

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).