



Pas de cryptomonnaies sans technologie blockchain

C'est avec le lancement du bitcoin en 2009 qu'un vaste public a pris connaissance de la technologie blockchain. Mais l'idée d'une cryptomonnaie qui s'impose hors de toute intervention étatique et sans se soumettre au diktat des banques centrales ou des banques commerciales serait inconcevable sans la technologie blockchain sur laquelle elle s'appuie.

La technologie blockchain repose, pour son utilisation pratique, sur la croissance exponentielle de la puissance de calcul des ordinateurs, également appelée loi de Moore. Celle-ci stipule que la complexité des circuits intégrés ayant des coûts de composants minimes double tous les 12 à 24 mois, tout comme la disponibilité et la reproductibilité croissantes des informations sous forme numérique par le biais d'Internet.

Il existe déjà depuis des décennies des bases de données centralisées avec des droits d'accès communs. Wikipédia en est l'exemple le plus connu. En parallèle, les bases de données distribuées enregistrent toutes les entrées de manière décentralisée sur des ordinateurs différents – et c'est précisément sur ce principe que repose l'infrastructure bitcoin. Toutes les transactions financières y sont gérées conjointement par les participants par le biais d'un livre de comptes distribué, de manière sûre et sans possibilité de le modifier. Pour des raisons de performance, les inscriptions correspondantes se font de façon groupée en blocs, d'où la désignation de chaîne de blocs ou blockchain.

La vague du bitcoin a fait d'innombrables émules. Il existe désormais de nombreuses cryptomonnaies, dont le point commun est de s'appuyer sur une blockchain. Les critiques estiment néanmoins que les cryptomonnaies présentent quelques faiblesses fondamentales, par exemple leur modularité limitée, la forte volatilité des prix ou l'absence de réglementations existantes. Une autre déficience tient à la

La vague du bitcoin a fait

d'innombrables émules

faible capacité de traitement des transactions. Alors que les émetteurs de cartes de crédit établis traitent un volume de quelque 2000 transactions par seconde, le protocole bitcoin actuel n'en permet que sept et n'est donc pas compatible pour l'instant avec des opérations de masse.

La croissance des volumes monétaires en bitcoins est programmée par le logiciel et absolument limitée. Par comparaison, les banques commerciales peuvent, en octroyant des crédits dans le cadre des prescriptions réglementaires, créer de l'argent scriptural de manière pratiquement illimitée. C'est pourquoi le bitcoin n'acquerra sans doute pas de poids économique vital dans un avenir proche. En outre, la structure

d'incitation pour le minage de bitcoins entraîne une consommation d'énergie absurde en raison de la puissance informatique requise pour résoudre les énigmes cryptographiques. Le fait qu'un seul mineur à la fois se voie attribuer des bitcoins pour avoir réussi à résoudre une énigme cryptographique

entraîne en fin de compte des investissements excessifs dans la capacité de calcul et donc une concentration croissante sur un nombre de plus en plus petit de pools de mineurs, composés en revanche de mineurs de plus en plus nombreux. Ceux-ci ont implanté de préférence leurs fermes de minage dans des régions ayant de faibles coûts d'électricité, par exemple en Chine ou en Russie. En dernière analyse, le bitcoin perd ainsi son statut de monnaie décentralisée.

Bien que les bitcoins ne possèdent aucune contre-valeur réelle, ou peut-être justement à cause de cela, le prix du marché d'un bitcoin a bondi à 16500 dollars. L'évolution des prix est extrêmement volatile, ce qui donne à penser que la plupart des participants négocient les bitcoins à des fins spéculatives. En outre, les paiements en bitcoins se font par principe de



manière anonyme, rendant ainsi difficile l'application de la loi sur le blanchiment d'argent. De même, les critiques mettent régulièrement le bitcoin en rapport avec des opérations illégales. Enfin, certains soupçonnent les bitcoins d'être utilisés dans certains pays pour contourner les contrôles des mouvements de capitaux.

Depuis 2015, un consortium bancaire placé sous la houlette d'UBS élabore une alternative valable au bitcoin, appelée Utility Settlement Coin (USC) – mais l'USC restera réservé à un petit groupe de grandes banques. Le but de l'USC est de réaliser les transactions interbancaires directement et sans passer par les banques centrales. Cela vise à économiser des coûts et à accroître l'efficacité. L'USC est couplé à une monnaie étatique et, contrairement au bitcoin, possède une contre-valeur immédiate et stable en unités monétaires de la banque centrale. Les transactions sont à leur tour consignées sur une blockchain, mais, contrairement au bitcoin, sont légalisées par des notaires de confiance utilisant des signatures numériques.

Malgré les Cassandre et leurs prédictions alarmistes, la technologie blockchain va révolutionner l'industrie financière dès lors qu'un cadre juridique contraignant sera créé et mis en œuvre. Dans cette mesure, le développement du bitcoin est un jalon important dans la numérisation continue, qui ne pourra plus être stoppée. ■

DAMIR FILIPOVIĆ PROFESSEUR DE FINANCE AU SWISS FINANCE INSTITUTE ET TITULAIRE DE LA CHAIRE SWISSQUOTE DE FINANCE QUANTITATIVE À L'EPFL



ALEXANDER LIPTON FONDATEUR ET CEO DE STRONGHOLD LABS, ACTUELLEMENT VISITING PROFESSOR À L'EPFL

