ACADÉMIE DES TECHNOLOGIES
POUR UN PROGRÈS RAISONNÉ, CHOISI ET PARTAGÉ

# CRÉER DE LA CONFIANCE DANS UN ENVIRONNEMENT NUMÉRIQUE ANARCHIQUE AVEC LA BLOCKCHAIN : À QUEL COÛT ÉNERGÉTIQUE ?

Christian de Boissieu et Gérard Roucairol

Membres de l'Académie des technologies, pour les pôles Technologies, économies et sociétés et Numérique

Séance du 22 mars 2023

## Résumé

Une blockchain, concept initialement inventé dans le contexte des cryptomonnaies, ou monnaies virtuelles, peut être comparée à un grand livre dans lequel sont enregistrées toutes les transactions monétaires effectuées depuis sa création, et dont chaque utilisateur possède une copie. Son fonctionnement repose sur quatre grands ingrédients : cryptographie, réseau de communication pair-à-pair, algorithmique distribuée, mécanismes d'incitation économique.
Le système de blockchain offre la possibilité d'enregistrer de l'information de manière irréfutable et permanente, sans recourir à un tiers de confiance. Cette capacité est très utile dans bien d'autres domaines que le domaine bancaire : droit, commerce, industrie, etc. La blockchain apparaît ainsi comme un mécanisme générique facilitant l'organisation et la régulation fiable des communautés les plus diverses.
Toutefois, dans le contexte de systèmes distribués dont elle relève, de nombreux problèmes de maintien de cohérence et donc de confiance se posent. La validation des transactions constitue un enjeu clef et différentes méthodes existent pour cela. La validation par preuve de travail, méthode la plus connue et la plus sûre, présente l'inconvénient d'une consommation énergétique considérable. Sans assurer de manière formellement prouvée le même degré de confiance, d'autres méthodes de validation moins gourmandes en énergie existent, comme la preuve par enjeu. La question se pose désormais de savoir comment, à l'échelle mondiale, faire migrer les monnaies virtuelles vers des consommations énergétiques réduites.

## Intervenants

**Emmanuelle Anceaume**
Directrice de recherche au CNRS (UMR 6074/IRISA Rennes)

**Michel Laroche**
Membre de l'Académie des technologies

**Olivier Pironneau**
Membre de l'Académie des sciences

## Sommaire

## Introduction par Gérard Roucairol

Lors de la séance de janvier dernier, nous avons évoqué l'impact monétaire et économique des cryptomonnaies, en distinguant deux grands cas de figure. D'un côté, des systèmes de paiement centralisés, avec un seul livre de compte tenu par une banque, ce qui en assure, par principe, la cohérence. De l'autre, un modèle distribué dans lequel chaque utilisateur détient une copie du livre de compte et devient ainsi le contrôleur de tous les autres, ce qui pose la question de la cohérence entre les différentes copies. Nous allons, aujourd'hui, examiner de façon plus approfondie les aspects techniques des cryptomonnaies.

Les systèmes distribués relèvent d'une inspiration « anarchique » au sens où, conformément à la formule « *Ni Dieu, ni maître* », ils ne disposent pas d'arbitre ou de contrôleur suprême, ni de références communes ou d'informations partagées. Ainsi leurs utilisateurs sont considérés comme tous égaux a priori et, par ailleurs, ne sont pas dotés d'une horloge commune, ni d'une mémoire commune. La seule façon pour eux de partager des informations consiste à échanger des messages, avec pour corollaire que, lorsqu'un message part, on ne sait pas quand il arrivera, ni s'il est déjà arrivé, et que, lorsqu'un message arrive à destination, l'information qu'il contient est probablement déjà périmée. À cette difficulté s'ajoute le fait que les serveurs et réseaux des systèmes distribués peuvent à tout moment tomber en panne ou subir des actes malveillants ou des tentatives de fraude.

