

3. L'inversion d'une fonction de hachage

Expliquons une méthode pour définir et ajuster l'énigme d'une preuve de travail.

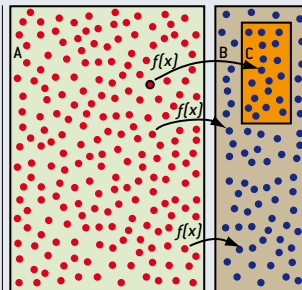
La fonction f de hachage transforme une suite x de 0 et de 1 de longueur quelconque en une autre, y , de longueur 256 (comme le SHA-256). Puisqu'il est impossible en pratique de trouver pour un y donné un x tel que $f(x) = y$ (inversion complète de f), on crée une énigme plus raisonnable et exigeant un travail faisable en ne demandant qu'une inversion partielle de f : trouver un x tel que $f(x)$ soit une suite de caractères commençant par k fois '0' (donc une suite de la forme $000\dots0a_1a_2a_3\dots a_n$).

Plus k est grand, plus il sera difficile de trouver un x satisfaisant. On peut même être plus précis: pour trouver un tel x , il faut en moyenne essayer environ 2^k valeurs de x . L'énigme « trouver un x tel que $f(x)$ commence

par dix fois '0' » exige donc environ $2^{10} = 1024$ calculs de $f(x)$. Pour 20 fois '0', il en faudrait un million environ. En choisissant k , on ajuste donc la difficulté de l'énigme qu'on formule. On a là une méthode rapide pour formuler des énigmes de « preuve de travail » dont la difficulté est facile à évaluer.

Dans les preuves de travail (pour se protéger des spams, ou interdire les attaques par déni de service), il faut éviter que les mêmes énigmes soient soumises plusieurs fois. Si c'était le cas, des bibliothèques de solutions seraient calculées par avance et les attaquants, au lieu de faire les calculs attendus, se contenteraient d'aller y puiser les solutions des problèmes qu'on leur soumet.

Pour éviter cela, on fait dépendre l'énigme posée d'un paramètre p . On demandera par exemple de trou-



La fonction f envoie les éléments x de l'ensemble A [grand] dans l'ensemble B [petit]. Inverser partiellement f , c'est trouver un élément x tel que $f(x)$ soit dans C . Plus C est petit, plus la tâche est difficile.

ver un x commençant par la chaîne $p = 0100011010100$ et tel que $f(x) < y$.

Le nombre de paramètres possibles p étant illimité, l'idée de constituer des bibliothèques de so-

lutions calculées par avance n'est plus applicable.

Les énigmes possibles posées par la méthode de l'inversion partielle des fonctions de hachage sont donc à la fois parfaitement ajustables, et si nombreuses que celui à qui on les propose ne peut que se soumettre et faire le travail de les résoudre en essayant de très nombreux x , ce qui en moyenne lui prendra le temps qu'on aura choisi. Quand il aura trouvé la solution, il aura vraiment prouvé qu'il a travaillé !

Notons encore que si l'on est gêné par le fait que le temps de travail varie trop, selon que celui qui tente de résoudre le problème posé a de la chance ou pas (variance importante), on peut remplacer la demande de résoudre un problème, par la demande de résoudre plusieurs petits problèmes, ce qui a pour effet de diminuer la variance du temps nécessaire pour aboutir.

durée moyenne est de dix minutes, mais elle sera plus longue ou plus courte selon que les mineurs auront eu de la chance ou pas dans leur tentative de résolution du problème de la preuve de travail.

Une course folle à la puissance...

Si chaque machine n'utilisait que sa propre puissance pour gagner, la probabilité pour chacune de gagner serait proportionnelle à sa puissance. Cependant, comme la fonction f est fixée et connue de tous, le problème de trouver un x tel que $f_p(x) < y$ est très particulier. Les personnes intéressées par le minage des *bitcoins* se sont mises à utiliser des puces conçues spécialement pour résoudre rapidement le type particulier de problèmes posés dans les preuves de travail de *Bitcoin*. Une course folle à la puissance de minage en a résulté, conduisant à une véritable industrie du minage !

La puissance de minage d'un système informatique se mesure en comptant le

nombre de calculs de type $x \rightarrow f(x)$ que le système est capable de faire par seconde, pour la fonction SHA-256. On est ainsi passé de 24×10^{12} calculs de valeurs de f par seconde pour l'ensemble des mineurs en janvier 2013 à 11×10^{15} en janvier 2014, soit une multiplication par plus de 500 en un an.

Le coût en électricité de ces minages (coût des « preuves de travail ») a été évalué. Certains ont calculé qu'il est de plus de dix millions d'euros par jour. C'est plus que la valeur des *bitcoins* gagnés chaque jour (environ deux millions d'euros). Les spécialistes ne sont pas d'accord sur ce nombre de dix millions, mais, même imprécis, il signifie qu'être mineur de *bitcoins* aujourd'hui n'est pas nécessairement rentable. Acheter du matériel et dépenser de l'électricité en le faisant fonctionner est un pari risqué, dont le succès dépend de deux facteurs très difficiles à contrôler ou même à anticiper: la puissance de calcul de vos concurrents, et le cours extrêmement volatil du *bitcoin*.

