Les *blockchains* sont-elles stables ?

Professeur de finance, Christophe Bisière est membre du Centre de Recherche en Management (UMR5303, CNRS / Université Toulouse 1 Capitole) et à la Toulouse School of Economics. Ses recherches portent sur la microstructure des marchés financiers.

Conçue à l'origine pour valider les transactions au sein du réseau de monnaie virtuelle *Bitcoin*, la technologie *blockchain* (ou « chaîne de blocs ») promet aujourd'hui de révolutionner l'industrie des services financiers. Disparition d'intermédiaires rendus obsolètes, amélioration de la sécurité et réduction drastique des coûts des transactions financières, apparition de nouvelles applications innovantes à destination des entreprises ou des particuliers : les effets attendus sont de nature à bouleverser le secteur financier de manière durable.

Le potentiel de rupture de la technologie *blockchain* tient au fait qu'elle représente une solution très efficace à un problème générique : comment maintenir de manière décentralisée un registre partagé entre des participants n'ayant pas nécessairement confiance entre eux ? Dans le réseau Bitcoin, ce registre contient des transactions en monnaie virtuelle, permettant de reconstituer les avoirs de chacun et d'assurer qu'un participant ne peut dépenser plus de bitcoins qu'il n'en possède. Dans le réseau Ethereum, ces transactions sont de véritables programmes informatiques — appelés « contrats intelligents » — qui décrivent les conditions sous lesquelles se déclenchent des transferts entre les parties prenantes. Ils sont exécutés au sein de la *blockchain*, de manière automatique, irréversible et observable par tous.

La solution au problème du registre distribué sans recours à un tiers de confiance, proposée par la technologie *blockchain*, repose sur une combinaison astucieuse de technologies connues, comme les techniques de cryptographie, et de propositions originales, en particulier concernant le protocole permettant aux participants de parvenir à un consensus sur l'état courant du registre.

Si les propriétés des techniques de cryptographie sont bien connues, celles du protocole de consensus distribué le sont beaucoup moins. Pourtant, les conséquences d'une éventuelle rupture de ce consensus ne peuvent être négligées : les participants ne s'accordant plus sur l'état du registre, plusieurs « vérités » cohabitent au sujet des transactions effectuées et des droits de propriété de chacun. Une telle situation d'instabilité serait critique pour un système dont l'intérêt pour ses usagers dépend étroitement de la confiance qu'ils accordent à sa capacité à maintenir ce consensus.

Ainsi, la technologie *blockchain* est en passe d'être massivement utilisée dans nos systèmes financiers, alors que sa stabilité intrinsèque relève davantage d'une croyance généralement admise que d'une analyse rigoureuse. Dans un travail de recherche collectif[1], nous développons une analyse de la stabilité des systèmes à base de *blockchain*.

Comment fonctionne une *blockchain* ?

Dans un réseau *blockchain*, le flux des transactions à valider (c'est-à-dire à ajouter au registre) est dirigé vers des participants appelés « mineurs ». Chaque mineur stocke ces transactions dans un bloc, y ajoute une transaction spéciale correspondant à sa récompense pour ce bloc, puis cherche à valider ce bloc. Pour ce faire, il doit résoudre un problème numérique difficile, dont le bloc est une donnée en entrée, et qui ne peut être résolu que par la force brute. Le mineur procède donc par essais-erreurs, jusqu'à ce qu'il trouve une solution. Il diffuse alors ce bloc et sa solution (appelée une « preuve de travail ») au sein du réseau, pour informer les autres mineurs de son succès. Les autres mineurs vérifient que la solution reçue est bien correcte (une opération facile, contrairement à la recherche de la solution elle-même), et marquent leur acceptation de ce bloc en abandonnant leur bloc courant et en minant un nouveau bloc de transactions à valider, rattaché à ce bloc gagnant « parent ». Le processus de recherche et de diffusion de solutions se poursuit, créant de proche en proche une chaîne de blocs validés, représentant l'état courant du registre.

Une chaîne unique, comme celle du schéma 1, reflète un consensus parfait entre les participants : à cet instant, tous observent la même chaîne et la considèrent comme représentant l'état courant du registre. Ils minent donc tous sur le même bloc parent (ici, le bloc numéro 3). Mais une telle situation, idéale, n'est pas garantie.

