L'AGEFIHEBDO
Pays : France
Périodicité : Hebdomadaire

Date : 26 JAN/01 FEV 17
Page de l'article : p.18
Journaliste : Bruno Biais

ÉCONOMIE & FINANCE

L'ANALYSE DE... Bruno Biais,
TOULOUSE SCHOOL OF ECONOMICS (CNRS/CRM, CHAIRE FBF IDEI SUR LA BANQUE D'INVESTISSEMENT ET LES MARCHÉS FINANCIERS)

Risques et promesses de la Blockchain

Pour établir les droits de propriété et permettre les échanges, on a besoin d'un registre fiable des détentions et transactions. Ainsi, une transaction immobilière est validée et enregistrée par un notaire. La *Blockchain* est un mécanisme décentralisé d'enregistrement des transactions dans un registre sur internet, développé pour la monnaie « digitale », *bitcoin*, mais dont le principe s'étend à d'autres actifs. Comment fonctionne-t-il et quels risques peut-il présenter ?

Les participants au réseau *Blockchain* observent le registre des détentions de *bitcoins*. Lorsqu'une transaction a lieu (par exemple A verse 10 *bitcoins* à B pour lui acheter sa voiture), tous les participants au réseau reçoivent un message les en informant. Après avoir reçu un certain nombre de messages, un participant peut les regrouper en un bloc et décider de miner ce bloc. Le bloc contient, pour chaque transaction, l'information spécifiant qui a versé des *bitcoins* et à qui. Le « mineur » rattache le bloc sur lequel il travaille au bloc précédent. Ce faisant, il doit vérifier que l'état antérieur du registre indique bien que les personnes qui proposent de verser des *bitcoins* les possèdent effectivement. Ce travail de validation ne demande que relativement peu de capacité de calcul, mais pour ajouter un bloc à la chaîne, le « mineur » doit aussi effectuer un autre travail, demandant une grande capacité de calcul : résoudre un problème cryptographique très difficile, mais dont il est très facile de vérifier la solution. Une fois qu'il a résolu ce problème, le « mineur » ajoute son bloc à la chaîne. Si les autres « mineurs » y enchaînent leurs propres blocs ultérieurs, se développe une chaîne faisant l'objet d'un consensus distribué.

L'apparition de fourches pourrait contrevenir à la formation d'un consensus. Supposons que les blocs n, n+1 et n+2 ont été minés et attachés à la chaîne. Une fourche apparaît si des « mineurs » se rattachent non au dernier bloc, n+2, mais à un bloc antérieur, par exemple n. Si cette fourche devient majoritaire, alors les transactions enregistrées dans les blocs n+1 et n+2 sont remises en cause. Cela pourrait correspondre à une stratégie de « *double spending* » : A verse 10 *bitcoins* à B pour lui acheter sa voiture. Cette transaction est enregistrée dans le bloc n+1. Par la suite, A mine à partir du bloc n, s'efforçant de créer une fourche. S'il réussit, les blocs n+1 et n+2 sont ignorés et le paiement reçu par B effacé.


DR

Cette technologie n'est pas exempte de fragilités

C'est pour éviter ce problème que la *Blockchain* freine la capacité des « mineurs » à rajouter des blocs à la chaîne. Pour amener la majorité des participants à ignorer les blocs n+1 et n+2, le manipulateur doit résoudre ses blocs plus rapidement que les autres, faisant ainsi rapidement croître sa fourche, qui, devenue plus longue que la chaîne originelle, pourrait la remplacer. Cette croissance rapide est empêchée par la difficulté du problème cryptographique qui doit être résolu pour ajouter chaque bloc.

Cette discussion montre que, pour évaluer la fiabilité de la *Blockchain*, il faut analyser les stratégies des « mineurs ». C'est ce que nous faisons, à l'aide des outils de la théorie des jeux, dans le cadre de la chaire FBF IDEI à Toulouse. Nos travaux montrent l'existence d'une autre source de fragilité : l'interaction stratégique entre « mineurs » est un jeu de coordination. Il est attractif pour un « mineur » de travailler sur une branche dans la *Blockchain* s'il anticipe que les autres « mineurs » se concentrent sur la même branche. Dans ce contexte, comme c'est souvent le cas dans les jeux de coordination, il existe plusieurs équilibres. La difficulté à se coordonner sur un équilibre peut être source d'instabilité. De plus, nous montrons que des fourches persistantes peuvent apparaître à l'équilibre (comme c'est le cas en pratique avec les deux branches de la chaîne Ethereum : ETH et ETC).

Si la technologie *Blockchain* est pleine de promesses, elle n'est pas exempte de fragilités. Chercheurs, régulateurs et praticiens doivent mener à son sujet une réflexion critique approfondie, sur la base de laquelle pourrait se développer un système de consensus distribué fiable et sûr. ■