LES ECONOMISTES DE TSE SUR LES CRYTPO-MONNAIES

AVRIL 2018

L'analyse de Bruno Biais, chercheur TSE
sur les dimensions technologiques et socio-politiques
des crypto-monnaies.

Toulouse School of Economics

ÉDITO

L'objectif de Nakamoto était de permettre la création et la circulation d'une monnaie sans aucune intervention d'une banque centrale ou d'institutions financières. Pour ce faire, il a créé le protocole de la chaine de blocs et la crypto-monnaie bitcoin. Comme l'écrit Nakamoto dans le résumé au début de son article de 2008 :

"Une monnaie électronique gérée par un réseau de pairs ("peer to peer network") permettrait d'effectuer des paiements en ligne sans recourir à un intermédiaire financier. Les signatures digitales joueraient un rôle dans ce réseau, mais ne seraient pas suffisantes pour éviter le recours à un tiers de confiance. Nous proposons une solution à ce problème."

Un bitcoin ne valait pas plus de 50 cents en 2010, aujourd'hui il vaut près de 10 mille dollars. Belle performance ! Et pourtant, le bitcoin fait l'objet de doutes et même de critiques sévères. Ainsi, en 2018, à l'université de Francfort, le président de la Banque des Règlements Internationaux disait *(voir son allocation sur* ***https://www.bis.org/speeches/sp180206.htm****)*

"Une monnaie est une indispensable convention sociale, bénéficiant du soutien d'une institution publique responsable en laquelle on a confiance. La meilleure institution de ce type étant une banque centrale… Les jetons digitaux privés qui se prétendent des devises, comme bitcoin, ne doivent pas mettre en danger la confiance en la valeur fondamentale et la nature de la monnaie."

De sérieux avertissements ont aussi été prononcés par les plus grands économistes, au rang desquels Joseph Stiglitz ou Jean Tirole, lequel écrivait dans une lettre ouverte au Financial Times le 30 Novembre 2017.

"Nous devons être prudent face à la hausse du bitcoin : les investisseurs doivent être protégés, et les banques régulées, les compagnies d'assurance et les fonds de pension ne devraient pas être autorisés à s'exposer au risque de ces instruments… Les gouvernements qui considèrent avec sympathie le bitcoin et les ICO devraient protéger leurs citoyens et leurs institutions financières contre le risque d'évolutions couteuses pour la société."

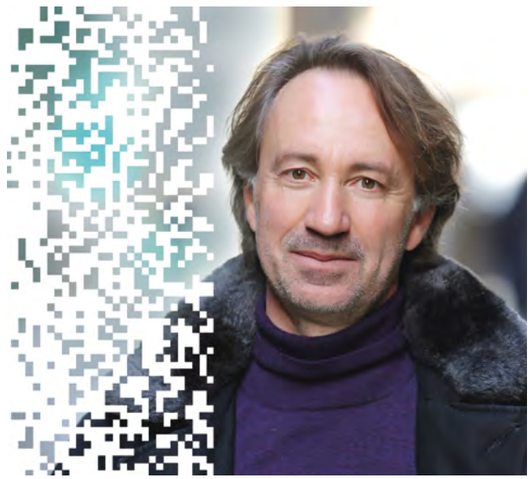
Deux visions s'opposent donc : d'un côté la vision libertarienne et technologique, selon laquelle la monnaie est créée et échangée dans un réseau de pairs, grâce à un protocole informatique, sans aucune intervention extérieure ; de l'autre coté la vision institutionnelle et politique, selon laquelle la monnaie ne peut être digne de confiance que si son émission est encadrée par une institution publique fiable, telle qu'une banque centrale indépendante.

Le développement des crypto-monnaies s'inscrit donc dans le contexte de deux tendances lourdes de nos sociétés : remise en cause de l'establishment et des institutions, essor et influence révolutionnaire des nouvelles technologies de l'information. Plutôt qu'un pouvoir central, arbitre en dernier ressort de l'allocation et de la valorisation de la monnaie, les partisans des crypto-monnaies défendent l'idée d'une démocratie directe des internautes, se déployant dans le cadre d'une chaine de blocs publique, ouverte et transparente[1].

Comment se situer face à ces deux visions contradictoires ? Faut-il souscrire à la vision libertarienne ou à la vision institutionnelle ? La chaine de blocs et les crypto-monnaies vont-elles révolutionner nos sociétés et nos économies, ou bien ne sont-elles que de dangereuses illusions ?

Pour apporter un éclairage sur ces questions , Bruno Biais, chercheur TSE, utilise les outils de la théorie économique, afin d'analyser le fonctionnement de la chaine de blocs, dans la première partie, de ce cahier puis la valeur des crypto-monnaies, dans la seconde partie.

1/ Des institutions financières, des banques centrales et des entreprises développent actuellement des chaines de blocs privées. Ces initiatives sont très intéressantes, mais radicalement différentes des chaines de blocs publiques, qui sont décentralisées, transparentes et ouvertes à tous, alors qu'une chaine de blocs privée est gérée par une autorité centrale qui décide qui a accès à la chaine, qui peut intervenir et comment. Nous ne traiterons ici que des chaines de blocs publiques.



BRUNO BIAIS

Professeur à la Toulouse School of Economics, Bruno Biais est également chercheur senior au Centre de Recherche en Management (CNRS). Son travail a été publié dans Econometrica, le JPE, l'ARE, la Review of Economic Studies, le Journal of Finance et le RFS. Il a enseigné à HEC, CMU, LBS, Oxford et LSE. Il a été conseiller scientifique d'Euronext et du NYSE. Il a reçu la médaille de bronze du CNRS et est membre de la Société économétrique. Il a été rédacteur en chef de la Review of Economic Studies et co-éditeur du Journal of Finance.