Une première raison est liée aux propriétés physiques du réseau : les blocs gagnants mettent du temps à le parcourir. Il est donc possible que deux mineurs, relativement éloignés l'un de l'autre, valident leur bloc à des moments rapprochés, avant d'avoir reçu le bloc gagnant de l'autre. À ce stade, deux visions de la *blockchain* cohabitent au sein du réseau, les autres mineurs adoptant la vision du mineur gagnant le plus proche, comme illustré en haut du schéma 2.

Pour retrouver un consensus, les mineurs sont censés suivre une règle de sélection du bloc parent sur lequel miner, règle qui consiste à toujours miner au bout de la chaîne la plus longue connue d'eux. Ainsi, le dissensus évoqué plus haut disparaîtra naturellement lorsqu'un mineur validera et diffusera un nouveau bloc (par exemple, le Bloc 3', en bas du schéma 2), créant une chaîne plus longue d'un bloc que celles des autres mineurs, et imposant ainsi très rapidement un consensus correspondant à sa vision du registre. Une « fourche » est bien apparue, mais elle était très courte et n'a persisté qu'un court moment.

Schéma 1 : Une *blockchain*, et des mineurs (« m ») travaillant de concert pour la prolonger

1. Biais B., Bisière C., Bouvard M., Casamatta C. 2016, *The blockchain folk theorem*, working paper.

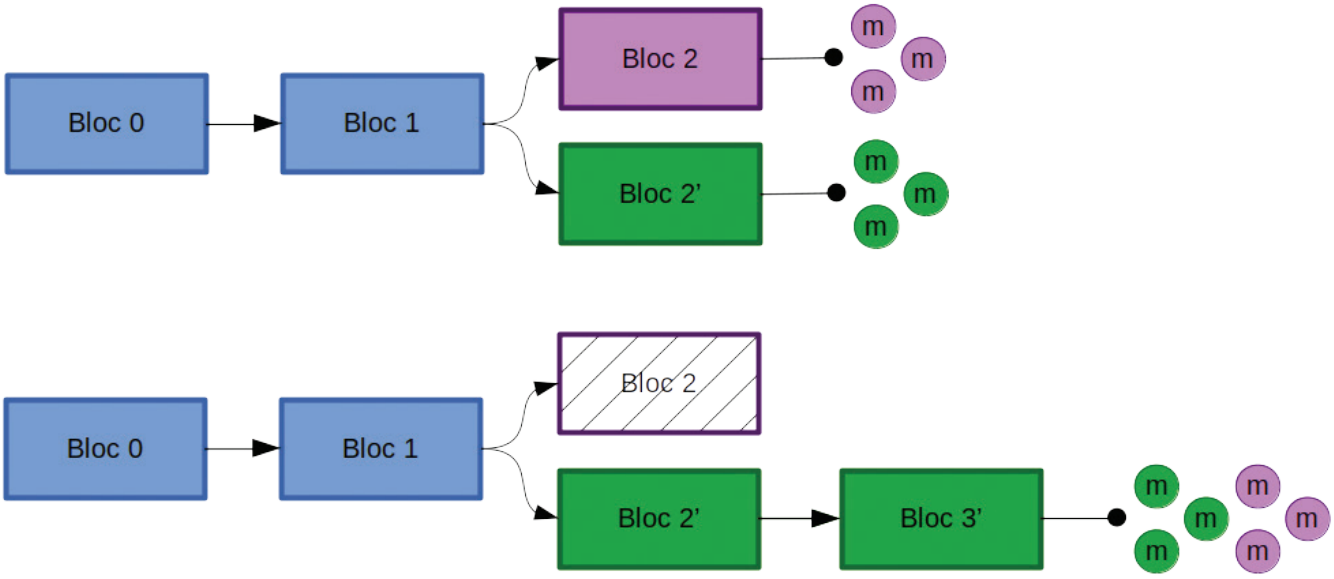

Schéma 2 : Résolution d'un dissensus par la règle de la chaîne la plus longue.
En haut : à cause des délais dans le réseau, les mineurs se retrouvent à miner sur deux branches différentes.
En bas : le groupe qui trouve le bloc suivant (ici 3') impose sa branche comme nouveau consensus. Le Bloc 2 est abandonné.

