

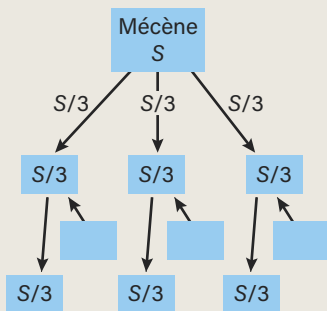
LE JEU DU MÉCÈNE ET DES ENVELOPPES

1

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

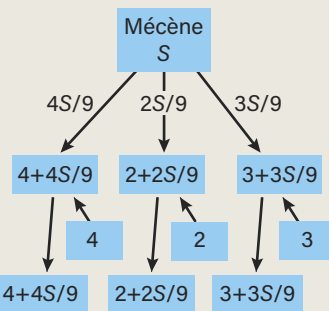


Méthode S/N

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

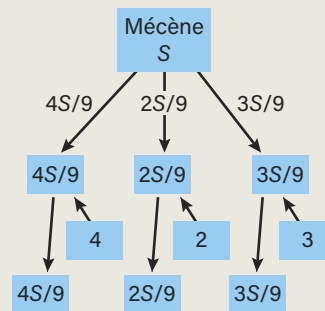


Méthode de l'enjeu

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.



Méthode du travail

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'approprièrent 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 ,

après l'avoir vidée de son ruban et avoir détruit le ruban, l'organisateur y placera la somme $S \times L_i / (L_1 + \dots + L_n)$ et la renverra. Comme précédemment, la méthode rend inopérant l'envoi de plusieurs enveloppes par un même joueur car, en envoyant deux enveloppes avec 10 centimètres de ruban, il gagnera autant qu'en envoyant une seule enveloppe avec 20 centimètres de ruban. Il y a un travail à faire pour réaliser le ruban en dentelle, c'est une mesure de confiance que le joueur accorde à l'organisateur de la distribution et un engagement de sa part. Le travail de fabrication du ruban qu'il met dans son enveloppe détermine le gain d'un joueur. Plus un joueur travaille à fabriquer un long ruban plus il reçoit une part importante de S . On nommera cette méthode « La méthode du travail ».

DES MÉTHODES ÉQUIVALENTES ?

On peut imaginer d'autres méthodes mais ce n'est pas facile et aucune n'est parfaite, aucune ne permet d'assurer que chaque joueur gagne la même partie de S . Dans un premier temps, comparons « La méthode de l'enjeu » et « La méthode du travail ».

Posons-nous deux questions. Est-ce que les deux méthodes sont équivalentes l'une à l'autre, ou l'une est-elle meilleure ? Que se

passé-t-il si la distribution de la somme S est répétée toutes les semaines pendant une longue période ?

La méthode de l'enjeu favorise ceux qui sont assez riches pour joindre à leur enveloppe une somme importante. Mais la méthode du travail souffre du même inconvénient, car si vous êtes riches, vous paierez d'autres personnes pour faire de grandes longueurs de ruban qui vous permettront de gagner plus. Sur ce plan, les deux méthodes se valent, elles favorisent ceux qui ont les moyens de s'engager et prennent le risque de le faire.

Quand la distribution des S euros est opérée chaque semaine par la méthode de l'enjeu, il se produit quelques petits changements au cours du temps. Une fois persuadés que le jeu est sérieux, un nombre plus grand de joueurs y participent, certains joueurs empruntent de l'argent pour pouvoir s'engager plus et gagner plus. L'évolution principale est sans doute une augmentation globale des sommes engagées de semaine en semaine.

Si on suppose que la distribution est opérée par la méthode du travail, il se produit un phénomène très différent, mais assez simple à analyser, car il s'agit d'un problème élémentaire d'économie. Certains joueurs développent des moyens pour produire le plus de rubans de

2

LE FONCTIONNEMENT DES CRYPTOMONNAIES ANONYMES

Une cryptomonnaie s'appuie sur un réseau de validateurs indépendants qui s'occupent, chacun, de garder le registre des comptes (dénommé « fichier blockchain ») et de le mettre à jour en accord avec les autres validateurs. Pour que la monnaie puisse circuler et qu'elle soit bien sécurisée, il faut qu'il y ait assez de validateurs. On rémunère donc les validateurs pour ce travail. Ce paiement s'opère souvent en créant de nouvelles unités de la cryptomonnaie, et en demandant aux utilisateurs du réseau (ceux qui détiennent des comptes) de payer des commissions quand ils font des opérations sur leurs comptes. Ce sont ces nouvelles unités et ces commissions qui constituent la somme S que le réseau distribue aux validateurs. Sur le schéma, les validateurs sont au centre du réseau, les utilisateurs à l'extérieur. La distribution de S se fait périodiquement, par exemple toutes les 10 minutes pour

le réseau Bitcoin. Lorsque les validateurs sont bien identifiés, la distribution de S est facile, par exemple par la méthode S/N : chacun des N validateurs reçoit S/N . Lorsque les validateurs sont anonymes une tricherie est à craindre : que chaque validateur apparaisse plusieurs fois, voire des centaines de fois car l'anonymat rend impossible de savoir si des validateurs apparemment différents le sont réellement. C'est ce

qu'on dénomme « une attaque Sybil ». Pour éviter l'injustice que créent de telles attaques, il faut trouver autre méthode que celle de S/N .

Une idée est souvent utilisée : on demande à chaque validateur V_i d'engager une somme s_i , puis de la mettre sous séquestre. La distribution se fait en proportion des s_i . La méthode se dénomme « la preuve d'enjeu ». Satoshi Nakamoto (c'est un pseudonyme), l'inventeur des cryptomonnaies,

a proposé la méthode de la « preuve de travail », qui consiste à demander à chaque validateur V_i de réaliser un travail de calcul en choisissant et en mettant en œuvre une puissance de calcul c_i , plus ou moins importante. La distribution se fait en proportion des c_i . La preuve de travail et la preuve d'enjeu résolvent le problème des attaques Sybil, mais elles produisent des effets économiques très différents.