DOMAINES DE RECHERCE

- Microstructure du marché
- Finance d'entreprise
- Contrats financiers
- Économie politique
- Psychologie et économie
- Économie expérimentale

Le fonctionnement d'une chaîne de blocs

Le résumé au début de l'article de Nakamoto (2008), dont nous avons plus haut cité les premières phrases, continue de la manière suivante :
"Le réseau date les transactions en les incluant dans une chaine de "hash-based proof of work", donnant ainsi lieu à un enregistrement qui ne peut être changé sans refaire la "proof of work". La chaine la plus longue sert non seulement de preuve de la séquence d'événements enregistrés, mais aussi de preuve que ces enregistrements ont été effectués par la capacité de calcul agrégée la plus puissante. Tant que la majorité de la capacité de calcul est contrôlée par des nœuds qui ne s'allient pas pour attaquer le réseau, elle donnera lieu à la chaine la plus longue et dépassera les attaquants. La structure du réseau est minimale : les messages sont diffusés dans la mesure du possible, les nœuds peuvent quitter le réseau quand ils le veulent, et, quand ils reviennent au réseau, acceptent la plus longue chaine de blocs."

Ces phrases ne sont pas évidentes à comprendre au premier abord. En particulier elles utilisent des expressions mystérieuses, comme *"proof of work"*, *"hash"* et *"chaine la plus longue"*. Pour essayer de clarifier tout cela, nous allons dans un premier temps expliquer l'objectif et le mécanisme de la chaine de blocs. Dans un deuxième temps nous présenterons les prédictions de la théorie économique pour le fonctionnement de cette chaine.

La vision de Nakamoto *(2008)*

Rappelons d'abord les trois caractéristiques essentielles de la chaine de blocs :

1) C'est un registre indiquant à qui (en fait à quelle identification informatique) appartiennent des objets ou des actifs, par exemple des bitcoins. Chaque bloc dans la chaine décrit les modifications du registre.

2) C'est un registre distribué car il est accessible à tous ceux qui se connectent au réseau, et qui peuvent ainsi le consulter, et aussi le modifier. La chaine de blocs est une "distributed ledger technology".

3) Dans ce registre distribué les décisions sont prises par les internautes membres du réseau. Le protocole de la chaine de blocs organise ainsi une sorte de « vote informatisé » par les membres du réseau. L'objectif est que nul ne puisse décider à lui seul (au contraire de ce qui se passe avec une autorité centrale). En fait, plutôt qu'un vote stricto sensu, le protocole de la chaine de blocs permet une sorte de tirage au hasard, parmi tous les membres du réseau. Pour chaque bloc, c'est-à-dire pour chaque modification de la chaine de blocs, on tire au sort un membre du réseau, qui décide ou non de valider la modification.

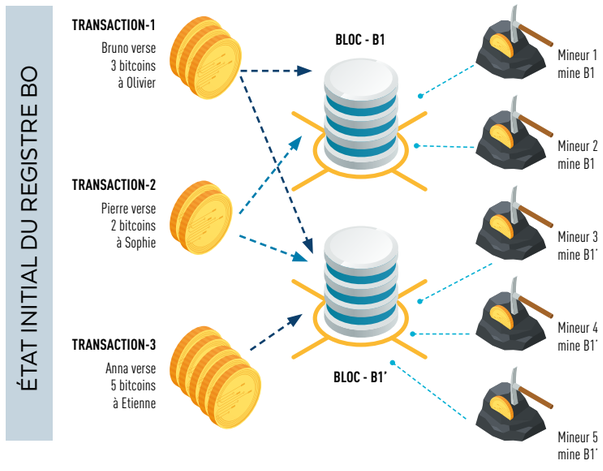


Figure 1A : mineurs, transactions et blocs

La première chaine de blocs, et la plus importante aujourd'hui encore, est le registre indiquant à qui appartient chaque bitcoin. Lorsqu'un détenteur de bitcoin l'échange contre un bien, un service, ou une autre monnaie, il en informe le réseau. La tâche du réseau est alors de valider cette transaction, de l'inclure dans un bloc avec d'autres transactions, et de rattacher ce bloc à un bloc précédent. Cette chaine révisée par l'ajout d'un bloc supplémentaire donne le nouvel état du registre.

Les membres du réseau procédant à cette validation des transactions et ce rattachement des blocs sont les mineurs. Nakamoto (2008) décrit la façon dont il propose que les mineurs travaillent *(illustrée dans la Figure 1)*:

I) Le mineur reçoit sur le réseau les messages indiquant les transactions ;

II) il regroupe un ensemble de messages dans un bloc ;

III) il vérifie que ces messages sont valides (par exemple que ceux qui disent qu'ils ont transféré un bitcoin le possédait bien) - cette étape est très rapide ;

IV) il travaille à résoudre un problème numérique très compliqué, sans aucun intérêt intrinsèque, et sans aucune relation avec le nombre ou la nature des transactions contenues dans le bloc.

Dès qu'un mineur a résolu son problème numérique, il annonce au réseau qu'il vient de résoudre un bloc donné, et à quel bloc précédent il le rattache. Les autres mineurs reçoivent cette information. Ils pourraient choisir de l'ignorer, et continuer à chercher la solution du problème correspondant à leur bloc. Cependant, Nakamoto (2008) recommande aux mineurs d'abandonner leur propre bloc, commencer à en miner un nouveau, et l'enchainer au bloc qui vient d'être résolu. Suivre cette recommandation c'est suivre la règle de la chaine la plus longue, qui stipule qu'à tout moment le bloc qu'un mineur cherche à résoudre doit s'enchainer à la chaine la plus longue à ce moment-là.