Une autre raison, souvent soulignée, est celle d'un comportement malveillant. Un participant qui souhaiterait provoquer l'annulation d'une transaction présente dans un bloc déjà miné — dans le but de récupérer des unités de monnaie virtuelle déjà dépensées — devra miner un bloc à partir d'un bloc parent situé avant le bloc contenant cette transaction, et tenter de créer à partir de là une chaîne concurrente plus longue que la chaîne actuelle, afin que les autres mineurs abandonnent spontanément la portion de la chaîne contenant la transaction. Cependant, les chances de réussite d'un mineur luttant contre tous (car seul sur sa fourche) pour résoudre le problème numérique difficile, sont minces, à moins que ce mineur possède une puissance de calcul considérable — impossible à atteindre dans les réseaux *blockchains* matures. En d'autres termes, réécrire l'histoire des transactions dans la *blockchain* est excessivement coûteux.

Une *blockchain* est un jeu de coordination

Tout semble indiquer que la règle de la chaîne la plus longue, associée à la difficulté du problème numérique à résoudre, élimine toute possibilité d'apparition de fourches « sérieuses » (c'est-à-dire longues et éventuellement persistantes), garantissant ainsi la stabilité de la *blockchain*.

Notre travail consiste à évaluer cette conjecture, du point de vue théorique, à l'aide de la théorie des jeux. Pour ce faire, nous modélisons une *blockchain* comme un jeu dans lequel des mineurs rationnels choisissent stratégiquement le bloc parent sur lequel miner. Stratégique, un mineur prend en compte ce qu'il anticipe des choix des autres pour prendre sa propre décision. La règle de la chaîne la plus longue est une stratégie possible, mais ce n'est pas la seule. Pour simplifier, nous supposons que les mineurs observent instantanément toutes les transactions et tous les blocs, et que leurs gains ne sont constitués que des récompenses en monnaie virtuelle attachées aux blocs qu'ils ont minés. Éliminant ainsi les frictions à l'origine des instabilités évoquées plus haut, nos résultats sur la possibilité de fourches en seront renforcés.

Dans ce cadre, comment se comporte un mineur ? On voit qu'il est soumis à deux forces. En premier lieu, les récompenses qu'il a éventuellement obtenues en minant des blocs dans une chaîne donnée vont le rendre réticent à abandonner cette chaîne pour aller miner sur une éventuelle fourche en amont. En effet, si cette fourche devenait un nouveau consensus, ses récompenses, associées à des blocs maintenant exclus du registre, ne vaudraient plus rien. Cette première force a tendance à stabiliser toute situation, qu'il s'agisse d'une situation avec fourche ou sans fourche. En second lieu, un mineur préfère *a priori* miner là où il anticipe que les autres mineurs vont miner. En effet, miner seul sur une branche, quand tous les autres travaillent à prolonger une autre branche, revient à utiliser sa puissance de calcul en pure perte, puisque les récompenses éventuellement obtenues ne vaudront rien. Cette seconde force peut favoriser l'apparition de fourches, suivant les anticipations des mineurs.

Il est important de noter que, pour un mineur, le fait d'avoir commencé à miner un bloc n'est pas une raison en soi de continuer à le miner. La nature du problème numérique à résoudre fait qu'un essai de solution a toujours la même probabilité de succès, indépendamment du nombre de tentatives déjà effectuées sur ce bloc. Cette probabilité ne dépend que de la capacité de calcul du mineur et de la difficulté du problème à résoudre, fixée par le protocole. La probabilité ne dépendant ni du bloc miné ni des blocs que les autres mineurs ont choisi de miner, l'activité de minage n'est pas une course entre mineurs, dans laquelle le premier à trouver la solution au problème gagnerait une récompense au détriment des autres.

Ainsi, le jeu entre les mineurs apparaît comme un jeu de coordination, dans lequel l'anticipation du comportement des autres joue un rôle essentiel.

Consensus et dissensus

Dans ce jeu stratégique, une configuration de la *blockchain* peut être qualifiée d'équilibre quand les stratégies des mineurs sont cohérentes entre elles, au sens où aucun mineur, si on lui révélait les choix effectués par les autres, ne souhaiterait modifier son propre choix. Ainsi, à l'équilibre, aucun mineur n'a intérêt à changer de stratégie, c'est-à-dire à changer le bloc parent sur lequel il mine.

