Nicolas Houy

Bitcoin et Economie

Chargé de recherche au CNRS, Nicolas Houy est membre de l'axe Théorie des jeux, choix collectifs et marchés du GATE..

Parce qu'il permet de faire ou de faciliter des échanges de biens ou de services, parce que le grand public le définit souvent comme une monnaie, toujours «électronique» ou «virtuelle», parce qu'il a un cours fixé sur des marchés libres où se rencontrent utilisateurs et spéculateurs, parce que les parlementaires français se posent la question de sa définition fiscale, Bitcoin est ou devrait être un phénomène d'intérêt pour les économistes. Les principes qui régissent Bitcoin ont été décrits dans un court article publié en 2008 par une (ou des) personne(s) sous le pseudonyme de Satoshi Nakamoto. La source du logiciel qui met en application ces principes a commencé à être distribuée et executée en janvier 2009. Depuis, le nombre d'utilisateurs n'a cessé d'augmenter de manière exponentielle. Aujourd'hui, chaque jour, l'équivalent d'environ une centaine de millions de dollars sont échangés en bitcoins.

Bitcoin, qu'est-ce que c'est?

Si Bitcoin est un objet économique, il a très certainement été imaginé par un (ou des) informaticien(s). Strictement, il s'agit d'un protocole, c'est-à-dire d'un ensemble de règles et de formats qui forment un langage et permettent à des ordinateurs et à ceux qui les contrôlent de communiquer entre eux de manière harmonieuse. Les protocoles HTTP - pour consulter des pages du web - ou SMTP - pour envoyer des emails - sont deux autres exemples de protocoles utilisés quotidiennement par des milliards d'individus. Dans le cas de Bitcoin, il s'agit d'un protocole qui permet de garantir des droits de propriété sur des unités de compte, les bitcoins, produits en quantité limitée dans un réseau d'ordinateurs totalement décentralisé. On distingue donc Bitcoin avec un «B» majuscule, le protocole, et les bitcoins, avec un «b» minuscule, qui sont les unités de compte qui circule sur le réseau des utilisateurs du protocole. Bien sûr, l'analogie avec la monnaie, voire l'argent en espèce est immédiate. C'est tellement vrai que l'article fondateur a pour titre «Bitcoin: a peer-to-peer electronic cash system». Le véritable tour de force de Bitcoin est que ce cash électronique est produit en quantité limitée, sans qu'aucune autorité centrale ne garde trace de toutes les transactions comme le ferait un réseau de banques ou une chambre de compensation. Et c'est une prouesse technique: si les données informatiques sont des suites de bits (quantité minimale d'information sur un ordinateur, un bit vaut 0 ou 1), tout peut être copié à l'infini et le cash électronique devrait pouvoir être imprimé hors de tout contrôle. Grâce à un mécanisme complexe intégrant des aspects de cryptographie, de réseaux, et de théorie des jeux, Bitcoin assure que le nombre de bitcoins en circulation ne dépassera jamais 21 millions d'unités et que personne ne peut «imprimer» des bitcoins et les introduire dans le système.

La science économique au service de Bitcoin

Les économistes ont beaucoup à apporter à Bitcoin. D'une part, pour que Bitcoin ait une existence viable à long terme, d'autre part pour que son utilisation soit aussi profitable que possible à ses utilisateurs. Et les travaux étudiant Bitcoin peuvent avoir un impact important et même vital pour le futur du protocole. En effet, Bitcoin est encore dans une phase de développement très active et ses spécifications évoluent régulièrement. On parle encore dans la communauté des utilisateurs avertis d'une phase expérimentale en parlant de la période actuelle. Etudier Bitcoin et proposer de l'améliorer, c'est aider à son développement dans le cadre d'un processus de création collectif et dynamique. Prenons quelques exemples sans entrer dans les détails techniques du protocole.

La question au centre des reflexions actuelles dans la communauté interdisciplinaire des personnes intéressées à développer Bitcoin est celle des coûts de transactions. D'un coté, les transactions (et donc ceux qui en sont à l'initiative) sont en concurrence entre elles pour être validées par un groupe un peu particulier d'utilisateurs, appelés les mineurs. Les mineurs, eux aussi sont en concurrence entre eux et quiconque veut devenir mineur le peut, il n'y a aucune barrière à l'entrée. Jusque là, pas de difficulté, les coûts de transaction devenant les prix sur un marché où tous les agents sont en situation de concurrence. Cependant, si les mineurs ont le rôle de valider les transactions, ils ont aussi celui, par le même mécanisme indissociable, d'assurer la sécurité de tout le protocole. C'est leur travail qui interdit à quiconque le voudrait de «fermer» Bitcoin. Mais cette fonction de sécurisation est une externalité positive. Si on laisse donc les coûts de transaction être le résultat de la confrontation entre la demande et l'offre pour la

validation des transactions, l'offre des mineurs sera trop faible et par conséquent la sécurité du système ne sera pas assurée. Bien sûr, la réponse naturelle d'un économiste serait de subventionner l'activité des mineurs. Mais dans un système qui refuse la création monétaire à long terme et où toute taxe est une option techniquement ou politiquement difficile, voire impossible à mettre en œuvre (le consensus des utilisateurs et mineurs est nécessaire pour qu'une telle modification du protocole soit adoptée), cette solution n'est pas acceptable. La question de l'alignement des intérêts publics et privés devient alors pleine de pertinence dans ce cadre.

