

R

ENDEZ-VOUS

P.80 Logique & calcul
P.86 Art & science
P.88 Idées de physique
P.92 Chroniques de l'évolution
P.96 Science & gastronomie
P.98 À picorer

DES CRYPTO-MONNAIES SOBRES EN ÉNERGIE ?

Un problème de récréation mathématique met en lumière la difficulté à concevoir des cryptomonnaies justes, économes et écologiques.

L'AUTEUR



JEAN-PAUL DELAHAYE
professeur émérite
à l'université de Lille
et chercheur au
laboratoire Cristal
(Centre de recherche
en informatique, signal
et automatique de Lille)

U

n débat fait rage depuis une dizaine d'années concernant les méthodes de sécurisation des cryptomonnaies anonymes. Il concerne le système Bitcoin et ses concurrents principaux Ethereum, Cardano ou Solana et a pris une importance de plus en plus grande avec la montée de leurs cours. De la conclusion qu'on tirera de ce débat dépendra sans doute l'avenir des cryptomonnaies et plus généralement des cryptoactifs dont l'impact écologique s'accroît gravement aujourd'hui.

Le problème posé peut s'expliquer en considérant un jeu assez simple qui dégage le problème de son contexte un peu confus. Ce jeu permet à chacun de comparer les deux solutions principales et peut-être d'en imaginer de nouvelles. Voici ce « jeu du mécène et des enveloppes anonymes ».

DISTRIBUER AU MIEUX DE L'ARGENT

Imaginez qu'un riche mécène vous confie une certaine somme S , par exemple 1 million d'euros, en vous demandant de la distribuer. Vous êtes chargé d'organiser une sorte de jeu pour répartir le plus équitablement possible la somme S entre les gens qui acceptent de recevoir une part de cet argent. Vous leur demandez de manifester leur souhait en vous faisant

parvenir à un lieu fixé une enveloppe avec une adresse, dans laquelle vous mettrez ce que vous leur attribuez avant de renvoyer l'enveloppe à l'adresse inscrite.

Si vous collectez N enveloppes, la méthode qui vient immédiatement à l'esprit consiste à mettre S/N euros dans chacune des enveloppes et à les renvoyer.

La « méthode S/N » n'est pas parfaite, car les personnes ayant plusieurs domiciles pourraient mettre plusieurs enveloppes à leur nom avec des adresses différentes, ce qui vous empêcherait de savoir que l'argent ira à la même personne. Il y a pire : le mécène vous a demandé de concevoir une méthode qui n'oblige pas ceux qui veulent recevoir une part de S à transmettre leur adresse véritable. Vous acceptez donc que des joueurs se regroupent sur une même adresse et vous soumettent des enveloppes avec des adresses anonymes du type « joueur 237 au 11, rue Dupont, à Paris ».

Vous comprenez bien que si vous utilisez la méthode S/N , chaque joueur sera tenté d'envoyer une multitude d'enveloppes dont les contenus lui seront destinés. Il utilisera plusieurs adresses, ou une seule adresse A en prenant le rôle du joueur 1, du joueur 2, etc. de l'adresse A . Si vous utilisez la méthode S/N , vous allez donc recevoir des milliers



Jean-Paul Delahaye a notamment publié : **Les Mathématiciens se plient au jeu**, une sélection de ses chroniques parues dans *Pour la Science* (Belin, 2017).

LE JEU DU MÉCÈNE ET DES ENVELOPPES

Un mécène veut distribuer une somme S le plus équitablement possible. Il reçoit des enveloppes dans lesquelles il répartit S . La question est de savoir quelle est la meilleure méthode.

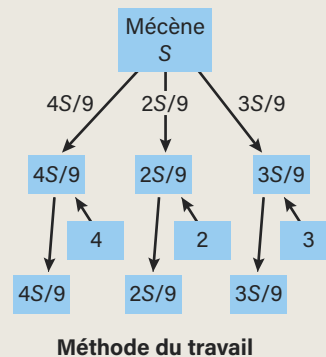
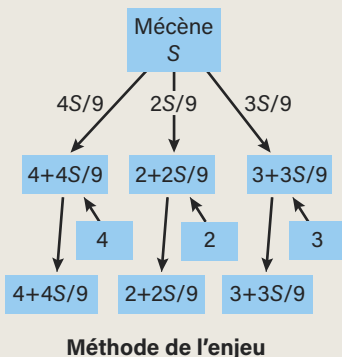
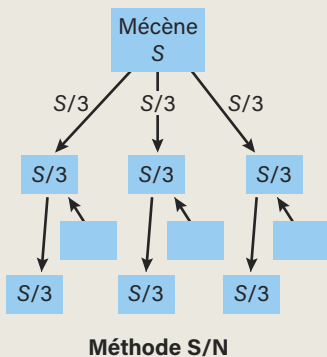
• **Méthode S/N**
S'il reçoit N enveloppes, il dépose dans chacune S/N

et les renvoie. Ceux qui ont envoyé plusieurs enveloppes sont favorisés.