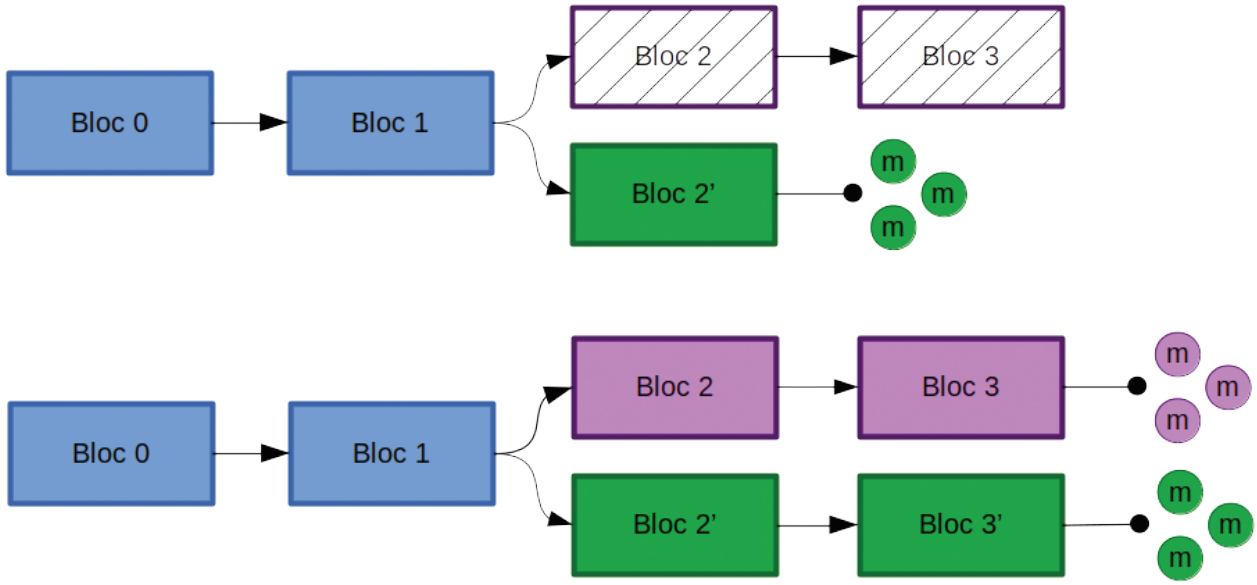

Schéma 3 : Deux configurations d'équilibre, sous-optimales

Un premier résultat est rassurant : parce qu'un mineur qui anticipe que les autres mineurs appliquent la règle de la chaîne la plus longue a intérêt à la suivre également, une chaîne unique, sans fourche, est une configuration d'équilibre. De plus, cette configuration « consensuelle » est robuste, face à de petits écarts anticipés quant à l'application de la règle de la chaîne la plus longue.

Cependant, comme souvent dans les jeux de coordination, d'autres équilibres sont possibles. Comme illustré en haut du schéma 3, on peut avoir à l'équilibre une configuration dans laquelle une portion de la chaîne est collectivement abandonnée au profit d'une branche créée en amont. C'est une configuration sous-optimale, car les récompenses attachées aux blocs abandonnés sont définitivement perdues. Un autre résultat du modèle, plus négatif encore, est illustré en bas du schéma 3. Il est possible d'obtenir à l'équilibre une fourche persistante, les mineurs se répartissant sur les deux branches, et continuant à y miner. Le dissensus est ici complet et la valeur sociale de la *blockchain* est sérieusement entamée.

En somme, nous montrons que le consensus peut être atteint au sein de la *blockchain*, mais qu'il n'est pas possible d'exclure les situations dans lesquelles des fourches temporaires ou persistantes apparaissent, et ce même en l'absence de mineurs malveillants.

De telles situations ont bien été observées dans les deux plus grands réseaux à base de *blockchain*, Bitcoin et Ethereum.

contact&info
▶ Christophe Bisière, CRM
bisiere@univ-tlse1.fr