Compte tenu de ces particularités, trois questions se posent : quelle algorithmique peut-on mettre en œuvre dans un système distribué afin de créer la confiance pour les applications qui le nécessitent, notamment en matière bancaire, commerciale, de traçabilité ou encore de certification par des actes notariés ? Comment la blockchain répond-elle à ces besoins ? Quel est le coût énergétique de ces applications ?

# Le fonctionnement des blockchains

Emmanuelle Anceaume

*Emmanuelle Anceaume est directrice de recherche au CNRS (UMR 6074/IRISA Rennes).*

La notion de blockchain est apparue pour la première fois en 2008 dans un article d'une dizaine de pages signé Satoshi Nakamoto, un pseudonyme. Cet article décrit les principes de fonctionnement d'une cryptomonnaie destinée à permettre à tout un chacun d'effectuer des transactions monétaires sans passer par une banque, grâce à la technologie de la blockchain.

Une blockchain peut être comparée à un grand livre dans lequel sont enregistrées toutes les transactions monétaires effectuées depuis sa création, et dont chaque utilisateur possède une copie. Le contenu de ce grand livre est accessible à tous à la fois en lecture et en écriture. Chaque écriture est le fruit d'un consensus et il est impossible de modifier ou effacer l'une des écritures. Enfin, aucun tiers de confiance (banque, entreprise, institution, État…) n'a de contrôle sur ce livre. Une combinaison à la fois simple et prodigieusement astucieuse entre quatre ingrédients (cryptographie, réseau de communication, algorithmique distribuée, mécanismes d'incitation économique) permet de construire de la confiance dans une infrastructure où personne ne fait a priori confiance aux autres.

### *La création des comptes monétaires*

La cryptographie permet à chaque utilisateur de se doter d'un compte monétaire, d'obtenir des résumés vérifiables et non modifiables d'une grande quantité de données, et de relier de façon non falsifiable des informations entre elles. La création du compte monétaire ne prend que quelques secondes. Elle passe par la définition d'une clé privée destinée à la signature et d'une clé publique permettant la vérification de l'authenticité. Un algorithme permet de lier intimement les deux, sans pour autant que la clé privée (que l'on

conserve chez soi) puisse être déduite de la clé publique, qui est diffusée sur le réseau.

Concrètement, si je souhaite acheter le vélo de mon voisin, je lui demande de me communiquer la clé publique d'un de ses comptes monétaires (chacun peut en créer des milliers), à l'aide de laquelle je vais créer une transaction monétaire entre son compte et le mien, accompagnée d'un défi que seul le propriétaire du vélo pourra résoudre et qui lui permettra de toucher effectivement les bitcoins que je vais lui verser. S'il veut utiliser l'argent correspondant pour acheter un nouvel objet, il créera une nouvelle transaction dans laquelle, en entrée, il mettra la référence du compte que j'ai crédité et la preuve qu'il possède ce compte, et en sortie, il indiquera le compte sur lequel il veut verser l'argent pour acheter l'objet, avec un défi que seul le possesseur de ce compte pourra résoudre.

## *Un réseau pair-à-pair*

Ces différentes transactions doivent être communiquées à la communauté entière, c'est-à-dire, potentiellement, à des milliers d'utilisateurs, via un réseau pair-à-pair, dont la topologie est fortement dynamique, dans la mesure où les utilisateurs se connectent de façon intermittente. Lorsqu'une personne se connecte, son compte cherche une vingtaine de « voisins » à qui envoyer la transaction, lesquels l'envoient à leur tour à une vingtaine de voisins. Une vingtaine d'itérations environ suffit à ce qu'un million de personnes reçoivent la transaction.

## *La compétition pour la création des blocs*

Toutes les dix minutes environ, ces transactions sont organisées en blocs protégés par des outils cryptographiques. En principe, tous les utilisateurs ont le droit de créer des blocs mais, sachant que tous ne reçoivent pas les différentes transactions en même temps, il est nécessaire de réserver cette tâche à certains d'entre eux, afin que tous disposent du même historique des transactions. Le mécanisme d'attribution de cette mission doit être vérifiable, non prédictible (pour éviter les attaques) et non monopolisable (ce qui engendrerait un risque trop grand dans le cas où l'entité chargée de créer les blocs serait malveillante).