Comme nous l'avons dit, l'émission de bitcoins est limitée. A sa création en 2009, 50 bitcoins étaient créés toutes les dix minutes environ et versés au crédit des mineurs. Tous les quatre ans approximativement, cette récompense, qui constitue la seule source de création de bitcoins dans le système, est divisée par deux, de sorte que la quantité de bitcoins en circulation tend asymptotiquement vers 21 millions. Aujourd'hui, quelques 13 millions de bitcoins sont en circulation. Ainsi, à très long terme (le dernier bitcoin sera émis vers 2140), Bitcoin en tant que monnaie sera déflationniste et ne pourra pas s'adapter à la conjoncture économique. La macroéconomie peut certainement apporter une meilleure compréhension des conséquences de ces caractéristiques dans un monde où Bitcoin est en concurrence monétaire avec les monnaies nationales traditionnelles mais aussi, comme nous le verrons plus bas, d'autres monnaies «électroniques».

Enfin, pour donner un dernier exemple, Bitcoin est un protocole «open-source» et celà est nécessaire. En effet, Bitcoin ne peut subsister comme monnaie que si chacun peut avoir une confiance totale dans toutes ses caractéristiques et seul l'accès libre à son code source peut garantir cette confiance. Mais une des conséquences de l'ouverture de Bitcoin implique la possibilité de créer indéfiniment et sans coût des clones plus ou moins modifiés de ce protocole. Il existe aujourd'hui plus de 450 protocoles qui ont été créés sur le modèle de Bitcoin. Dans ce cadre, l'Economie peut aider à analyser cette situation qui s'approche d'un modèle de concurrence monétaire où chacun pourrait créer sans coût sa propre monnaie. Cependant, il existerait une spécificité par rapport au modèle de monnaie privée puisque la quantité émise de chaque monnaie doit être spécifiée ex-ante dans chaque protocole.

Bitcoin au service de la science économique

Si la science économique peut apporter une meilleure compréhension du protocole Bitcoin, la contribution de Bitcoin à la science économique est, elle aussi, possible et même souhaitable. Donnons ici aussi quelques exemples.

Tout d'abord, assez évidemment, Bitcoin soulève la question de la nature et de la définition de la monnaie telles que celles-ci sont comprises actuellement. Théoriquement, rien ne s'oppose à ce que Bitcoin devienne une réserve de valeur (aujourd'hui assez risquée étant donnée la volatilité du cours des bitcoins) ou une unité de compte. Bitcoin est aussi en train de devenir un moyen d'échange de plus en plus répandu. Et sur ce dernier point, Bitcoin a beaucoup d'avantages par rapport aux moyens déjà existants. Par exemple, parce que c'est un objet virtuel et sans frontière, une transaction internationale en bitcoins peut se faire sans coût et presque instantanément en bitcoins. Notons seulement, qu'aucune institution ne garantit la valeur des bitcoins ni qu'aucune institution n'est responsable de leur impression. Une conséquence est que ,par rapport à un système avec une Banque Centrale, la confiance nécessaire de l'utilisateur est déplacée d'une institution vers un programme informatique, voire vers les algorithmes de cryptographie qui régissent le protocole Bitcoin.

Bitcoin ouvre aussi de nouveaux horizons pour les économistes. Prenons l'exemple des contrats. Ceux-ci sont toujours soumis à des contraintes de faisabilité. Ainsi, de nombreuses études se donnent pour but de trouver les meilleurs contrats dans des situations où l'optimum sans contrainte ne peut être obtenu. Bitcoin peut permettre de repousser certaines limites de faisabilité qui sont existantes aujourd'hui et ainsi rapprocher le second rang du premier. On peut, dès à présent, effectuer grâce à Bitcoin des mises sous séquestre sans tierce partie (particulièrement utile dans le cas du commerce électronique où la confiance entre acheteur et vendeur qui ne se connaissent pas est peu justifiée), des contrats avec paiements conditionnels (pensons ici à la possibilité de créer facilement des marchés complets), des opérations d'horodatage et même des élections totalement sécurisées et auditables par tous. Ces quelques exemples sont seulement quelques idées qui ont été proposées et sont en cours de développement. En fait, les possibilités sont certainement infinies. Puisque Bitcoin est fondamentalement un langage, tout ce que permet Bitcoin est à inventer. C'est en considérant ce point qu'un récent rapport d'information de la commission des finances du Sénat a recommandé de bien prendre en compte les «opportunités à découvrir» de Bitcoin quand la question de son statut fiscal est étudié.