dentelle possible. Ils finissent par concevoir des machines spécialisées pour faire efficacement les rubans demandés et réussissent à diminuer les coûts de fabrication. À la longue, certains d'entre eux disposent de multiples machines performantes et fabriquent des longueurs énormes de rubans pourtant destinés à être détruits. Ils deviennent ce que nous appellerons des « industriels des rubans ». Ils sont concurrents et les joueurs qui fabriquent les rubans à la main voient leur part de l'attribution diminuer de semaine en semaine et même devenir négligeable, car les industriels des rubans s'emparent de la presque totalité de S à chaque distribution.

Comparée à la preuve d'enjeu, la preuve de travail semble catastrophique

La concurrence entre les industriels des rubans engendre un problème de rentabilité. Un industriel ne gagne une somme G, lors de la distribution hebdomadaire de la somme S, que s'il dépense pour la fabrication des rubans une somme qui se rapproche de G. En effet, si la fabrication pour gagner G coûte sensiblement moins que G, des concurrents attirés par le bon rendement de ce type d'investissement développent leurs outils et entrent sur le marché, ce qui fait baisser le rendement. À la longue, le rendement de la fabrication des rubans diminue et par exemple conduit les industriels du ruban à dépenser 80% (peut-être plus) de la somme G qu'ils gagnent chaque semaine en coût de production des rubans. Globalement, à cause de la compétition, les industriels des rubans qui se sont presque emparés de la totalité de la somme S distribuée chaque semaine dépensent par exemple 80% de S chaque semaine pour produire les rubans qui leur rapportent donc collectivement 20% de S. Le rendement sous cette hypothèse est de 25% (20% comparé à 80%), ce qui est suffisant pour que l'activité se poursuive. L'équilibre évoluera peut-être et la concurrence suscitera des progrès dans la fabrication des rubans, mais le rendement des investissements des industriels des rubans sera toujours assez réduit, par exemple 25% ou moins si la concurrence devient plus féroce.

La situation est en réalité devenue absurde: au lieu de distribuer chaque semaine la somme S, si on prend en compte les dépenses pour produire les rubans, chaque semaine c'est seulement 20% de S qui est réellement distribuée par le mécène. Non seulement il y a concentration de la distribution sur les industriels du ruban, mais en plus 80% de la somme S ou plus est en quelque sorte utilisée en pure perte pour fabriquer des rubans aussitôt détruits.

Comparée à la méthode de l'enjeu, la méthode du travail semble catastrophique et le mécène qui donne la somme S chaque semaine ne sera certainement pas satisfait qu'on distribue S par la méthode du travail. Les deux méthodes évitent la tricherie des enveloppes multiples, aucune des deux méthodes n'est parfaite, mais la méthode de l'enjeu est clairement meilleure.

VARIANTE À ENJEU CONFISQUÉ

On peut aussi imaginer que les sommes s_i ne sont pas rendues, mais confisquées. Un problème assez délicat en résulte. Chacun essaiera d'engager le plus d'argent possible en mettant une somme s_i élevée dans son enveloppe. Mais si le total de l'argent engagé par les joueurs est supérieur à S, alors la somme redistribuée sera inférieure à ce que les joueurs auront engagé et sacrifié; puisque l'argent redistribué à chacun est proportionnel à son enjeu, chaque joueur sera perdant. Le jeu deviendrait un peu fou car chacun serait tenté d'engager le plus possible en espérant que les autres engagent le moins possible. Une sorte de piège serait tendu aux joueurs qui risqueraient tous de perdre de

3 LES ATTAQUES SYBIL

Lorsqu'un système de communication accepte l'anonymat des utilisateurs, cela engendre des difficultés imprévues. Cela est apparu en informatique à l'occasion de la mise au point des réseaux pair-à-pair, c'est-à-dire sans administrateur central. La possibilité pour une même personne d'utiliser plusieurs pseudonymes différents lui procure des avantages assimilables à une tricherie, comme dans le cas de la distribution par la méthode S/N quand un joueur envoie plusieurs enveloppes. Sur les réseaux sociaux ou les forums, c'est par exemple un moyen de faire croire que plusieurs personnes soutiennent une même idée alors qu'en réalité il n'y en a qu'une. Ce procédé est nommé « attaque Sybil ». Ce nom provient du titre du livre *Sybil*, publié en 1973 par Flora Schreiber, qui raconte la vie de Shirley Mason, une femme qui aurait été atteinte d'un trouble dissociatif de l'identité, c'est-à-dire de personnalités multiples. Le nom d'« attaque Sybil » fut introduit en informatique par John Douceur en 2002. Le risque d'attaques Sybil a contraint Satoshi Nakamoto à introduire les preuves de travail dans la cryptomonnaie Bitcoin, bien que la solution des preuves d'enjeu introduite quelques années plus tard soit maintenant reconnue comme bien meilleure, ce que le jeu du mécène rend évident.

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.