La solution proposée par Satoshi Nakamoto pour le bitcoin est une compétition probabiliste parmi tous les volontaires (appelés *mineurs*) pour créer le prochain bloc de transactions. Le gagnant (l'idéal est qu'il n'y en ait qu'un) est le premier qui réussira à résoudre un problème informatique requérant une énorme puissance de calcul. La compétition doit être suffisamment difficile pour qu'un bloc soit créé toutes les dix minutes en moyenne, délai permettant à la fois de vérifier le bloc précédent et de limiter le nombre de blocs concurrents (appelés *forks*). Le gagnant reçoit une récompense monétaire de 6,25 bitcoins, soit environ 120 000 euros, mais seulement une fois que son bloc a été suivi de 100 autres blocs, ce qui signifie qu'au moins 100 autres mineurs lui font confiance, ce qui constitue, pour lui, une forte incitation à bien se comporter. Dans le cas où deux mineurs auraient créé deux blocs en même temps, la règle est de sélectionner la chaîne qui aura demandé le plus de puissance de calcul, c'est-à-dire, en pratique, la chaîne la plus longue.

Lorsqu'un individu malveillant cherche à modifier l'histoire des transactions, c'est-à-dire à remplacer un bloc contenant une transaction qu'il veut effacer (pour pouvoir utiliser à nouveau l'argent qu'il a déjà dépensé, par exemple), il doit, pour cela, être capable de générer la chaîne la plus longue. Ceci demande une énorme quantité d'énergie et devient pratiquement impossible après l'arrivée du 6$^{ème}$ bloc : la probabilité de réussir tombe alors à 6 chances sur 10 000, et décroît encore avec l'arrivée des blocs suivants. En d'autres termes, la confiance dans la blockchain augmente de façon exponentielle au fil du temps.

## *Une piste pour limiter la consommation d'énergie ?*

L'inconvénient de ce dispositif est qu'il mobilise énormément d'énergie, ce qui est inacceptable dans le contexte actuel de réchauffement climatique et de nécessité de réduire les émissions de GES.

Une solution alternative consisterait à se fonder sur une « preuve d'enjeu », c'est-à-dire à choisir le mineur possédant la plus grande quantité de cryptomonnaie. Selon les types de cryptomonnaie qui ont retenu cette option, cette somme doit, au préalable, être placée sous séquestre, ou non. La preuve d'enjeu respecte les trois critères déjà cités pour les mécanismes d'attribution : ils doivent être à la fois vérifiables, non prédictibles et non monopolisables. Elle présente cependant un inconvénient, le fait que le processus a un coût nul pour le mineur (contrairement à la résolution d'un problème informatique, qui demande d'investir dans de la puissance de calcul), ce qui peut entraîner la multiplication des créateurs de blocs. Une solution consiste à constituer un comité de validateurs des blocs, dont les membres sont sélectionnés de façon vérifiable et randomisée, et fréquemment remplacés.

# La blockchain, au-delà du bitcoin

Michel Laroche

*Michel Laroche est membre de l'Académie des technologies.*

J'ai découvert la technologie de la blockchain il y a quelques mois seulement, lorsque j'ai accepté de relire un article publié dans le cadre de la Fondation de l'Académie. C'est un univers passionnant, stupéfiant de créativité.

J'en profite pour apporter une précision par rapport à ce qui vient d'être dit, concernant un point que je n'avais pas bien compris au départ : lorsqu'on parle de vérification des blocks, celle-ci n'est pas effectuée par des personnes, mais seulement par des ordinateurs qui dialoguent entre eux.

