Bitcoin, un protocole ouvert

PAR NICOLAS HOUY
chargé de recherche au CNRS
ET
FRANÇOIS LE GRAND
professeur de finance à l'EMLyon business school

Un nouveau langage qui a encore besoin d'une bonne grammaire.

S'IL A beaucoup fait parler de lui ces derniers mois, le bitcoin est encore mal connu. Première des cryptomonnaies, il reste, à ce jour, la plus importante d'entre elles. Inventé en 2008, il fonctionne sans interruption depuis le début de l'année 2009.

Qu'est-ce que le bitcoin exactement ? C'est un protocole, c'est-à-dire un ensemble de règles et de normes qui permettent à des ordinateurs – et donc à ceux qui les contrôlent – de communiquer entre eux. Plus qu'une monnaie, c'est un langage. La fonction de ce langage est de garantir des droits de propriété exclusifs et cessibles. Ce langage doit aussi respecter une contrainte d'absence de confiance *a priori*, ce qui implique que les droits de propriété ne peuvent être garantis par une entité de référence. La légitimité ou l'utilité de relever un tel défi peuvent évidemment être débattues. Toutefois, il faut reconnaître que, dans un monde numérique, y répondre avec succès est une réelle prouesse technique. En effet, comment faire pour qu'un individu puisse détenir une unité de compte, qui n'est autre qu'une succession dématérialisée de 0 et de 1, *a priori* facilement duplicable ? Comment ensuite lui permettre de céder cette unité de compte à une autre personne et, ce faisant, d'en transférer la propriété ?

Pour l'euro, des objets physiques plus ou moins infalsifiables, comme les pièces, les billets ou les titres au porteur, peuvent être utilisés. Dans leur version dématérialisée, les échanges en euros reposent sur la confiance que les utilisateurs placent dans les banques commerciales et les systèmes de paiement, comme Mastercard ou Visa. Transposer cela dans un réseau informatique au sein duquel toute confiance en une entité tierce est, par principe, interdite, est une véritable gageure.

PLUS QU'UNE MONNAIE, UN LANGAGE. Le bitcoin est une réponse à ce défi qui ne connaît pas d'équivalent historique. Aussi pose-t-il des questions inédites dont la portée n'est pas toujours clairement comprise. C'est pour cette raison que les développeurs de l'écosystème ont toujours présenté le bitcoin comme une expérience, informatique certes, mais également sociale. Ainsi, la gouvernance du bitcoin est singulière. Un aspect fondamental et, probablement assez mal compris, est que le bitcoin est un protocole ouvert : parce que le bitcoin est un langage ouvert, les règles qu'il énonce sont totalement publiques. Si le bitcoin permet de garantir des droits de propriété sur des unités de compte et évite ainsi leur multiplication ou leur copie, le protocole lui-même

"Avec quelques compétences informatiques, **quiconque est en mesure de créer une cryptomonnaie à son propre nom.**"

peut être dupliqué à l'infini pour un coût minime. Le nouveau protocole ainsi dupliqué ne sera plus le bitcoin, mais une autre cryptomonnaie dont les unités de compte ne seront pas reconnues par celui-ci. Cette ouverture n'est donc pas une contradiction interne du protocole. Avec quelques compétences informatiques et un peu de temps, quiconque est en mesure de créer une cryptomonnaie à son propre nom. Il existe d'ailleurs des milliers de cryptomonnaies. Certaines sont de simples clones du bitcoin, voire de véritables arnaques. D'autres sont créées dans le but d'améliorer le langage ou de répondre à un usage spécifique (micro-paiement, paiement entre objets connectés, développement d'organisations autonomes décentralisées...). Ce foisonnement et cette ouverture sont des conséquences directes du principe d'absence de confiance du bitcoin.

A contrario, des protocoles fermés existent. Skype, par exemple, permet d'échanger des données sous forme de son et d'image en utilisant un protocole protégé par le secret. La fermeture du protocole impose d'avoir confiance en l'entreprise qui l'exécute. Cette confiance *a priori* n'est pas permise par le bitcoin qui est un protocole ouvert. Cette ouverture s'accompagne de la possibilité d'être copié, mais aussi amélioré par chacun.

Cette caractéristique est souvent vue par le grand public, à tort, comme un signe du manque d'organisation et de maturité de la communauté du bitcoin. C'est, en effet, une différence de taille avec les institutions qui gèrent la monnaie fiduciaire, pour qui l'exclusivité est synonyme de garantie de confiance. Avec le bitcoin, il n'est pas question d'un monopole d'émission. Au contraire, son ouverture offre des environnements de test pour de nouvelles idées et favorise aussi la concurrence entre les cryptomonnaies. Ces deux aspects sont jugés capitaux par la communauté du bitcoin. Depuis sa création, le bitcoin a beaucoup évolué et va continuer d'évoluer. Néanmoins, chaque évolution comporte des risques, d'ordre technique, par exemple. Tester les évolutions avant leur mise en œuvre est d'autant plus important que les enjeux sont élevés. À l'heure où cet article est publié, environ 120 milliards d'euros sont placés en bitcoins. L'ouverture du bitcoin permet de réaliser ces tests très facilement. Chaque idée peut être testée en conditions quasi réelles et cela permet à la communauté de juger de sa pertinence. Si la proposition fait consensus, elle pourra être intégrée et déployée dans le protocole. En l'absence de consensus, plusieurs solutions sont possibles. Outre l'abandon pur et simple, l'idée peut être développée à l'extérieur du protocole, comme une couche complémentaire que les utilisateurs sont libres d'adopter. Une autre option, plus radicale, est de créer une copie du bitcoin prenant en compte l'idée et de laisser les utilisateurs choisir. C'est ce que l'on appelle un *fork*. Le bitcoin en a connu trois principaux qui ont respectivement donné naissance à litecoin, bitcoinCash et bitcoinGold. Cette concurrence d'autres protocoles n'est pas seulement une source de chaos, elle constitue une incitation à l'excellence et à l'amélioration continue. •