Supposons donc que les mineurs suivent la règle de la chaine la plus longue. Après qu'un bloc a été résolu, ils vérifient que la solution proposée par le mineur est la bonne. Cette vérification est rapide car si les problèmes numériques proposés aux mineurs sont difficiles à résoudre, leur solution est facile à vérifier. En effectuant cette vérification, les participants au réseau obtiennent la preuve que le mineur a bien fait son travail : c'est la "proof of work". Après avoir vérifié la "proof of work", les mineurs décident d'accepter le nouveau bloc ou non. S'ils l'acceptent, ils enchainent à ce bloc les blocs qu'ils résoudront eux-mêmes par la suite.

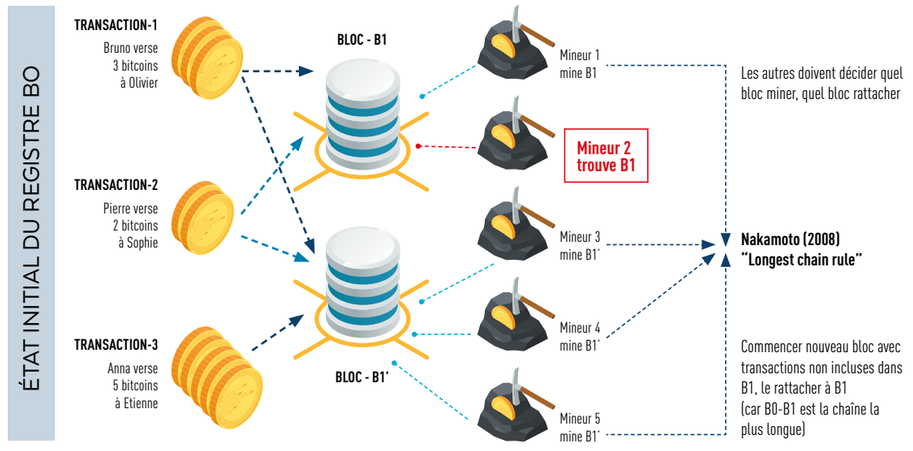


Figure 1B : règle de la chaîne le plus longue

Qu'est-ce qui pourrait amener un mineur à suivre la règle de la chaine la plus longue et abandonner le minage de son propre bloc pour se concentrer sur le bloc qui vient d'être résolu par un autre mineur ?

Un premier élément de réponse est fourni par la nature du processus de résolution des blocs. Pour résoudre le problème numérique correspondant à son bloc, le mineur tire des solutions au hasard et à chaque tirage teste si c'est la bonne solution. Pour ce faire, le mineur utilise des ordinateurs. Plus la capacité de calcul de ces ordinateurs est grande, plus le nombre de solutions possibles que le mineur tire chaque seconde (hash rate) est grand, et plus il résout vite son problème en moyenne. Cependant, à capacité de calcul et difficulté du problème constantes, le nombre de tirage au hasard que le mineur devra faire avant de trouver la solution est une variable aléatoire. Par conséquent, le temps de résolution d'un problème est variable. Une propriété très importante de cette variable aléatoire est que le temps qui reste avant la résolution d'un problème est indépendant du temps déjà passé à tenter de résoudre ce problème. On peut avoir l'intuition de cette propriété en imaginant que le mineur effectue des tirages avec remise dans une urne contenant de nombreuses boules, dont l'une contient la solution

alors que les autres ne contiennent aucune information. Dès lors, un mineur qui a travaillé une seconde sur son problème a autant de chances de le résoudre pendant la seconde suivante qu'un mineur qui a déjà travaillé un quart d'heure sur son problème. De ce point de vue, un mineur n'a pas plus intérêt à s'obstiner sur le problème qu'il a commencé à chercher à résoudre qu'à s'attaquer à un problème nouveau.

Mais pourquoi les mineurs consacrent ils leur capacité de calcul, leur temps et leur électricité à la résolution des blocs ? C'est parce que, pour chaque bloc résolu, le mineur reçoit une récompense. Ainsi, dans le protocole bitcoin il est prévu que le mineur qui résout un bloc reçoit un certain nombre de bitcoins, actuellement 12,5. En pratique, le mineur inscrit dans son bloc une transaction qui attribue ces bitcoins à lui-même. Si les autres mineurs expriment leur accord avec le bloc qu'il a miné, en y enchainant les leurs, ils expriment leur accord à l'attribution de cette récompense. Ces 12,5 bitcoins sont créés ex nihilo. Ce sont ces récompenses qui alimentent la création de la crypto-monnaie. Cette création monétaire est prédéterminée par le protocole Bitcoin, qui prévoit que le montant gagné par un mineur baissera progressivement. Il était initialement égal à 50 bitcoins, et est divisé par 2 tous les 4 ans. Ainsi il s'établira à 6,25 en 2020. En 2140, 21 millions de bitcoins auront été miné, et il est prévu que la création monétaire de bitcoin s'arrête alors.

Comment les mineurs seront-ils rémunérés lorsque la création de bitcoin cessera? En plus de la création monétaire, les mineurs bénéficient du paiement de commissions par les agents économiques à l'origine des transactions. Si je veux transférer 1 bitcoin à un de mes enfants, et désire que cette transaction soit rapidement minée, je promets une commission élevée, par exemple 0,01 bitcoin, au mineur qui résoudra le bloc incluant ma transaction. Quand il n'y aura plus de création monétaire, les mineurs seront rémunérés seulement par ces commissions.