## *Un objectif ambitieux*

La création du bitcoin date d'une quinzaine d'années, mais c'est seulement en 2019 que France Stratégie a commencé à s'y intéresser. Faisant montre d'un grand enthousiasme, elle a défini pour notre pays un objectif ambitieux, celui de devenir une « *nation de la blockchain* ». Un groupe de travail comprenant des membres du CEA (Commissariat à l'énergie atomique et aux énergies alternatives), de l'IMT (Institut Mines-Télécom) et de l'INRIA (Institut national de recherche en sciences et technologies du numérique) a été chargé d'identifier l'ensemble des verrous technologiques des nouvelles « *technologies de registres distribués* », plus particulièrement celle du type blockchain, d'analyser les enjeux et les potentiels de ces technologies, notamment en matière de souveraineté, de sécurité, d'interopérabilité et d'évolutivité, d'énergie et de modèles économiques, et de définir le programme de recherche nécessaire pour atteindre l'objectif visé.

## *Des applications diversifiées*

À partir des deux grands atouts de la blockchain, à savoir l'autoprotection contre la falsification des données enregistrées et l'accessibilité de l'information stockée, ce groupe de travail a identifié quatre grands domaines d'applications : l'enregistrement des données (notamment notariales), l'activité bancaire, le commerce, et enfin diverses autres activités.

Le domaine qui, de très loin, connaît le plus grand succès, est l'activité bancaire, avec pas moins de 10 000 cryptomonnaies recensées à l'heure actuelle. Cette réussite s'explique probablement par la possibilité offerte aux mineurs de gagner de l'argent et par toutes les formes de spéculation qui en découlent.

L'activité de stockage des données n'a guère prospéré, sans doute parce qu'elle est difficile à monétiser, or il est nécessaire de rémunérer les personnes qui se chargent de l'entretien de la blockchain. C'est dommage, car on pourrait imaginer des applications dans de nombreux domaines, comme celui de la santé.

Parmi les activités diverses, on peut citer les *smart contracts*, ou contrats intelligents, proposés notamment sur le réseau Ethereum. Dans la vie courante, de nombreuses situations impliquent des échanges entre plusieurs individus ou entités. Le principe des contrats intelligents consiste à formaliser les termes de ces échanges à travers des programmes mathématiques. Un exemple un peu simpliste de contrat intelligent est l'ordre de vente ou d'achat conditionné à la cote d'une action que vous pouvez donner à votre banquier. Ils peuvent, de surcroît, être abrités dans une blockchain afin de profiter de son infalsificabilité.

Le contrat intelligent se caractérise par trois propriétés fondamentales : l'autonomie (une fois validé et publié, il se suffit à lui-même et plus personne ne peut en modifier les termes), l'autosuffisance (pour son bon fonctionnement, le contrat intelligent doit s'appuyer uniquement sur des données stockées en blockchain), la décentralisation (les contrats intelligents sont distribués et autoexécutés à travers les nœuds du réseau de la blockchain). Ethereum propose désormais des contrats intelligents permettant d'effectuer des calculs, de stocker des données, de générer des NFT, d'envoyer des messages ou encore de produire des visuels.

Une quatrième application est le suivi des chaînes d'approvisionnement. La blockchain permet de stocker des informations de traçabilité afin que l'intégrateur final puisse s'assurer qu'il a bien reçu le produit promis par le fournisseur et que celui-ci respecte le niveau de qualité attendu. La blockchain permet également de garder trace de tous les échanges de documents, contrats et certificats entre les différents acteurs, et de recueillir des informations aussi bien sur les flux physiques que sur les transactions financières. Ethereum

propose également ce type d'application, moyennant l'obligation de réaliser tous les échanges financiers en recourant à sa cryptomonnaie.

Une autre application concerne deux outils dans lesquels l'informatique joue un rôle fondamental, les réseaux de télécom 5G, qui sont purement informatiques et devront être protégés, ce qui pourrait se faire à travers la blockchain, et les *smart grids*, qui impliquent des échanges de matières et d'énergie ainsi que des flux financiers entre plusieurs producteurs et consommateurs.

### *Comment conjuguer efficacité et sobriété ?*

La protection apportée par une base de données de type blockchain repose sur un triptyque, les contraintes imposées à la création des blocs, le nombre de copies actives, la fréquence de comparaison entre ces copies. Ce triptyque doit être respecté en permanence, même en l'absence d'ajout de blocs. On peut y ajouter deux facteurs favorables supplémentaires, la fréquence des ajouts de nouveaux blocs et l'incitation financière à la fiabilité des blocs.

