Comment être juste avec des anonymes ?

La mise au point de protocoles anonymes pour les blockchains suggère un intrigant problème de récréation mathématique

Jean-Paul Delahaye [1]

Un débat fait rage depuis une dizaine d'années concernant les méthodes de sécurisation des cryptomonnaies anonymes. Il concerne le Bitcoin et ses concurrents principaux Ethereum, Cardano, Solana et a pris une importance de plus en plus grande. De la conclusion qu'on tire de ce débat dépend sans doute l'avenir des cryptomonnaies et plus généralement des crypto-actifs dont l'impact écologique s'accroît gravement aujourd'hui.

Le problème posé peut s'expliquer en considérant un jeu assez simple qui dégage le problème de son contexte un peu confus. Ce jeu permet à chacun de comparer les deux solutions principales opposées et peut-être d'en imaginer de nouvelles. Voici ce « jeu du mécène et des enveloppes anonymes ».

Distribuer au mieux de l'argent

Imaginez qu'un riche mécène vous confie une certaine somme S, par exemple un million d'euros, en vous demandant de la distribuer. Vous êtes chargé d'organiser une sorte de jeu pour répartir le plus équitablement possible la somme S entre les gens qui acceptent de recevoir une part de cet argent. Vous leur demandez de manifester leur souhait en vous faisant parvenir dans un lieu fixé une enveloppe avec

1. Professeur émérite, université de Lille, campus Cité scientifique, CRIStAL UMR CNRS, 9189 Centre de recherche en informatique signal et automatique de Lille, bâtiment ESPRIT, 59655, Villeneuve d'Ascq Cedex France. E-mail : jean-paul.delahaye@univ-lille.fr.

DOI:10.48556/SIF.1024.19.121

une adresse dans laquelle vous mettrez ce que vous leur attribuez, avant de renvoyer l'enveloppe à l'adresse inscrite. Si vous collectez N enveloppes, la méthode qui vient immédiatement à l'esprit consiste à mettre $\frac{S}{N}$ euros dans chacune des enveloppes et à les renvoyer.

La « méthode S/N » n'est pas parfaite car les personnes ayant plusieurs maisons pourraient mettre plusieurs enveloppes à leur nom avec des adresses différentes ce qui vous empêcherait de savoir que l'argent ira à la même personne. Il y a pire, le mécène vous a demandé de concevoir une méthode qui n'oblige pas ceux qui veulent recevoir une part de S à délivrer leur adresse véritable. Vous acceptez donc que des joueurs se regroupent sur une même adresse et vous soumettent des enveloppes avec des adresses anonymes du type « Joueur 237, 11 rue Dupont à Paris ».

Vous comprenez bien que si vous utilisez la méthode S/N, chaque joueur va être tenté d'envoyer une multitude d'enveloppes dont les contenus lui seront destinés. Il utilisera plusieurs adresses, ou une seule adresse A en prenant le rôle du joueur 1, du joueur 2, etc. de l'adresse A. Si vous utilisez la méthode S/N, vous allez donc recevoir des milliers 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'approprieront 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 ?

Réfléchissez bien, ce n'est pas facile. Il n'existe aucune façon parfaite de résoudre le problème, mais il existe quand même plusieurs façons d'organiser la distribution rendant totalement inopérante la tricherie de l'envoi de plusieurs enveloppes et assurant une certaine équité entre les joueurs. Nous expliquerons plus loin que cette petite énigme mathématique est la transposition du problème du consensus dans les blockchains anonymes de cryptomonnaies.

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 s_i, vous laissez s_i dans l'enveloppe, vous y ajoutez $S \times \frac{s_i}{s_1+\ldots+s_n}$, puis vous renvoyez l'enveloppe.

Il est immédiat de vérifier que cela constitue bien une distribution totale de S. Ceux qui ont manifesté un soutient 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, par exemple, quelqu'un envoie 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 puisque l'organisateur pourrait garder l'argent.