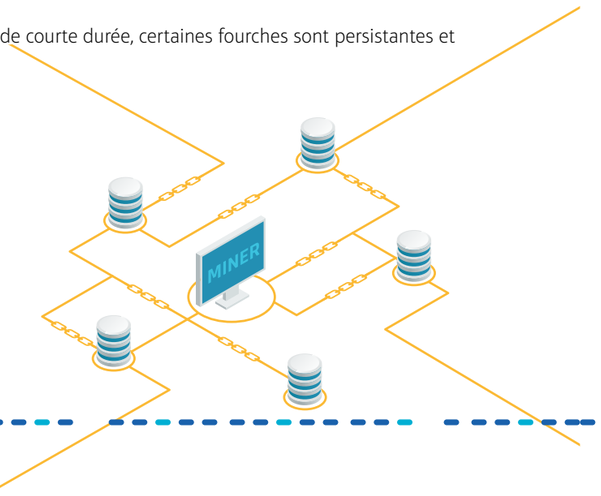
Selon la vision de Nakamoto (2008), le protocole décrit ci-dessus, et le respect de la règle de la chaine la plus longue, doivent permettre l'émergence d'une chaine unique, transparente et ouverte à tous, proposant un registre faisant l'objet d'un consensus fiable et durable. Cette vision est-elle réaliste ? Qu'a-t-on observé en pratique, et quel éclairage apporte la théorie sur ce qui s'est produit dans le passé et sur ce qui peut se produire dans l'avenir ?

L'épreuve des faits et de la théorie

Le constat premier est que le bitcoin connait un immense succès. Beaucoup de personnes en achètent et en vendent, ce qui donne lieu à de nombreuses transactions, qui sont validées par les mineurs. De manière correspondante, on observe un nombre croissant de mineurs, utilisant une capacité de calcul et une quantité d'électricité croissantes *(10 térawatt-heure il y a un an, 44 il y a 3 mois, 62 aujourd'hui, voir* ***https://digiconomist.net/bitcoin-energy-consumption****)*. Cette consommation d'électricité correspond actuellement à celle de la Suisse. D'autres crypto-monnaies, elles aussi utilisatrices de capacité de calcul et d'électricité, connaissent un grand succès, au premier rang desquelles l'ether, basée sur la chaine de blocs Ethereum.

En fait on observe la création de très nombreuses nouvelles crypto-monnaies, créant souvent des fourches depuis les crypto-monnaies initiales. Ainsi, durant l'été 2016, une fourche s'est produite sur Ethereum, donnant lieu à une crypto-monnaie concurrente, ether classic. En août 2017, une fourche s'est produite dans Bitcoin, donnant lieu à la création de Bitcoin Cash, et à l'automne 2017, une nouvelle fourche est apparue avec Bitcoin Gold. En décembre 2017, alors que le cours du bitcoin s'envolait, le rythme d'apparition des fourches a connu une forte accélération, avec Super Bitcoin, Bitcoin X, Oil Bitcoin, Bitcoin World, Lightning Bitcoin, etc.

Même si la plupart des fourches récentes seront vraisemblablement de courte durée, certaines fourches sont persistantes et attirent mineurs et investisseurs. C'est le cas, par exemple, de Bitcoin Cash. Le nombre de tirage de solutions par seconde (hash rate) sur le réseau bitcoin s'élève actuellement à 30 exahash par seconde (30 fois 10 puissance 18). Ce n'est que 8 fois plus élevé que celui de Bitcoin Cash. D'ailleurs un bitcoin cash vaut à peu près 0,16 bitcoins. Or chaque fourche I) correspond à une déviation de la règle de la plus longue chaine proposée par Nakamoto, II) éloigne du consensus en créant des chaines de blocs proposant des registres différents, et III) risque d'éroder la valeur des crypto-monnaies.



Pourquoi cette multiplication des fourches ? Comment est-elle possible, alors que Nakamoto annonçait l'émergence d'une chaine de blocs unique ?

À l'origine des principales fourches mentionnées ci-dessus il y a des désaccords au sein de la communauté des mineurs et développeurs. Dans le cas d'Ethereum Classic, des ethers avaient été détourné d'un fonds de placement (TheDAO, acronyme de Decentralized Autonomous Organization). Des membres de la communauté avaient proposé de revenir en arrière dans la chaine des blocs, pour annuler le détournement de fonds. On crut d'abord que toute la communauté se rangeait à cette solution, mais on s'aperçut rapidement qu'une minorité s'y opposait, car elle était attachée au principe de l'immutabilité de la chaine de blocs. Un an et demi plus tard, cette fourche subsiste : l'ether classic vaut environ 20 dollars, alors que l'ether vaut environ 700 dollars. Dans le cas de Bitcoin Cash, il s'agissait d'un désaccord sur la manière de modifier le protocole pour accroitre la taille des blocs, et dans le cas de Bitcoin Gold le désaccord portait sur l'utilisation d'ASIC, des circuits intégrés spécifiques, qui ne peuvent être utilisés que pour le protocole Bitcoin, et dont la production est dominée par une puissante entreprise chinoise.