Ceci soulève la question de savoir comment conjuguer efficacité et sobriété. Quelles sont les valeurs minimales des différents paramètres (nombre de nœuds, contraintes sur les empreintes, fréquence de comparaison…) permettant d'assurer un niveau de protection suffisant ?

À mon sens, pour réduire la consommation d'énergie, il faut sans doute limiter le nombre de nœuds miniers, accepter le risque de perdre certaines applications ou données, et recourir à des solutions moins lourdes qu'actuellement pour reconstituer les données après une attaque. On pourrait aussi créer de grosses blockchains fourre-tout qui accueilleraient des informations diversifiées, plutôt que de multiplier les petits dispositifs dédiés. Enfin, peut-être serait-il possible de raccourcir les chaînes ? Supprimer les blocs initiaux ne changerait rien à la validité de la chaîne aval, à condition, bien sûr, de s'assurer que ceux-ci ne comprennent plus d'informations utiles.

## La consommation énergétique des cryptomonnaies

Olivier Pironneau

*Olivier Pironneau est membre de l'Académie des sciences.*

Je suis algorithmicien et, bien que non spécialiste des blockchains, j'ai été amené à m'intéresser à cette technologie dans le cadre des travaux de l'Académie des sciences, dont je suis membre. Nous avons, en effet, créé un groupe de travail sur les dépenses énergétiques liées aux différentes activités informatiques, et j'ai été chargé de la partie concernant les cryptomonnaies et autres blockchains.

L'essentiel des informations que je vais vous présenter vient de l'ouvrage *Au-delà du Bitcoin* de Jean-Paul Delahaye, directeur scientifique de la revue *Sciences et Avenir*.

C'est en 2008 que Satoshi Nakamoto a inventé la première monnaie digitale réellement utilisable, le bitcoin. On ne sait qui se cache derrière ce pseudonyme : un banquier, un informaticien, une personne seule, un groupe de travail ?

Cette monnaie n'existe que par une liste de transactions, organisée en chaîne de blocs cryptés et partagés en pair-à-pair sur Internet. Le propriétaire de bitcoins n'est identifié que par son mot de passe, en sorte qu'il suffit de se rendre chez lui avec une arme et d'exiger son mot de passe pour s'approprier ses bitcoins. Le système n'est donc que partiellement sûr.

### *Un gaspillage d'énergie*

Les transactions sont validées par une « preuve de travail » reposant sur le *hachage*, une technique proposée par Moni Naor & Cynthia Dwor pour éviter les dénis de service et les spams. Par exemple, vous pouvez convenir avec vos correspondants que vous ne recevrez que les mèls de ceux qui, connaissant $n$ et $e$ premier,

auront trouvé $p$, $q$ premier et $d$ tel que $n = p \times q$ et $e \times d + m \times (p - 1)(q - 1) = 1$, calcul qui leur prendra environ une demi-heure. Bitcoin utilise le même type de « pénalisation informatique » afin de sélectionner les utilisateurs sérieux, ce qui a l'inconvénient de se traduire par une importante consommation d'énergie.

À lui seul, le bitcoin a nécessité 110 TWh pour son fonctionnement en 2022, soit davantage que la Belgique (82 TWh) et près du double de la consommation suisse (58 TWh), ou encore la moitié de la consommation de tous les *data centers* du monde. Compte tenu de la popularité du bitcoin, cette dépense d'énergie risque d'être multipliée par dix d'ici vingt ans. À ceci s'ajoute le gaspillage de terres rares pour la fabrication des serveurs et l'utilisation de circuits dédiés reposant sur la technologie ASIC, non recyclables.

### *Les arguments des défenseurs du bitcoin*

Les défenseurs du bitcoin invoquent le caractère démocratique et anonyme des cryptomonnaies qui, selon eux, permettent de se libérer de toute emprise étatique et bancaire – faisant fi de tout le versant sombre des transactions illégales que facilitent ces outils.

