Laurent Tedesco
CEO d'Humbrain

La blockchain : révolution ou fausse bonne idée ?

Au vu de l'engouement qu'a généré cette technologie, du nombre d'articles dithyrambiques publiés sur le sujet, des start-up aux millions levés qu'elle a fait naître, poser cette question est une hérésie. Pourtant, en creusant un peu, quelques interrogations émergent sur sa pertinence et son devenir.

Commençons par revenir sur la définition du procédé visé. On peut le résumer à un ensemble de mécanismes logiciels permettant la traçabilité sécurisée de transactions entre pairs. Dans l'esprit, il vise à se passer du tiers de confiance auquel on fait habituellement appel dans des relations contractuelles bilatérales. A la fois une logique et une infrastructure, la technologie *« BlockChain »* est le fruit de plusieurs procédés :

- L'internet d'abord, et son protocole sous-jacent, le TCP/IP. Sans lui, pas de réseau structurant, mondial et à coût quasi-nul.
- Les technologies en peer to peer, très en vogue la décennie précédente (réseau eDonkey, Bittorrent…), qui ont banalisé le stockage distribué entre de multiples nœuds distants.
- Les procédés cryptographiques, notamment le SHA issu de la NSA, qui permettent de garantir confidentialité et intégrité aux données véhiculées.

En résumé, une blockchain est un réseau d'ordinateurs – les nœuds – agissant selon un protocole défini en vue de certifier et stocker les paquets qui lui sont soumis.

On le rappelle souvent, le Bitcoin, est la première manifestation d'une blockchain.

En pratique, cette cryptomonnaie correspond à la récompense qu'obtiennent les nœuds qui prennent en charge les traitements de validation des blocs.
Ces opérations, surnommées *« minage »*, impliquent de lourds calculs. Il s'agit en effet de s'assurer de la consistance et de l'unicité d'un nouveau bloc dans la chaine de blocs existants. Le minage, et plus largement ces mécanismes délégués de validation et stockage des données, sont les premiers griefs portés contre cette technologie. L'une des critiques les plus courantes porte sur le temps de calcul. Dans le cas de Bitcoin, il faut compter une dizaine de minutes le temps nécessaire à l'intégration d'un nouveau bloc. Conséquence : selon un récent rapport, ce réseau serait à peine capable d'opérer 80 transactions par minute quand les réseaux de paiement Visa et Mastercard en traiteraient 100000. Une autre critique porte sur la consommation d'énergie. Le site Bitcoin.fr chiffrait en mars 2019 la consommation du réseau Bitcoin à une quarantaine de milliards de kWh par an, soit la production de 5 à 6 centrales nucléaires. Ce n'est pas anodin.

IDÉALISATION DES MODÈLES SOUS-JACENTS

En prenant de la hauteur, on comprend aussi que cette technologie s'est forgée dans un monde idéalisé. Par exemple, on part du principe que le réseau support est invisible, comme un substrat devenu naturel et

évidant et surtout gratuit. Cette situation est-elle pérenne ? Je ne crois pas : qu'en sera-t-il lorsque, voulant récupérer leur part du gâteau, les opérateurs réseaux demanderont un droit de passage pour aller faire miner vos transactions à l'autre bout de la planète ? le modèle économique interne et autogéré serait alors mis à mal.

Le deuxième idéal chahuté est la belle ambition d'une mutualisation équitable entre pairs de la prise en charge des transactions. C'est en grande partie la raison d'être du procédé : ainsi, inspirés par les services peer-to-peer historiques, les concepteurs imaginaient naïvement que plein de petits ordinateurs répartis ici ou là allaient se répartir la charge de manière homogène et quasi démocratique, comme si chaque humain sur terre allait stocker chez lui une ou quelques pages de ce grand registre que constituerait la blockchain. C'est idée semble hélas en voie de décomposition. La surenchère aux calculs pousse en effet à la concentration des moyens et le minage est peu à peu vampirisé par quelques gros acteurs, dont une bonne partie chinoise. Quand 5 ou 6 gros acteurs accaparerons la majeure partie des flux, on sera loin de l'idéal originel…

UNE SOLIDITÉ UN PEU SURJOUÉE

Enfin, le procédé de blockchain est largement vendu comme une technologie sûre et solide. Une idée aujourd'hui malmenée. Cela reste un procédé logiciel, avec un algorithme qui peut être challengé comme n'importe quel autre et notre monde ne manque pas de petits génies en capacité de relever le pari, l'histoire l'a déjà prouvé. Le récent cas de Ethereum est signifiant : des hackers ont réussi à *« braquer »* - ne me demandez pas comment - le réseau en s'appropriant une partie des Ether en circulation (15% dit-on). Un débat a suivi dans la communauté sur le devenir de cette partie volée de la masse monétaire globale existante, partie bien évidemment pas stockée dans un coffre-fort caché sous une montagne secrète mais bien noyée au milieu de toutes les transactions. L'option de les décréter *« sans valeur »* a été discutée, sans grande conviction.
Il faut dire qu'on touche là un caractère intangible de la blockchain : ce qui est inscrit est forcément vrai, le faux ne peut y exister.

Ou alors je n'ai rien compris, c'est une option ;-).