Par-delà ces désaccords, il y a une raison profonde à l'apparition de ces fourches : le minage est un jeu de coordination, qui admet des équilibres multiples, et des fourches sur le sentier d'équilibre. Pour comprendre ce phénomène, rappelons-nous que les mineurs sont récompensés par des bitcoins nouvellement créés, inscrits dans le bloc qu'ils résolvent. Or ces bitcoins ne seront reconnus comme valables par les autres agents économiques que si le bloc lui-même est reconnu comme valable. Ce sera le cas si les autres mineurs décident d'enchainer leurs propres blocs à ce bloc. Et ils le feront s'ils pensent que la chaine dans laquelle est incluse ce bloc est la chaine faisant l'objet d'un consensus. Ainsi, de multiples équilibres peuvent émerger. Dans un équilibre, les mineurs anticipent que la chaine A va faire l'objet d'un consensus, ils décident alors de rattacher leurs blocs à cette chaine, par conséquent la chaine attire de nombreux blocs, faisant ainsi l'objet d'un consensus, conformément à l'anticipation initiale, qui s'avère rationnelle. Mais dans un autre équilibre la grande majorité des mineurs pensent que A n'est pas valable, ils décident donc de rattacher leurs blocs à d'autres chaines, A est abandonnée, s'avérant ainsi non valable, conformément à l'anticipation initiale. Dans notre article de recherche en commun avec Christophe Bisière, Matthieu Bouvard et Catherine Casamatta *("The blockchain folk theorem")* nous montrons l'existence de ces équilibres multiples, et que plusieurs fourches concurrentes coexistent à long terme à l'équilibre, voir :
https://www.tse-fr.eu/sites/default/files/TSE/documents/doc/wp/2017/wp_tse_817.pdf

Pour conclure cette première partie, rappelons que, conformément à la vision de Nakamoto, la chaine de blocs fonctionne, attire des mineurs et sert de registre pour des crypto-monnaies qui sont valorisées par les investisseurs. Cependant, en contradiction avec la vision de Nakamoto, les mineurs ne suivent pas toujours la règle de la chaine la plus longue, il n'y a pas de chaine unique faisant l'objet d'un consensus complet, mais des fourches proposant différentes versions du registre. L'apparition et la persistance de ces fourches est liée au fait que le minage est un jeu de coordination, qui admet de multiples équilibres.

La valeur économique d'une cryptomonnaie

Étant données les promesses et les difficultés de la technologie de la chaine de blocs sur laquelle elles sont fondées, quelle est la valeur économique des crypto-monnaies ? Pourraient-elles un jour concurrencer les monnaies supervisées par les banques centrales ? Pour apporter un éclairage sur cette question, nous commencerons par préciser la fonction économique de la monnaie, puis nous nous interrogerons sur la capacité des crypto-monnaies à remplir cette fonction.

Qu'est-ce qu'une monnaie, en général, et quels sont les déterminants de sa valeur ?

Une monnaie est quelque chose que j'accepte en paiement car j'anticipe qu'elle sera acceptée en paiement par les autres quand je voudrai à mon tour acheter. Dès cette définition, notre attention est attirée sur la notion d'anticipation, de croyance. Nous verrons qu'en ce qui concerne la monnaie tout est affaire de croyances.

Pour réfléchir au rôle économique de la monnaie, on peut commencer par considérer une économie de troc, et ensuite analyser comment la situation s'améliore quand on introduit la monnaie.

Dans une économie de troc, où seulement des échanges bilatéraux de biens et services prévalent, se pose le problème de la double coïncidence des besoins. Supposons qu'Alain a des abricots mais aime les carottes, alors que Bernard aime les abricots

mais a des bananes. Lorsqu'Alain rencontre Bernard, Bernard voudrait les abricots d'Alain, mais Alain n'a pas envie des bananes de Bernard. Il n'y a pas double coïncidence des besoins, l'échange ne peut avoir lieu.

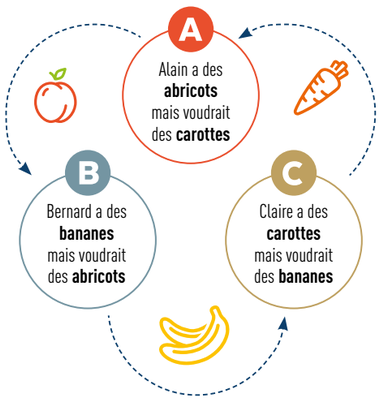
Pour permettre des échanges, on a besoin d'une relation sociale plus sophistiquée, comme celle analysée par le Triangle de Wicksell, grand économiste suédois né en 1851 et mort en 1926 *(voir Figure 2)*. Supposons qu'en plus d'Alain et Bernard, il existe un troisième agent économique, Claire, qui a des carottes mais aime les bananes. Gardons l'hypothèse que les transactions sont bilatérales et supposons de plus que les fruits ou légumes ne peuvent être achetés, stockés puis revendus.

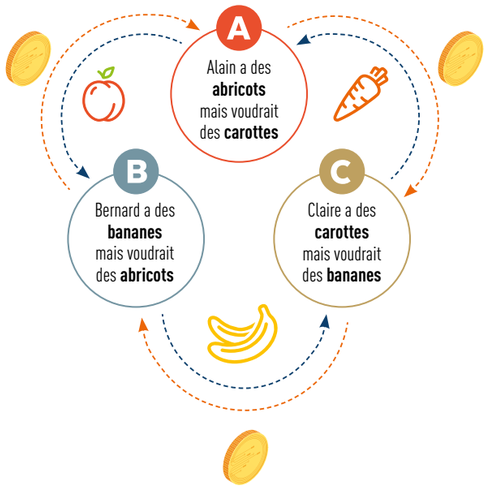
Pour que chacun puisse manger le fruit qu'il aime, il faudrait les échanges suivants :

- *Alain donne ses abricots à Bernard*
- *Bernard donne ses bananes à Claire*
- *Claire donne ses carottes à Alain*

Comment parvenir à cette allocation ? Il suffit d'introduire une pièce de monnaie, jeton, ou "coin", créée, par exemple, par une autorité centrale, roi Crésus ou banque centrale, qui accepte de la prêter, mais exige qu'on la lui rende à la fin des échanges. Dans ce contexte on peut parvenir à l'allocation optimale de la façon suivante :

- *Bernard emprunte un jeton à la banque centrale et donne ce jeton à Alain en échange de ses abricots.*
- *Alain donne alors un jeton à Claire en échange de ses carottes.*
- *Finalement Claire donne un jeton à Bernard en échange de ses bananes, et Bernard peut rendre le jeton à la banque centrale.*





Dans ce modèle, alors qu'elle n'a aucune valeur intrinsèque, la monnaie permet de réaliser des échanges, et ainsi d'améliorer la satisfaction de tous les agents économiques. On peut généraliser ce type de modélisation de la monnaie à de nombreux agents, interagissant pendant de nombreuses période. Une telle généralisation est proposée par le modèle à générations imbriquées, initialement proposé par Maurice Allais en 1947 dans son ouvrage *Économie et Intérêt*.