Ils estiment que la dépense d'énergie liée à cette monnaie digitale n'est pas supérieure à celle nécessaire pour produire de l'or dans le système bancaire classique. Prédisant que le prix croissant de l'énergie et les lois du marché vont aboutir à une concentration des acteurs, ils préconisent la migration des *data centers* dans des zones où l'énergie est abondante et fatale, comme l'Islande, dont toute l'électricité vient de la géothermie.

Concernant les failles du système, ils considèrent que celles-ci ne viennent pas des blockchains elles-mêmes, mais des plateformes de trading comme FTX. Enfin, sachant que le bitcoin alimente actuellement 300 millions de comptes pour un montant total de mille milliards de dollars, ils estiment qu'une éventuelle faillite du bitcoin ne serait pas capable d'entraîner une crise financière générale.

### *Vers la preuve d'enjeu ?*

La solution pour réduire la consommation d'énergie consisterait à passer de la preuve de travail à la preuve d'enjeu. Dans ce modèle, un comité des plus gros mineurs assigne aléatoirement une transaction à celui qui place sous séquestre le plus grand montant de cryptomonnaie. Ethereum a partiellement basculé vers ce dispositif depuis septembre 2022 et a réduit sa consommation par mille, sans que cela provoque un effondrement de son cours.

Dans la mesure où le bitcoin représente, à lui seul, 90 % de l'usage des cryptomonnaies, le problème de la consommation énergétique de la blockchain ne sera pas résolu tant que le bitcoin n'aura pas également basculé vers la preuve d'enjeu, à moins que, entre-temps, cette cryptomonnaie soit abandonnée au profit d'ethereum. La difficulté vient du fait que personne n'a le contrôle complet du bitcoin et que la seule solution consisterait à créer un « nouveau bitcoin » concurrent, hypothèse peu crédible.

Si les États prenaient l'initiative d'interdire le recours à la preuve de travail, on peut craindre que quelques pays moins intransigeants servent de refuge aux cryptomonnaies utilisant cette technologie. Peut-être la concurrence des banques, qui préparent actuellement leurs propres cryptomonnaies, pourrait-elle contribuer au basculement vers la preuve d'enjeu. De même, si les cryptomonnaies prenaient davantage d'ampleur et provoquaient une crise financière semblable à celle des *subprimes*, sans doute assisterait-on à une concentration des acteurs qui faciliterait le passage à la preuve d'enjeu. Enfin, peut-être est-ce tout simplement l'augmentation massive du prix de l'énergie qui rendra le système non viable.

## Débats

### *Le poids des cryptomonnaies dans la finance mondiale*

**Christian de Boissieu :** La part de marché du bitcoin est de 40 % et non de 90 %. Celle de l'ethereum est de 20 %. Ces deux monnaies représentent ainsi 60 % des 1 000 milliards de dollars que représente le marché des bitcoins. À l'époque où le bitcoin valait 65 000 dollars, celui-ci approchait des 3 000 milliards de dollars, mais ces montants sont très éloignés de la valeur des contrats sur instruments dérivés, estimée à 700 000 milliards de dollars, dont 90 % s'effectuent sur les marchés OTC, c'est-à-dire de gré à gré et non régulés, malgré l'expérience de la crise de 2008. Il est donc peu probable que ce soient les cryptomonnaies, au stade actuel, qui provoquent une crise systémique.

## *Interdire ou convaincre ?*

**Emmanuelle Anceaume :** J'approuve l'idée qu'interdire la preuve de travail n'est pas la solution. Il vaudrait mieux convaincre les utilisateurs qu'il existe une alternative aussi sûre que la preuve de travail. Cela peut être la preuve d'enjeu ou toute autre preuve, à inventer. À nous, chercheurs, de montrer que l'on peut imaginer une meilleure solution qui coûtera moins d'énergie.

**Olivier Pironneau :** La démonstration de l'efficacité de la preuve d'enjeu semble déjà acquise par l'expérience d'Ethereum.