Solutions 2. La méthode du travail

Une seconde idée réussit aussi à éviter les tricheurs qui envoient plusieurs enveloppes. L'organisateur de la distribution demande à chaque joueur de réaliser un ruban de dentelle brodée d'un type bien précisé. 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 cm de ruban, d'autres joueurs un 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. En clair, si l'enveloppe E_i contient un ruban de longueur L_i, après l'avoir vidée de son ruban, l'organisateur y placera la somme $S\frac{L_i}{L_1+\ldots+L_n}$ et la renverra. Comme précédemment, la méthode rend inopérante l'envoi de plusieurs enveloppes par un même joueur car, en envoyant deux enveloppes avec 10 cm de ruban, il gagnera autant qu'en envoyant une seule enveloppe avec 20 cm de ruban. Il y a un certain travail à faire pour réaliser le ruban en dentelle, c'est en quelque sorte une mesure de confiance que le joueur accorde à l'organisateur de la distribution et un engagement de sa part. C'est ce travail qui détermine son gain. 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 ».

On peut imaginer d'autres méthodes mais ce n'est pas facile et aucune n'est parfaite. Dans un premier temps, comparons la « méthode de l'enjeu » et la « méthode du travail ».

Comparaison

Posons-nous deux questions. Est-ce que les deux méthodes sont équivalentes l'une à l'autre, ou l'une est-elle meilleure que l'autre ? 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. C'est assez ennuyeux, mais la méthode du travail souffre du même inconvénient, car si vous être 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.

1. Le jeu du mécène et des enveloppes

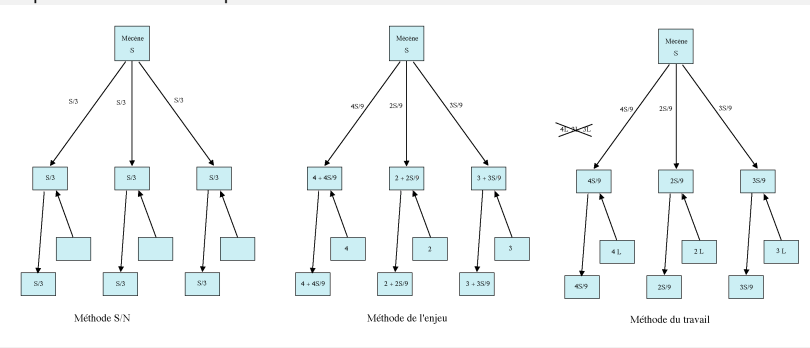
Un mécène veut distribuer une somme S le plus équitablement possible. Il reçoit des enveloppes, il veut répartir S dans les enveloppes.

— Méthode S/N : S'il reçoit N enveloppes, il dépose dans chacune S/N et les renvoie. Ceux qui ont envoyé plusieurs enveloppes sont favorisés.

— Méthode de l'enjeu : Il 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 à l'enjeu trouvée 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 trouvée dans l'enveloppe.

La question est de savoir qu'elle est la meilleure méthode ?



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 persuadé 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 quelque chose de 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 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 en compétition les uns avec les autres 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.

La concurrence entre les industriels des rubans engendre un problème de rentabilité. Un industriel ne peut gagner 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 qui règne entre eux, les industriels des rubans qui se sont 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, en fait, est 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 est en quelque sorte dépensée en pure perte pour fabriquer des rubans aussitôt détruits.

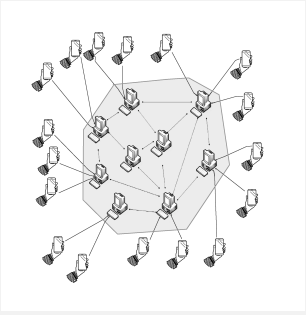
Comparé à la méthode de l'enjeu, la méthode du travail semble catastrophique et le mécène qui donne la somme S chaque semaine ne sera certainement pas satisfait qu'on distribue S par la méthode du travail. Les deux méthodes évitent la tricherie des enveloppes multiples, aucune des deux méthodes n'est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

Une variante

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 — donc en mettant une somme s_i la plus élevée possible dans son enveloppe.