Le Triangle de Wicksell illustre bien le rôle crucial joué par les croyances dans le fonctionnement des échanges monétaires : Alain accepte le jeton que lui propose Bernard en échange de ses abricots, car il anticipe que Claire, à son tour, acceptera le jeton qu'il lui proposera en échange de ses carottes. Quant à Claire, si elle accepte le jeton d'Alain, c'est parce qu'elle anticipe que Bernard, à son tour, acceptera le jeton qu'elle lui proposera en échange de ses bananes. C'est donc bien un équilibre en anticipations rationnelles que tous acceptent la monnaie, car ils pensent qu'elle sera acceptée. Mais cette hiérarchie de croyances (croyances, croyances sur les croyances, etc.) n'est pas la seule possible à l'équilibre. Il existe aussi un équilibre de la défiance : chacun croit que les autres n'accepteront pas le jeton qu'il proposera, donc chacun refuse d'accepter le jeton qu'on lui propose. La défiance est ainsi une anticipation rationnelle. Nous retrouvons, ici encore, la multiplicité des équilibres que nous avions rencontrée dans notre analyse de la chaine de blocs.

Dans l'analyse ci-dessus, tous les fruits et légumes avaient le même prix : un jeton. Dans un environnement plus complexe, de nombreux prix vont intervenir : prix variés des différents biens et services relativement à une monnaie (par exemple prix de la baguette en euros) mais aussi prix des différentes monnaies les unes par rapport aux autres (par exemple cours de l'euro vis-à-vis du dollar). Que nous apprend la théorie économique sur ces prix ?

Comme le montre Jean Tirole dans son article publié en 1985 dans Econometrica *"Asset bubbles and overlapping generations"*, les monnaies sont un actif bien particulier, tout à fait différent d'actifs comme les actions : la valeur fondamentale de ces dernières reflète la valeur actuelle des biens réels et services qu'elles produiront dans le futur. C'est donc le fondamental à venir qui détermine le prix aujourd'hui. À l'inverse, les monnaies ne créent pas de bien réel, mais procurent un service de transaction : on pourra les utiliser dans le futur pour acheter des biens ou services. Or la valeur de ce service croit avec le prix qu'aura la monnaie dans le futur. Plus le cours de l'euro sera élevé dans un mois, plus le service de transaction que me procurera dans un mois l'euro que j'achète aujourd'hui sera élevé. Ainsi, au contraire des actions, c'est le prix futur qui détermine la valeur fondamentale aujourd'hui. Dès lors le prix aujourd'hui reflète les croyances au sujet du prix de demain.

Et, à nouveau, l'importance des croyances entraine l'existence de nombreux équilibres en anticipations rationnelles : certains dans lesquels le cours de la monnaie est faible aujourd'hui car on anticipe qu'il sera faible demain, et d'autres dans lesquels il est élevé aujourd'hui car on anticipe qu'il sera élevé demain! De plus, au cours du temps, les croyances peuvent changer, même si rien ne change dans l'économie réelle, entrainant des fluctuations, de la volatilité, dans le cours des monnaies.

Comment stabiliser la valeur de la monnaie ? En coordonnant les anticipations. C'est le rôle de l'autorité centrale. Rôle qu'elle peut exercer si elle est fiable, comme peut l'être, par exemple, une banque centrale indépendante et dont les objectifs et la détermination sont clairs. Un instrument supplémentaire pour ancrer les anticipations est de s'engager à accepter la monnaie en paiement, comme le fait l'état d'un pays en s'engageant à accepter la devise nationale pour le paiement des impôts.

Mais, si l'intervention d'une autorité centrale peut stabiliser les cours, en coordonnant les anticipations, elle peut aussi déstabiliser la monnaie. C'est le cas lorsque l'état est prédateur. Il peut alors spolier la valeur des avoirs monétaires en créant de l'inflation ou bien en empêchant les agents économiques d'utiliser leurs avoirs, par exemple en instaurant un contrôle des capitaux. En amont, la défiance par rapport à l'autorité centrale, état ou banque centrale, peut entrainer des croyances pessimistes, et une baisse de la valeur de la monnaie.

Comment situer les crypto-monnaies par rapport à ce cadre d'analyse ?

Dans la logique de l'inspiration libertaire qui a présidé à sa création, le bitcoin peut s'avérer très utile lorsque la situation politique empêche les agents d'utiliser la monnaie émise par la banque centrale et le système bancaire pour satisfaire pleinement leurs besoins. Ainsi, la faillite politique du Zimbabwe est telle que sa monnaie a perdu toute crédibilité, et son système bancaire est devenu extrêmement fragile et risqué.