Notons que certains pirates informatiques ont conçu des programmes, nommés

chevaux de Troie, qui s'installent par le biais du réseau sur une multitude d'ordinateurs (le vôtre peut-être) et leur font exécuter le minage. Bien évidemment, lorsque le minage réussit, la solution est transmise au pirate qui, pour son propre compte, touche les 25 *bitcoins*. C'est vous qui payez l'électricité, mais c'est lui qui empêche le bénéfice !

...et un énorme gâchis ?

Parmi les nombreuses critiques formulées à l'encontre de *Bitcoin*, l'une d'elles concerne justement les preuves de travail qui définissent le minage. Les sommes d'argent considérables dépensées en électricité et pour fabriquer du matériel spécialisé calculant le plus rapidement possible des $f_p(x)$ semblent absurdes, car en soi de tels calculs ne servent à rien. N'est-ce pas là un gâchis terrifiant, engendrant par ailleurs une importante pollution liée à l'électricité consommée, qu'il faut bien produire ?

Une double réponse a été donnée à cette critique. D'une part, il a été répliqué

que les moyens dépensés pour le minage n'étaient pas vains, puisqu'ils permettent à ces monnaies de fonctionner. Fabriquer des billets de banques, les transporter dans des véhicules blindés, les enfermer dans des coffres que l'on fait garder : tout cela coûte cher et pourtant personne ne conteste la nécessité de ces dépenses puisqu'elles servent à faire fonctionner les monnaies fiduciaires habituelles émises par les banques centrales. Le *bitcoin* n'a pas besoin d'être imprimé (c'est une monnaie numérique), il n'y a pas besoin de voitures blindées pour son transport, mais il faut que sa gestion soit assurée. Le minage assure en partie cette gestion, qui n'est donc que l'équivalent des dépenses de fonctionnement des autres monnaies et n'a finalement rien d'absurde.

Concevoir des preuves de travail utiles

L'autre réponse est plus intéressante, elle est aujourd'hui encore en discussion. Les preuves de travail les plus habituelles (dont celle utilisée par *Bitcoin*) consistent à faire des calculs pour résoudre un problème qui, malheureusement, est sans intérêt réel : une fois que l'on a trouvé un x tel que $f_p(x) < y$, ce x n'est utile à personne et ne le sera sans

doute jamais. Ne pourrait-on pas concevoir des preuves de travail fondées sur des problèmes dont la solution serait utile ?

On le sait, les mathématiciens aiment les nombres premiers dont la connaissance progresse et est utile (en particulier en cryptographie !). Divers groupes de nombres premiers sont jugés intéressants. Les paires de nombres premiers jumeaux sont les paires $[p, p + 2]$ de nombres premiers ayant un écart de deux unités, par exemple $[17, 19]$. On cherche toujours à prouver qu'il en existe une infinité. Il y a aussi les paires de nombres premiers de Sophie Germain (mathématicienne française qui vécut de 1776 à 1831) qui sont de la forme $[p, 2p + 1]$, par exemple $[3, 7]$, $[5, 11]$, $[11, 23]$. Elles conduisent aux chaînes de Cunningham $[p_1, p_2, \dots, p_k]$ où chaque couple $[p_i, p_{i+1}]$ est une paire de nombres de Sophie Germain : $p_2 = 2p_1 + 1$, $p_3 = 2p_2 + 1$, ..., $p_{k+1} = 2p_k + 1$, chaque p_i étant un nombre premier.

Des chercheurs tiennent à jour des sites Internet qui indiquent les records de longueur des chaînes de Cunningham. Sunny King a montré en 2013 qu'une telle recherche peut servir de base à des preuves de travail aux propriétés à peu près équivalentes à celles provenant des fonctions à sens unique.

S. King a créé en juillet 2013 sa propre cryptomonnaie, *Primecoin*, proche dans sa conception de *Bitcoin*, mais utilisant des preuves de travail qui conduisent à des chaînes de Cunningham nouvelles. Des chaînes de Cunningham records, de longueur 10, 11, 12 et 13, ont ainsi été découvertes, ce qui prouve l'efficacité de la méthode proposée et sa capacité à contribuer à la recherche mathématique.

Précisons toutefois que l'intérêt de connaître des chaînes de Cunningham n'est pas très grand, et que la sûreté des preuves de travail fondées sur leur recherche n'est pas aussi bonne que celle des preuves de travail fondées sur les fonctions à sens unique. Les utilisateurs des cryptomonnaies ont cependant fait bon accueil à cette nouveauté. Parmi toutes les cryptomonnaies existantes (il y en a aujourd'hui plus de 80, voir <http://coinmarketcap.com/>), *Primecoin* se classe onzième pour la capitalisation. Le total des *primecoins* émis vaut dix millions de dollars (le 7 février 2014). Qui a dit que les mathématiques n'étaient pas un bon moyen de gagner de l'argent ?

