après l'avoir vidée de son ruban et avoir détruit le ruban, l'organisateur y placera la somme $S \times L_i/(L_1+...+L_n)$ 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 passe-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.