Pour régler leurs transactions les agents économiques se sont donc tournés vers le bitcoin, qui ne peut être confisqué par le pouvoir politique. De même, au Venezuela, l'inflation galopante et la crise politique ont presque annulé la valeur et la crédibilité de la monnaie nationale. Les agents économiques se sont donc tournés vers les crypto-monnaies, en particulier le bitcoin ou l'ether. En fait, comme l'électricité est peu couteuse au Venezuela, les agents économiques se sont même lancés dans le minage de crypto-devises. En Chine, le gouvernement contrôle les banques et les mouvements de capitaux hors du pays. Pour contourner ces contrôles, les chinois ont eu, de plus en plus, recours aux crypto-monnaies. C'est ce qui explique la réaction très négative du gouvernement chinois par rapport à ces monnaies, et les régulations visant à restreindre leur utilisation.

Même si la situation politique d'un pays est relativement stable, il est possible que son système bancaire soit peu développé et peu efficace, rendant les paiements difficiles et couteux. Le règlement de transactions par crypto-monnaies sur internet pourrait alors s'avérer utile. Les crypto-monnaies pourraient aussi être utiles pour effectuer des transferts de fonds internationaux quand les méthodes traditionnelles de transfert sont inefficaces et couteuses.

Le développement de l'utilisation des crypto-monnaies se heurte cependant à de nombreux inconvénients, parmi lesquels figurent les suivants :

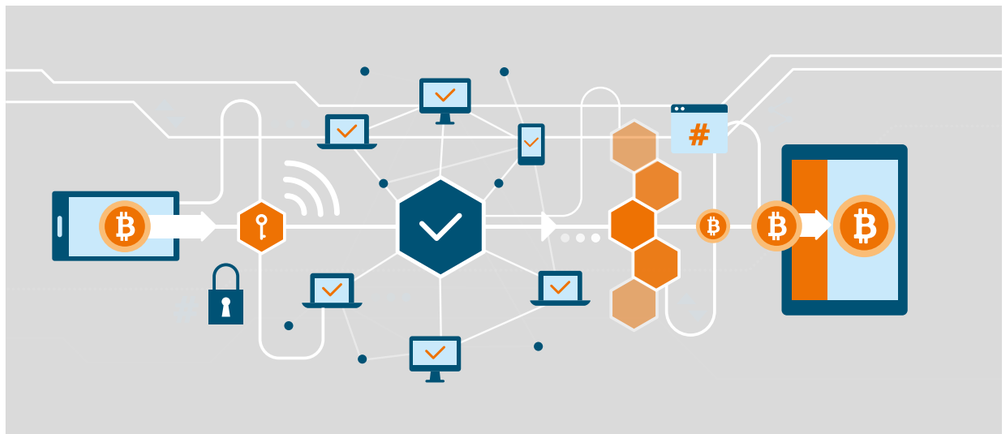
a) Comme on l'a rappelé plus haut, la valeur d'une monnaie à un moment donné dépend des anticipations quant à sa valeur future. Or ces anticipations peuvent fluctuer considérablement, rendant le cours de la monnaie volatil. C'est probablement ce phénomène qui est à l'origine de la grande volatilité du bitcoin. De plus, par définition, nulle autorité centrale ne peut intervenir pour stabiliser le cours de la crypto-monnaie. Une conséquence de la grande volatilité des crypto-monnaies est qu'elles ne peuvent remplir une des trois fonctions essentielles de la monnaie qui est de servir d'unité de compte.

b) L'utilisation d'une crypto-monnaie pour payer un bien ou un service expose à un risque de contrepartie difficile à gérer : soit le vendeur ne livre son bien qu'après que la chaine de bloc a validé le transfert de la crypto-monnaie, et dans ce cas l'acheteur est exposé au risque que le vendeur ne livre pas le bien, soit le vendeur livre le bien immédiatement, auquel cas il est exposé au risque que la transaction ne soit finalement pas validée par la chaine de blocs.

c) L'essor des échanges de crypto-monnaies (alimenté par celui de la spéculation) a conduit à une congestion des chaines de blocs. Par exemple la chaine de blocs Bitcoin ne valide qu'un bloc toutes les dix minutes, et chaque bloc a une taille maximale d'un mégaoctet. Cela ralentit la vitesse avec laquelle les transactions sont validées. Pour que leur transaction soit incluse plus rapidement dans un bloc, et ainsi validée plus rapidement, les agents économiques peuvent promettre des commissions aux mineurs (comme cela a été expliqué plus haut). La commission moyenne pour une transaction sur Bitcoin est aujourd'hui proche de 30 dollars. Congestion et commissions rendent donc la validation des transactions en bitcoins lente et couteuse, ce qui réduit la capacité de la crypto-monnaie de remplir une autre des trois fonctions essentielles de la monnaie, celle de moyen de paiement.

d) Pour résoudre le problème de la congestion, il faudrait modifier le protocole, par exemple pour augmenter la taille des blocs. La communauté des mineurs et développeurs a cherché à résoudre ce problème depuis au moins un an, mais n'a pas encore réussi à se mettre d'accord sur une solution acceptée par tous. C'est que la coordination est difficile dans un contexte décentralisé.

e) Les crypto-monnaies ne jouent aujourd'hui qu'un rôle minime en tant que moyen de paiement, relativement aux monnaies émises par les banques et les banques centrales. Pour qu'elles puissent jouer un rôle significatif, il faudrait pouvoir augmenter le nombre de transactions validées, et, pour ce faire augmenter la taille des blocs. On vient de voir que cela s'avérait difficile.



CONCLUSION

Au début de notre réflexion nous avions noté que le développement des crypto-monnaie s'inscrivait dans le cadre de deux tendances lourdes de nos sociétés. L'une est de nature technologique : le recours croissant aux nouvelles technologies de l'information et de la communication. L'autre est de nature sociale et politique : la remise en cause des élites et le désir de redonner le pouvoir à la base. Que nous ont appris nos analyses sur les perspectives des crypto-monnaies au regard de ces deux dimensions, technologique et socio-politique ?

