession des équinoxes entraîne l'avancée périodique des glaces.

Cette année-là aussi, Sébastien Dumont d'Urville découvre l'Antarctique. Il ne connaît pas encore la taille de ce continent, mais, au fil des expéditions polaires, on prendra peu à peu conscience de la masse considérable de cette calotte polaire, pas si éloignée des estimations de Bernardin.

La nature est un immense réseau

La postérité a retenu qu'Adhémar était le découvreur de la cause des glaciations. Ne lui retirons pas le mérite d'avoir eu l'idée judicieuse du rôle de la précession des équinoxes dans les glaciations et d'avoir mathématisé le problème. Néanmoins, n'oublions pas qu'il recherchait surtout les causes du déluge et qu'il a emprunté à Bernardin son scénario. Enfin, pour expliquer les déluges périodiques, il a effectué un calcul tenté à la même époque par de nombreux autres savants, tel le philosophe Jean Reynaud, qui publia un tel calcul en 1841...

Ainsi, le rôle des glaces dans le système terrestre, que l'on sait si capital de nos jours, fut anticipé bien avant que l'on ne découvre les preuves de leur importance actuelle et passée. Certes, l'argumentation de Bernardin a de quoi laisser perplexe. Et en effet, l'écrivain a toujours été rejeté en tant que scientifique. Il a eu toutefois de remarquables intuitions. Il a combattu nombre d'idées fausses de l'époque, qu'il s'agisse du mythe de la mer libre de glace ou du refroidissement terrestre. Il a aussi eu une vision élaborée et complète du cycle de l'eau.

Enfin et surtout, il a bâti un système cohérent dans lequel tous les éléments terrestres se répondent. Pour Bernardin, chaque phénomène sur Terre est lié à un système complexe dont il est à la fois une cause et une conséquence. La nature est un immense réseau dont chaque composante est liée et imbriquée aux autres. Une vision plus que jamais d'actualité. ■

■ L'AUTEUR



Frédérique RÉMY, directrice de recherche au CNRS, est responsable de l'équipe « cryosphère » à l'Observatoire Midi-Pyrénées, à Toulouse.

■ À ÉCOUTER

Le jeudi 3 avril 2014, de 14h à 15h, Frédérique Rémy reviendra sur les glaces polaires imaginées par Bernardin de Saint-Pierre dans la partie Actualités de l'émission *La marche des sciences*, sur France Culture. www.franceculture.com

■ BIBLIOGRAPHIE

F. Rémy, *Le monde givré de Bernardin de Saint-Pierre*, dans J. Ducos (sous la dir.), *Météores et climats d'hier*, Hermann, pp. 81-96, 2013.

F. Rémy, *Histoire des pôles, Mythes et réalités polaires, XVII^e-XVIII^e siècles*, Desjonquères, 2009.

E. Bard, *Greenhouse effect and ice ages : historical perspective*, *C. R. Geoscience*, vol. 336, pp. 603-638, 2004.

La sélection de livres

■ POUR LA SCIENCE

Mathématiques, astronomie, aéronautique...
Découvrez toutes les nouveautés 2014. Partez
explorer l'univers des planètes et des étoiles,
les systèmes dynamiques, la géométrie
et bien d'autres sujets scientifiques...

Nouveauté



Le cerveau mélomane

Sous la direction d'Emmanuel Bigand

Réf. 84245118

La musique ne laisse personne indifférent et suscite de multiples émotions. Ce que l'on sait moins, c'est la puissance de la musique. Elle a des effets positifs sur les capacités cognitives et intellectuelles de ceux qui en écoutent souvent ou qui la pratiquent ; mais elle a aussi des effets thérapeutiques chez certains sujets.

Éditions Belin-Pour la Science 2013 – 200 pages – 21 euros – ISBN 978-2-8424-5118-9

Nouveauté



Les mille et une nuits de la science

Philippe Boulanger

Réf. 70118964

Quand Schéhérazade conte la science et les tribulations des savants ! Ce pastiche est une manière totalement originale de raconter la science, en abordant des sujets aussi divers que les mathématiques, la physique, la paléontologie, etc.

Éditions Belin 2014 – 160 pages – 15 euros – ISBN 978-2-7011-8964-2

Nouveauté



L'exploration des planètes

Thérèse Encrenaz et James Lequeux

Réf. 70116195

En retraçant la conquête pacifique du système solaire, ce livre met à la portée d'un large public les démarches et les résultats des générations d'astronomes qui se sont succédé depuis Galilée. Il ouvre sur une nouvelle dimension de la planétologie avec la découverte récente de près d'un millier d'exoplanètes... où peut-être d'autres formes de vie seront détectées ?

Éditions Belin 2014 – 224 pages – 23 euros – ISBN 978-2-7011-6195-2

Nouveauté

Concorde 001 et l'ombre de la Lune

Pierre Léna

Réf. 74650728*



Lors de l'éclipse totale du 30 juin 1973, sept scientifiques ont embarqué à bord de Concorde 001, prototype d'essais d'un avion extraordinaire qui sera le premier supersonique commercial. La science, la technique, l'aéronautique et l'histoire se marient dans le récit d'une aventure humaine singulière à bord d'un avion légendaire, illustré d'une iconographie riche et originale.

Éditions Le Pommier 2014 – 160 pages
17 euros – ISBN 978-2-7465-0728-9

Ce que disent les étoiles

Danielle Briot
et Noël Robichon

Réf. 70116285



Qu'est-ce qu'une étoile et par quel mécanisme brille-t-elle ? Comment naît une étoile, comment meurt-elle ? Qu'est-ce qu'un pulsar, une naine brune, une supernova ? Ce livre, signé de deux astronomes de l'Observatoire de Paris, propose un vaste panorama de l'astrophysique des étoiles en une trentaine de sujets de quatre pages chacun, abondamment illustrés de photographies époustouflantes.

Éditions Belin 2013 – 160 pages
25 euros – ISBN 978-2-7011-6285-0

En partenariat avec les éditeurs

Belin:
ÉDITEUR INDÉPENDANT
DEPUIS 1777

Le Pommier

Pour commander ces ouvrages www.pourlascience.fr/librairie *

ou en renvoyant le bon de commande ci-contre.

* Pour commander les titres édités par Le Pommier : www.editions-belin.fr