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.

rémunérés parce qu'ils le font fonctionner. Dans le cas du Bitcoin, 6,25 bitcoins sont créés toutes les dix minutes environ et attribués à l'un des validateurs du réseau, qui reçoit aussi des commissions provenant des utilisateurs du réseau.

Lorsque les validateurs sont anonymes, ce qui est le cas pour les cryptomonnaies mentionnées, le problème de l'attribution est alors exactement celui du «jeu du mécène et des enveloppes», car les validateurs peuvent apparaître sous plusieurs identités comme les joueurs qui envoient plusieurs enveloppes. En sécurité informatique, la tricherie consistant à apparaître sous plusieurs identités est nommée «une attaque Sybil» (*voir l'encadré 3*). Ces attaques ne sont possibles que sur les réseaux anonymes, et c'est bien parce que les cryptomonnaies mentionnées sont conçues avec des validateurs anonymes qu'il y a un problème. Si les validateurs étaient clairement identifiés, il serait possible de les rémunérer par la méthode S/N ou sa variante probabiliste. Pour les blockchains où les validateurs sont clairement identifiés, le problème de la distribution de l'incitation n'existe pas ou est très simple. Précisons que l'identification des validateurs n'oblige pas à l'identification des utilisateurs, qui peuvent rester anonymes même quand les validateurs sont connus.

Concevoir la méthode de rétribution des validateurs du réseau d'une cryptomonnaie dont les validateurs sont anonymes revient donc exactement à résoudre le «jeu du mécène et des enveloppes» décrit plus haut.

La méthode de l'enjeu a été proposée et elle est utilisée par de nombreux réseaux de cryptomonnaies avec des variations dans le détail. Elle prend le nom de «preuve d'enjeu» ou de «preuve de participation». La méthode du travail prend le nom de «preuve de travail». Les méthodes adoptées sont le plus souvent les versions probabilistes.

Le travail à faire dans le cas de la preuve de travail n'est pas, bien sûr, la fabrication de rubans en dentelle ensuite détruits. Le travail demandé est la réalisation de calculs dans le but de résoudre un problème numérique. Le problème à résoudre est conçu de façon qu'un validateur engageant une puissance de calcul c_i (à mettre en parallèle avec la capacité à fabriquer des rubans chaque semaine) gagnera avec une probabilité proportionnelle à c_i. Ces calculs ne servent à rien d'autre qu'à la distribution de l'incitation et donc dès qu'elle a eu lieu on ne garde rien des calculs qui sont parfaitement comparables aux rubans détruits.

Dans le cas de la méthode de la preuve d'enjeu, un validateur engage une somme en la mettant sous séquestre numériquement, ce que l'on sait faire sans avoir à lever l'anonymat, et il est rétribué avec une probabilité proportionnelle à cette somme mise sous séquestre, qui est l'équivalent de la somme s_i mise dans l'enveloppe envoyée à l'organisateur de la distribution.

L'évolution de ce que nous avons décrit pour «la méthode du travail» s'est produite pour les blockchains qui ont choisi la méthode de «la preuve de travail», ce qui est le cas du Bitcoin. Une industrie spécialisée dans ce calcul s'est progressivement mise en place, comparable à l'industrie des rubans de notre histoire. La compétition entre calculateurs est devenue de plus en plus forte et les moyens engagés pour mener les calculs de plus en plus importants.

SIX RÉACTEURS NUCLÉAIRES !

La logique économique incontournable, comme dans le cas des rubans, a conduit à l'utilisation de moyens industriels de calcul qui font qu'aujourd'hui l'électricité dépensée pour les calculs d'une cryptomonnaie comme le Bitcoin est équivalente à la production d'au moins six réacteurs nucléaires et sans doute trois fois plus. Une équipe de l'université de Cambridge a développé un outil de suivi en temps réel de cette consommation (*voir la bibliographie*). Cette dépense rogne les revenus des validateurs, comme le coût de fabrication des rubans diminue la somme S réellement distribuée par le mécène. Cette perte est absurde puisque la méthode de la «preuve d'enjeu» l'évite totalement (mais cette solution n'a été envisagée que plusieurs années après la création du Bitcoin). Il se trouve que le passage d'une méthode à l'autre n'est pas facile. Le Bitcoin ne l'envisage pas et restera économiquement inefficace et écologiquement scandaleux. Ethereum va passer de la preuve de travail à la preuve d'enjeu. Les cryptomonnaies récentes fonctionnent toutes selon la méthode de la preuve d'enjeu ou une variante.

De ces observations, retenons deux points principaux. La difficulté initiale provient de l'anonymat des validateurs. Si on y renonce, tout est assez simple. Les blockchains dites «privées» ou «de consortium» qui fonctionnent entre des utilisateurs en nombre limité et connus ne rencontrent de ce fait aucun problème de dépense électrique.

Même si on souhaite permettre aux validateurs d'une blockchain de cryptomonnaies de rester anonymes, les solutions de type «preuve d'enjeu» évitent aussi la dépense électrique et l'impact écologique de la «preuve de travail», qui apparaît comme une erreur initiale dans la conception du Bitcoin. Malgré l'admiration qu'on doit à Satoshi Nakamoto, l'inventeur de la première cryptomonnaie que fut le Bitcoin, sa «preuve de travail» est indubitablement une absurdité. Il est indispensable qu'elle soit abandonnée si on souhaite réellement que cette nouvelle sorte de monnaie se développe, permettant l'existence d'un argent liquide numérique anonyme respectueux de la vie privée de chacun. ■

BIBLIOGRAPHIE

J. P. Delahaye, **Au-delà du Bitcoin. Dans l'univers de la blockchain et des cryptomonnaies,** Dunod, août 2022.

J. P. Delahaye, **Les arguments en faveur de la preuve d'enjeu (POS) et contre la preuve de travail (POW),** Institut Rousseau, janvier 2022. bit.ly/PLS536_LC_Rousseau

Consommation électrique du réseau Bitcoin mis à jour en continu par l'université de Cambridge ccaf.io/cbeci/index

J. P. Delahaye, **Au-delà du Bitcoin,** *Pour la Science*, n° 499, mai 2019.

V. Faure-Muntian *et al.*, **Les enjeux technologiques des blockchains,** OPECST (Office parlementaire d'évaluation des choix scientifiques et technologiques), 2018. bit.ly/PLS536_LC_OPECST

J. P. Delahaye, **Consommation électrique des cryptomonnaies et des blockchains, document pour France-Stratégie dans le cadre de la réflexion « La consommation électrique des technologies disruptives »** bit.ly/PLS536_LC_FranceStrat