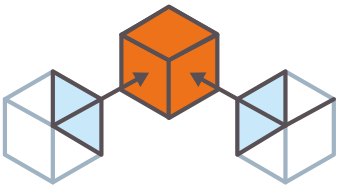
Du point de vue technologique, pour que les crypto-devises, qui actuellement ne jouent qu'un rôle très marginal dans les paiements, parviennent à jouer un rôle significatif, il faut qu'elles puissent valider un volume de transactions plus importants. Une solution pour augmenter ce volume serait de multiplier le nombre des crypto-monnaies et des chaines de blocs correspondantes. Cette solution ne serait guère satisfaisante, car la multiplication des crypto-monnaies réduirait leur fiabilité, alors que la multiplication des chaines de blocs (utilisant la "proof of work") accroitrait de manière non soutenable la consommation d'électricité. L'autre solution serait d'augmenter la taille de chaque bloc. On a vu plus haut que cette augmentation n'allait pas de soi. Supposons tout de même que la communauté des développeurs et mineurs finisse par mettre au point et adopter une modification du protocole augmentant la taille des blocs. Cette approche permettrait-elle d'augmenter le nombre de transactions validées sans une consommation d'électricité non soutenable ?

Dans un protocole reposant sur la "proof of work", plus la rémunération de la validation des blocs est élevée, plus les mineurs lui consacrent une grande capacité de calcul, plus la consommation d'électricité est grande. Pour limiter la consommation d'électricité, il faut donc limiter la rémunération de la résolution d'un bloc. On a vu plus haut que la récompense pour la résolution d'un bloc tend à décroitre : actuellement égale à 12,5 bitcoins, elle passera à 6,25 en 2020, puis 3,125 en 2024, etc. Cette tendance va dans le bon sens, mais pour qu'elle baisse la rémunération des mineurs il faut aussi que le cours du bitcoin ne soit pas trop élevé. Il est possible, et même probable que ce sera le cas, mais on ne peut en être sûr. De plus, il faut aussi que la valeur totale des commissions offertes par les agents économiques pour la validation de leurs transactions reste basse. Or s'il y a une augmentation du nombre des transactions (incluses dans des blocs plus larges) cela tendra à faire monter le niveau total des commissions. Pour contrer ce phénomène il faut que la valeur individuelle de chaque commission reste faible. Pour atteindre cet objectif, il est nécessaire que le réseau ne soit pas congestionné, mais plutôt en surcapacité. Cela nous ramène à la nécessité de l'augmentation de la taille des blocs, qui est vraiment une condition indispensable au développement des chaines de blocs et des cryptomonnaies.

Du point de vue politique et social, un des thèmes communs aux réflexions que nous avons proposées est la difficulté de coordonner les anticipations et les croyances d'agents économiques dispersés. Des croyances mal coordonnées et instables peuvent conduire à des mouvements de cours excessifs, et ainsi à des monnaies fragiles et volatiles. Des croyances mal coordonnées peuvent aussi conduire à une multiplication des fourches, empêchant la chaine de blocs de fonctionner correctement. C'est un problème important, qui pourrait grever l'avenir des chaines de blocs publiques et des crypto-monnaies. En effet, l'inspiration libertarienne de ces technologies interdit l'intervention d'une autorité centrale et exige que la coordination provienne de la base, ce qui est difficile à réaliser en pratique. En cela les crypto-monnaies diffèrent significativement des monnaies traditionnelles, pour lesquelles la banque centrale peut aider les agents à coordonner leurs croyances, comme le montrent Isabel Schnabel et Hyun Shin, dans un récent document de travail de la Banque des Règlements Internationaux, intitulé *"Money and Trust : Lessons from the 1620s for money in the digital age." (Voir* ***https://www.bis.org/publ/work698.htm****)*

Pour conclure cet exposé, rappelons un épisode d'histoire monétaire qui illustre bien les dangers créés par des croyances trop volatiles et mal ajustées. En 1707, John Law arrive en France. Il propose de remplacer les monnaies existantes (pièces en métal précieux) par des billets de papiers gagés sur les actions de la Compagnie des Indes Occidentale. Voilà bien une innovation, on pourrait même dire une disruption. En 1719, le cours des actions de la Compagnie est passé de 500 livres à 10000 livres. La monnaie nouvelle crée par John Law connait un succès retentissant. On se bouscule pour l'acheter. Certains la revendent à profit. Des nobles, des ecclésiastiques, des domestiques et des aubergistes amassent très rapidement des fortunes impressionnantes. En 1720, les cours s'effondrent, les billets du Mississipi ne valent plus rien, de nombreuses personnes sont ruinées.

LE GROUPE DE TRAVAIL TSE SUR LE BLOCKCHAIN



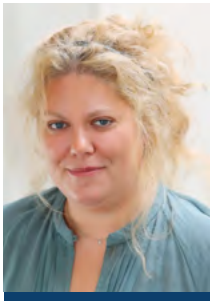
TSE a lancé en 2016 un groupe de travail sur la chaine de blocs avec six chercheurs : ***Bruno Biais, Christophe Bisière, Catherine Casamatta, Fany Declerck, Bertrand Gobillard*** *et* ***Alexandre Guembel.***

Le groupe a pour but d'expliquer l'impact de cette technologie sur l'intermédiation financière (système de paiement).

Bruno Biais

Christophe Bisière

Catherine Casamatta



Fany Declerck

Bertrand Gobillard

Alexandre Guembel

Toulouse School of Economics

www.tse-fr.eu - @TSEinfo
21 Allée de Brienne, F-31015 Toulouse Cedex 6
Tél. : 05 67 12 88 48 - priyanka.talim@tse-fr.eu