• **Méthode de l'enjeu**
Le mécène exige que chacun risque un enjeu en mettant une somme dans son enveloppe. Il renvoie les enveloppes en y laissant l'enjeu, et en y ajoutant une partie de S proportionnelle

à l'enjeu trouvé dans l'enveloppe.

• **Méthode du travail**
Il demande qu'on joigne à l'enveloppe un ruban difficile à fabriquer. Il détruit le ruban, et place dans l'enveloppe une partie de S proportionnelle à la longueur du ruban trouvé dans l'enveloppe.



d'enveloppes, peut-être des millions, et les plus malins seront ceux qui auront envoyé le plus grand nombre d'enveloppes pour eux-mêmes et s'approprieront une grande part de la somme S . Les plus gros tricheurs seront favorisés aux dépens de ceux, honnêtes, qui n'auront envoyé qu'une enveloppe. Comment éviter cela ?

Ce n'est pas facile. S'il n'y a aucune façon parfaite pour résoudre le problème, plusieurs méthodes organisent la distribution en rendant inopérante la tricherie de l'envoi de plusieurs enveloppes et en assurant une certaine équité entre les joueurs. Nous verrons plus loin que cette petite énigme mathématique est la transposition du problème du consensus dans les blockchains anonymes de cryptomonnaies (des bases de données détenant toutes les informations sur l'état de tous les comptes).

SOLUTION 1. LA MÉTHODE DE L'ENJEU

Vous demandez à chaque joueur de joindre à son enveloppe une certaine somme d'argent. Vous distribuez alors la somme S dans les enveloppes en proportion des sommes qui ont été jointes et en laissant la somme envoyée qui est donc retournée à l'envoyeur. En clair : si l'enveloppe E_i contient la somme s_i , vous laissez s_i dans l'enveloppe, vous y ajoutez $S \times s_i / (s_1 + \dots + s_n)$, puis vous renvoyez l'enveloppe.

On vérifie immédiatement que cela constitue bien une distribution totale de S . Ceux qui ont manifesté un soutien plus fort au jeu et donc une bonne confiance en son organisateur en mettant des sommes importantes dans leur

enveloppe sont favorisés proportionnellement au risque pris. Ce n'est pas absurde car justement vous voulez favoriser ceux qui soutiennent le jeu et ont confiance en vous. Le point important est que cette méthode rend inopérant l'envoi de plusieurs enveloppes par une même personne car si quelqu'un envoie, par exemple, deux enveloppes avec 10 euros dans chacune, le gain qu'il en tirera sera le même qu'avec une enveloppe contenant 20 euros. Le gain d'un joueur est proportionnel à ce qu'il est prêt à engager – la somme des s_i de ses enveloppes – et ne dépend pas du nombre d'enveloppes qu'il envoie. Utiliser plusieurs enveloppes plutôt qu'une ne fait rien gagner. Nous nommerons cette organisation de la distribution « La méthode de l'enjeu » car la somme mise par un joueur dans une enveloppe est comme un enjeu qu'il risque.

SOLUTION 2. LA MÉTHODE DU TRAVAIL

Une seconde idée évite aussi que des tricheurs envoient plusieurs enveloppes. L'organisateur de la distribution demande à chaque joueur de réaliser un ruban de dentelle brodée d'un type précis. Le joueur en fabrique la longueur qu'il souhaite, ce qui lui prend du temps, il met le bout de ruban dans l'enveloppe qu'il envoie à l'organisateur du jeu.

Certains joueurs enverront 10 centimètres de ruban, d'autres joueurs 1 mètre, etc. La distribution de la somme se fera alors en proportion de la longueur des rubans de chaque enveloppe et les rubans seront détruits. Si l'enveloppe E_i contient un ruban de longueur L_i ,