2. Le fonctionnement des crypto anonymes

Une cryptomonnaie s'appuie sur un réseau de validateurs indépendants qui s'occupe 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 paye donc les validateurs. Ce paiement s'opère souvent en créant des 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. 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 $\frac{S}{N}$. 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 chose que la méthode S/N.



Au centre : le réseau des validateurs, à l'extérieur : les utilisateurs.

Une idée est souvent utilisée. Demander à chaque validateur V_i d'engager une somme s_i en la mettant 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 dont il décide de la puissance c_i. 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 on a découvert qu'elles produisent des effets économiques très différents.

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 ; ils seront donc globalement perdants, et puisque l'argent redistribué à chacun est proportionnel à son enjeu, chaque joueur sera individuellement 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 globalement risqueraient de perdre de 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 dans 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, ce qui n'est pas le but du mécène.

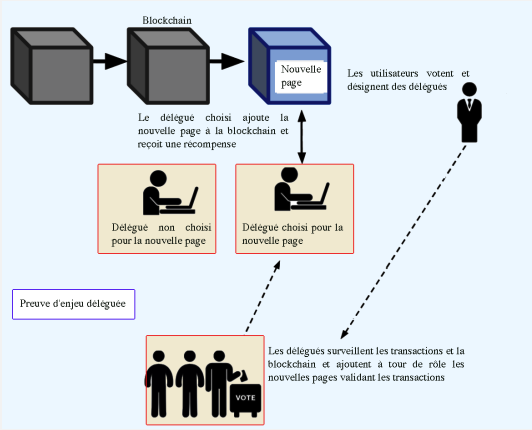
Rien ne semble sensiblement mieux que les deux premières méthodes décrites, mais si des lecteurs en imaginent d'autres plus satisfaisantes, ils doivent me le signaler.

Variantes probabilistes

La méthode de l'enjeu et la méthode du travail ont chacune une variante probabiliste essentiellement équivalente. Il faut les expliquer car elles vont nous approcher

3. Les variantes de la preuve d'enjeu

La preuve d'enjeu possède de nombreuses variantes dont en particulier la preuve d'enjeu par délégation dont le principe est le suivant. Les joueurs engagent de l'argent — comme dans la preuve d'enjeu — pour recevoir des parts de la somme S distribuée périodiquement. Cet argent misé leur donne le droit de participer à l'élection d'une série de délégués qui recevront l'argent distribué et qui dans un réseau de cryptomonnaies joueront le rôle de validateurs. Une redistribution de l'argent reçu par les délégués-validateurs permet à tous les joueurs de profiter de l'argent distribué. Un tel système est intéressant car il limite le nombre de validateurs ; ce qui permet au réseau de fonctionner plus rapidement, et il permet à ceux qui veulent profiter de l'argent distribué de ne pas à avoir à engager des moyens techniques nécessaires pour valider les transactions du réseau et le surveiller.



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 choisie 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 $\frac{1}{4}$ de S et l'enveloppe 2, reçoit $\frac{3}{4}$ 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 $\frac{1}{4}$ et de donner S à l'enveloppe 2 avec une probabilité de $\frac{3}{4}$. 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' sortent. La répétition de l'utilisation du tirage au sort produit à la longue une attribution de $\frac{1}{4}$ de l'argent distribué au premier joueur, et de $\frac{3}{4}$ 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.

Preuve d'enjeu et preuve de travail

Nous sommes maintenant arrivés exactement au problème qui se pose pour les blockchains anonymes de 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 fonctionne grâce à eux et que plus ils sont nombreux plus le réseau est décentralisé ; ce qui est souhaitable. La rémunération provient soit de nouvelles unités que le réseau crée, soit des commissions que les utilisateurs paient quand ils utilisent le réseau et qui naturellement doivent aller à ceux qui le font fonctionner. C'est la logique du modèle économique de tels réseaux décentralisés : certains payent pour l'utiliser, d'autres sont 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 se nomme une « attaque Sybil » (cf. encadré 4). 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 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 cryptomonnaies dont les validateurs sont anonymes revient donc exactement à résoudre le « problème 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 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 combinatoire. Le problème à résoudre est conçu de façon à ce 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.

4. 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, 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. On dénomme « attaque Sybil » ce procédé.

