l'argent au profit de l'organisateur. Cette méthode pourrait être intéressante pour l'organisateur, mais pour notre problème où le mécène veut vraiment donner S, cette option amusante n'a pas d'intérêt.

La variante selon laquelle l'argent des enjeux est donné à une organisation caritative est sympathique. Elle revient à forcer les joueurs à abandonner une part de leurs gains en la donnant à l'organisation caritative, mais ce n'est pas le but du mécène.

Rien ne semble sensiblement mieux que les deux premières méthodes décrites, mais si des lecteurs en imaginent d'autres plus satisfaisantes, ils peuvent me le signaler.

VARIANTES PROBABILISTES

La méthode de l'enjeu et la méthode du travail ont chacune une variante probabiliste essentiellement équivalente. Elles vont nous approcher encore un peu plus du problème réel des cryptomonnaies. Si la distribution du mécène se déroule un très grand nombre de fois, par exemple toutes les heures pendant des années, au lieu de distribuer la somme S en la fractionnant, l'organisateur du jeu pourrait choisir de la distribuer à l'une des enveloppes, qui serait désignée au hasard en utilisant la distribution de probabilité fixée par les sommes distribuées avec la méthode de l'enjeu, ou la méthode du travail.

Si par exemple la méthode de l'enjeu fixe que l'enveloppe 1 reçoit 1/4 de S et que l'enveloppe 2 reçoit 3/4 de S (il n'y a que deux enveloppes pour l'exemple), la « méthode de l'enjeu probabiliste » choisit de donner S à l'enveloppe 1 avec une probabilité de 1/4 et de donner S à l'enveloppe 2 avec une probabilité de 3/4. L'organisateur jette par exemple un dé tétraédrique et donne S à l'enveloppe 1 si le 1 sort et donne la somme S à l'enveloppe 2 si le 2, le 3 ou le 4 sort. La répétition de l'utilisation du tirage au sort produit à la longue une attribution de 1/4 de l'argent distribué au premier joueur, et de 3/4 au second.

Sur le long terme, « la méthode probabiliste de l'enjeu » est donc équivalente à la méthode de l'enjeu. De même, « la méthode probabiliste du travail » est équivalente à la méthode du travail. Les raisonnements proposés plus haut pour les comparer s'appliquent et conduisent à la conclusion que la méthode probabiliste du travail engendre une situation absurde de gâchis économique.

LE CAS DES CRYPTOMONNAIES

Nous sommes maintenant arrivés au problème posé par les blockchains anonymes des cryptomonnaies. Le réseau qui fait fonctionner une cryptomonnaie (Bitcoin, Ethereum, Cardano, Solana, etc.) distribue périodiquement une certaine somme d'argent pour qu'il y ait des joueurs, qui ici sont les validateurs du réseau, c'est-à-dire ceux qui le font fonctionner. Le réseau les rémunère parce que le réseau existe grâce à eux et que plus ils sont nombreux plus le réseau est décentralisé, ce qui est jugé souhaitable.

La rémunération provient soit de nouvelles unités monétaires que le réseau crée, soit des commissions que les utilisateurs paient quand ils utilisent le réseau et qui naturellement vont à ceux qui le font fonctionner. C'est la logique du modèle économique de tels réseaux décentralisés : certains paient pour l'utiliser, d'autres sont

© Marco Krohn/Wikimedia Commons

4 LES DIFFICULTÉS DE L'ANONYMAT

Il existe de bonnes raisons pour promouvoir des systèmes qui reposent sur l'anonymat : protéger la vie privée, éviter que des données sensibles soient exploitées par des personnes malintentionnées.
Cela peut cependant engendrer des inconvénients.
Par exemple, permettre aux validateurs d'une cryptomonnaie de rester anonymes oblige à un système de rémunération délicat alors que le problème est simple quand les validateurs sont bien identifiés, et que personne ne peut se cacher sous plusieurs pseudonymes. Cet anonymat, s'il concerne aussi les utilisateurs (ceux qui souhaitent détenir des comptes), ouvre la porte à une multitude de trafics et d'escroqueries. Les plus graves sont les rançongiciels : le pirate installe un programme sur le réseau d'une entreprise, d'une administration ou d'un hôpital ; le programme chiffre les fichiers du système informatique et fait apparaît un message indiquant qu'il faut payer une rançon à un utilisateur anonyme d'un réseau de cryptomonnaie pour retrouver les données perdues.
La preuve de travail introduit d'autres escroqueries, dont le *cryptojacking*. Dans un système fonctionnant avec la preuve de travail, la quantité de calculs qu'on est capable de faire fixe combien on gagne. Le pirate informatique installe un programme sur des ordinateurs qui ne sont pas à lui et leur demande de faire ces calculs rémunérateurs. Des milliers d'ordinateurs ont ainsi été mis au service de pirates.
Cela conduit parfois à des dysfonctionnements graves des systèmes informatiques concernés et à des vols importants d'électricité.
La preuve d'enjeu n'ouvre pas la possibilité de ce type de vol lié à la preuve de travail.