

Une brève histoire de la blockchain



A lire ce qui s'écrit depuis quelques semaines, on a le sentiment que le bitcoin peut bien être enterré (sous une bonne couche de suspicion ou d'oubli, qu'importe) mais que la blockchain est la promesse concrète de la grande disruption universelle. Pas un jour sans que l'on apprenne que l'une de ces banques qui ferment les comptes au moindre soupçon d'implication d'un client dans l'industrie naissante du bitcoin n'a ouvert un incubateur pour réfléchir sur la blockchain, n'a recruté des développeurs pour en faire tourner une mélodieusement dans ses sous-sols, ou n'a conclu une alliance avec d'autres établissements pour opérer des règlements interbancaires sur une blockchain privée. Il n'est pas jusqu'aux banques centrales et jusqu'à la vieille dame de Threadneedle Street qui n'entrent dans le jeu. Et ce n'est pas tout : les diamantaires veulent la leur, tandis que les anarchistes envisagent de placer leur identité, leurs tweets ou leurs DNS dans quelque blockchain.

L'usage s'installe de dire « la » blockchain pour parler de celle, ouverte et publique, du bitcoin, et « une » blockchain pour toutes les autres, publiques comme celle d'Ethereum ou fermées comme celles que fomentent les banques.

Avant de reprendre l'antienne, comme quoi la Blockchain va bien au delà du Bitcoin, il importe de dire ce qu'elle est : une partie (seulement) du dispositif inventé par Satoshi Nakamoto en 2008. Dans les propositions qu'il fit pour créer un système de paiement sans banque, le tiers centralisateur est remplacé par un serveur horodaté et distribué en pair à pair. Ceci est la blockchain (en tant que technologie de stockage distribuée) et produit la blockchain (en tant que livre de compte ouvert et public où l'on peut lire l'enchaînement des transactions depuis l'origine). Cette nouveauté ne vint cependant pas seule mais agencée à d'autres inventions ou intuitions : sa tenue assurée en unités de compte (le bitcoin et ses unités divisionnaires), sa probité assurée par un système de preuves de travail qu'apportent ceux qui participent à l'enregistrement des écritures (mais il y a d'autres preuves concevables), sa sécurité assurée par le recours à une cryptographie (parmi d'autres possibles), son entretien assuré par le minage rétribuant en bitcoins le travail des certificateurs. Parler de la blockchain en mettant tout cela entre parenthèses trahit souvent une information superficielle et n'est pas fructueux.

La blockchain fait parler d'elle d'abord dans les activités bancaires ou interbancaires de transferts de toutes sortes. On suppose son effet sur le coût de ces activités (par son emploi) on craint son effet sur leur marge (par la concurrence). On y songe dans tous les services financiers autour des transactions de paiement, crowdfunding ou crowdlending et la liste s'allonge chaque matin.