Le nom provient du titre du livre « Sybil » publié en 1973 par Flora Schreiber qui décrivait le cas d'une malade mentale appelée Sybil dans le livre mais dont la véritable identité est Shirley Mason. Elle était atteinte de trouble dissociatif de l'identité c'est-à-dire de personnalités multiples. Le nom d'attaque Sybil fut introduit en informatique par [9]. 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.

Shirley Mason.

Dans le cas de la méthode de la preuve d'enjeu, un validateur engage une somme en la mettant sous séquestre numériquement — ce qu'on sait faire sans avoir à lever l'anonymat — et il gagne avec une probabilité proportionnelle à cette somme 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 du calcul spécialisée 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. 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 de cinq centrales nucléaires au minimum, et sans doute trois fois plus. 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. 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.

Conclusion

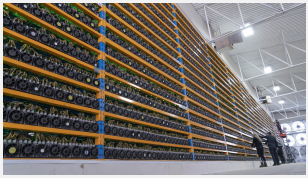
De ces questions concernant le fonctionnement des blockchains et des cryptomonnaies dont « le jeu du mécène et des enveloppes » permet la compréhension, il faut retenir deux points principaux :

— 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 l'invention de la première cryptomonnaie que fut le Bitcoin, sa « preuve de travail » est indubitablement une absurdité petit à petit abandonnée. C'est d'ailleurs indispensable 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.

5. Conséquences des choix faits

Permettre aux validateurs d'une cryptomonnaie de rester anonyme 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 apparaître un message indiquant qu'il faut payer une rançon en cryptomonnaie anonyme pour retrouver les données perdues.



Une usine de minage de la firme Bitfarms au Canada. On aperçoit au fond les ventilateurs de refroidissement qui évacue la chaleur produite par les milliers de machines participant au concours de calcul.

La preuve de travail introduit d'autres escroqueries encore, dont le *crypto-jacking*. Puisque dans un système fonctionnant avec la preuve de travail, c'est la quantité de calculs qu'on est capable de faire qui 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 important d'électricité. Il faut remarquer que la preuve d'enjeu n'ouvre pas la possibilité de ce type de vol lié uniquement à la preuve de travail.

Références

[1] Jean-Paul Delahaye. Se libérer du Bitcoin, Introduction aux blockchains et aux cryptomonnaies. Dunod, 2022.

[2] Université de Cambridge. *Bitcoin network power demand*, données mises à jour en continue sur la consommation électrique du réseau Bitcoin, `https://ccaf.io/cbeci` 2022.

[3] Manuel Valente. Qu'est-ce que le *Proof-of-Stake* (preuve d'enjeu) ? `https://www.coinhouse.com/fr/academie/blockchain/proof-of-stake/`. Coinhouse, 2022.

[4] Jean-Paul Delahaye. Au-delà du Bitcoin. Pour la science, n°499, 80-85, Mai, 2019.

[5] Valéria Faure-Muntian, Claude de Ganay, Ronan Le Gleut. Les enjeux technologiques des blockchains. OPECST (Office parlementaire d'évaluation des choix scientifiques et technologiques), `http://www.senat.fr/rap/r17-584/r17-5841.pdf`, 2018.

[6] Jean-Pierre Landau, Alban Genais. Les cryptomonnaies. Rapport au Ministre de l'économie et des finances, `https://www.mindfintech.fr/files/documents/Etudes/Landau_rapport_cryptomonnaies_2018.pdf`, 4 juillet 2018.

[7] Jean-Paul Delahaye. Consommation électrique des cryptomonnaies et des blockchains. Document pour France-Stratégie, « La consommation électrique des technologies disruptives », `http://cristal.univ-lille.fr/~jdelahay/temporaire/DelahayeFranceStrat4juin2018.pdf`, 4 juin 2018.

[8] Jean-Paul Delahaye. Les preuves de travail (Détails sur les concours de calculs utilisés par le Bitcoin). Pour la science, n°438, 80-85, avril 2014.

[9] John Douceur. The Sybil Attack. *International workshop on Peer-To-Peer Systems*, 2002.