**Christian de Boissieu :** Interdire les cryptomonnaies n'a aucun sens dans le monde numérique d'aujourd'hui. L'Algérie, la Chine et la Corée du sud l'ont fait, et leurs interdictions sont contournées.
À mon sens, la principale parade est la création de monnaies digitales publiques, car la volatilité des cryptomonnaies privées (y compris celles présentées comme stables), la faillite de FTX et les problèmes de liquidité rencontrés par certaines plateformes sont de nature à orienter les investisseurs vers des monnaies plus fiables.
En parallèle, le règlement européen MiCA *(Markets in Crypto-Assets)* va introduire un peu de régulation dans les cryptomonnaies privées en les obligeant non seulement à se faire enregistrer mais à obtenir un agrément, ce qui les contraindra à apporter un certain nombre de garanties en matière de modèle d'affaire, d'honorabilité des dirigeants, de respects des règles sur les fonds propres, etc.

## *Le bitcoin pour les nuls*

**Étant béotien en matière de cryptomonnaies, j'aimerais savoir comment l'on procède concrètement pour acheter ou vendre des bitcoins. À quel site faut-il se connecter ?**

**Emmanuelle Anceaume :** Pour récupérer des bitcoins, vous pouvez soit vendre des objets qui vous seront payés dans cette monnaie, soit en acheter sur des places de marché.

**Comment faire pour que le petit épargnant bénéficie, lui aussi, des cryptomonnaies ?**

**Olivier Pironneau :** La question préalable est de savoir si les cryptomonnaies représentent, ou non, un moyen de passer à travers les crises financières.

**Christian de Boissieu :** Elles constituent en elles-mêmes un facteur d'instabilité plutôt que de stabilité.

## *En cas de panne géante*

**Dans la mesure où la blockchain est un système dynamique qui doit fonctionner en permanence, que se passerait-il en cas de panne de courant géante, par exemple à l'échelle de l'Europe de l'ouest ?**

**Emmanuelle Anceaume :** Le niveau de difficulté de la preuve de travail est réévalué tous les 2 016 blocs, soit environ tous les quinze jours, en tenant compte de la puissance de calcul mondiale. En cas de panne géante dans toute l'Europe de l'ouest, et donc de chute importante de la puissance de calcul, ce niveau serait réévalué à la baisse, mais le processus de création de blocs toutes les dix minutes se poursuivrait.

## *Les blockchains consortiums*

**Toutes les applications de la blockchain, par exemple les applications de logistique, ne requièrent probablement pas le même niveau d'exigence que les cryptomonnaies. Ne faudrait-il pas clarifier les besoins de sécurité correspondant aux différents usages ?**

**Emmanuelle Anceaume :** Dans mon exposé, j'ai évoqué essentiellement les blockchains reposant sur la coopération entre personnes qui ne se connaissent pas et ne se font pas confiance. Il existe d'autres dispositifs également appelés blockchains, à tort d'après moi, réunissant des personnes qui se connaissent, même si elles ne se font pas nécessairement confiance. On parle alors de *blockchains consortiums*.
Enfin, on qualifie également de blockchains des systèmes dans lesquels une entité centrale se charge d'écrire et de lire le contenu des blocs, ce qui, à mon sens, n'a plus rien à voir avec le principe d'une blockchain, et ne nécessite même pas le recours à cette technologie : un bon serveur ferait parfaitement l'affaire, puisque l'on n'a pas à gérer le problème de l'absence de confiance.

**Michel Laroche :** Un serveur ne garantirait pas la validité de l'information au même degré qu'un block qui ne pourra jamais être modifié. C'est ce qui fait tout l'intérêt de cette technologie.

## *Un avis commun avec l'Académie des sciences ?*

**Notre Académie pourrait-elle formuler un avis sur les cryptomonnaies et la blockchain ?**

**Gérard Roucairol :** Nous allons commencer par publier les comptes rendus de ces deux séances, puis nous réfléchirons à l'opportunité d'émettre un avis,

éventuellement en commun avec l'Académie des sciences.