Un autre projet en cours de développement, nommé *Curecoin*, tente de concevoir une preuve de travail (et une cryptomonnaie associée) qui soit beaucoup plus clairement utile. Le calcul mené par les machines de-

4. Des preuves de travail utiles

Les preuves de travail utilisées aujourd'hui ont un côté absurde : on demande aux ordinateurs de résoudre des problèmes mathématiques qui n'ont aucun intérêt. Sunny King (pseudonyme d'une personne ou d'un groupe) a conçu une preuve de travail aussi facile à ajuster que l'inversion partielle des fonctions de hachage cryptographiques et qui permet de trouver des chaînes de nombres premiers intéressantes : les chaînes de Cunningham.

Ce sont des suites de nombres premiers $(p_1, p_2, \dots, p_k)$ vérifiant : $p_2 = 2p_1 + 1$, $p_3 = 2p_2 + 1$, ..., $p_{k+1} = 2p_k + 1$. Ces chaînes de Cunningham sont reliées aux nombres pre-

miers de Sophie Germain, une mathématicienne française (1776-1831) : un nombre premier p est un nombre premier de Sophie Germain si $2p + 1$ est aussi un nombre premier.

Ces nombres premiers particuliers ont un intérêt en raison d'un théorème de Sophie Germain lié au théorème de Fermat. Dans les chaînes de Cunningham, tous les nombres sont des nombres de Sophie Germain, sauf le dernier.

L'utilisation de ces preuves de travail où l'on recherche des nombres premiers est au cœur du fonctionnement de la cryptomonnaie *Primecoin*, concurrente de *Bitcoin*. Le travail de minage de *Primecoin* a au-



Sophie Germain à l'âge de 14 ans, portrait de Auguste Eugène Leray.

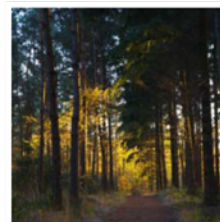
jourd'hui produit plusieurs chaînes nouvelles intéressantes. La chaîne de Cunningham de longueur 11 comportant les plus grands nombres premiers est l'une d'elles. Le premier nombre de cette chaîne record découverte le 3 août 2013 comporte plus de 200 chiffres. Il s'écrit :

$p_1 = k \times 151\# - 1$,
où $k = 73\ 853\ 903\ 764\ 168\ 979\ 088\ 206\ 401\ 473\ 739\ 410\ 396\ 455\ 001\ 112\ 581\ 722\ 569\ 026\ 969\ 860\ 983\ 656\ 346\ 568\ 919$
et où 151# désigne le produit des nombres premiers inférieurs ou égaux à 151 (voir http://users.cybercity.dk/~dsl522332/math/Cunningham_Chain_records.htm).



Master 2

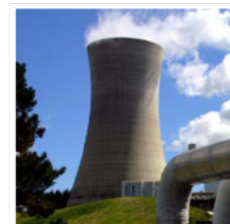
Économie Énergie Développement Durable



Deux parcours distincts

• **Le master Professionnel** forme de futurs cadres spécialistes de l'énergie pour des entreprises énergétiques, des grandes entreprises hors énergie, des cabinets de consultants, des collectivités territoriales et des organismes internationaux.

• **Le master Recherche** initie l'étudiant à la recherche en vue de son admission en thèse.



CONTENU

1^{er} semestre : commun aux parcours Professionnel et Recherche

Fondamentaux de l'énergie
Climat et énergie
Marchés énergétiques internationaux
Industries de réseau
Stratégies et politiques d'innovation
Anglais pour l'énergie / autre langue vivante

2^e semestre, parcours Professionnel

Institutions internationales et énergie
Politiques territoriales énergie-climat
Approches sectorielle et technologique énergie-climat
Stage

2^e semestre, parcours Recherche

Economie de l'énergie
Environnement et innovation
Approches expérimentales
Mémoire

DÉBOUCHÉS

Chargé de mission ou de projets énergie
Analyste de marché énergétique
Responsable énergie
Expert-conseil énergie-climat
Economiste de l'énergie et de l'environnement
Enseignant-chercheur

INTERVENANTS

Conférenciers de renom
Enseignants et chercheurs de l'équipe
Economie du Développement Durable et de l'Energie (CNRS-PACTE-EDDEN) et de
Grenoble Applied Economics Laboratory (INRA-GAEL)



Les + du Master 2 EEDD

- Formation présentielle en alternance
- Formation à distance
- Large réseau de partenaires

POUR PLUS D'INFORMATION

<http://www.upmf-grenoble.fr/master2-EEDD>
contact : odile.blanchard@upmf-grenoble.fr

Université Pierre-Mendès-France
Faculté d'Économie
1241 rue des Résidences
F - 38400 Saint-Martin-d'Hères