**Christian de Boissieu :** Si nous prenons en compte exclusivement l'aspect énergétique, nous serons amenés à condamner ces technologies mais, pour être crédibles, nous devrions mener une vraie analyse coûts/avantages, le coût énergétique ne représentant qu'un aspect du bilan.

*Échanges entre participants :*

Le chiffre de 110 TWh évoqué pour la consommation énergétique du bitcoin paraît colossal, mais il faudrait comparer le coût énergétique de deux unités de transaction comparables, l'une effectuée via la blockchain et l'autre via le système bancaire classique et tout ce qu'il implique (des serveurs informatiques mais aussi la construction de bâtiments ou encore la rémunération du personnel). Peut-être l'Académie pourrait-elle se lancer dans ce type de calcul ?

La technologie des blockchains paraît incroyablement astucieuse mais, sur le fond, je ne vois pas quel avantage présentent les cryptomonnaies, sauf pour les heureux initiés qui se sont lancés au bon moment. Qu'apportent-elles de positif vis-à-vis des enjeux auxquels nous faisons face ? Si nous publions un avis, nous devrons adopter une posture critique y compris sur les avantages de cette technologie.

## Conclusion par Gérard Roucairol

Le format de travail conjoint entre deux pôles que nous avons adopté pour préparer cette séance paraît très intéressant et c'est sans doute l'une des plus-values que pourra apporter l'Académie si elle décide de publier un avis.

Sur le fond, je suis frappé par le phénomène du *Winner-Takes-All* qu'illustrent à la fois le bitcoin et ChatGPT, sur lequel nous venons de préparer un avis. Plus la blockchain est massive, plus elle inspire confiance. Il en va de même de l'intelligence artificielle, dont la crédibilité repose sur le volume des archives mobilisées, puis sur son utilisation en ligne, grâce à laquelle le système ne cesse de s'autorenforcer. La règle selon laquelle la confiance naît de la massification semble difficile à contredire, or elle se traduit par des consommations d'énergie effarantes. Se pose aussi le problème de la recherche en intelligence artificielle : peut-elle être menée utilement par des acteurs publics qui n'ont pas les moyens d'investir autant que Microsoft dans ce domaine ?

Dans le cas du bitcoin, on peut observer, de surcroît, que ce sont les mineurs disposant des plus grosses ressources financières qui contrôlent tout le système, ce qui remet quelque peu en cause l'idéal démocratique mis en exergue à l'origine.

Les moyens dont les régulateurs disposent pour intervenir sur ce type d'initiative évoluent malheureusement souvent plus lentement que les technologies visées. Ils doivent cependant agir, car l'on ne peut pas laisser l'argent mondial ni la connaissance mondiale aux mains de groupes privés, sans exercer aucun contrôle.

Le rôle de nos académies est, dans un premier temps, de mettre en évidence ces enjeux en abordant à la fois leurs aspects technologiques et économiques, et en faisant preuve de la plus grande objectivité possible. Nous contribuerons ainsi, conformément à notre vocation, à un progrès raisonné, choisi et partagé.

**Mots clés :** algorithmique distribuée, bitcoin, blockchain, cryptographie, cryptomonnaies, ethereum, preuve d'enjeu, preuve de travail, réseau de communication pair-à-pair

**Citation :** Christian de Boissieu, Gérard Roucairol, Emmanuelle Anceaume, Michel Laroche & Olivier Pironneau. (2023). *Créer de la confiance dans un environnement numérique anarchique avec la blockchain : à quel coût énergétique ?* Les séances thématiques de l'Académie des technologies. @

**Retrouvez les autres parutions des séances thématiques de l'Académie des technologies sur notre site**

**Académie des technologies. Le Ponant, 19 rue Leblanc, 75015 Paris. 01 53 85 44 44. academie-technologies.fr**

**Production du comité des travaux. Directeur de la publication : Denis Ranque. Rédacteur en chef de la série : Hélène Louvel. Auteur : Élisabeth Bourguinat. N°ISSN : 2826-6196.**