CRYPTOMONNAIES

Bitcoin : l'utopie libertaire, c'est du baratin

Se libérer de la tutelle de l'Etat et des banques, reprendre le contrôle de la monnaie : le projet libertaire des partisans des « cryptos » a l'attrait des choses simples. Trop simples ?

DOMINIQUE BERNS

Les partisans du bitcoin n'en démordent pas : si les cryptomonnaies ont une vertu, c'est d'abord celle « d'accroître le pouvoir de l'individu par rapport au gouvernement », comme le répétait récemment Elon Musk, le célèbre patron de Tesla et de Space X, dont les petites phrases tantôt font grimper le cours du bitcoin, tantôt le font chuter.

Ses défauts – une extrême volatilité qui le rend fonctionnellement inutilisable comme moyen de paiement ; et une production, le « minage » comme on dit en référence à l'or, horriblement énergivore, qui en fait un scandale environnemental – ne seraient que des maladies de jeunesse. Supposons-le.

Le bitcoin vaudrait alors par la possibilité qu'il offre de se libérer de la tutelle de l'Etat et des intermédiaires financiers ; et, plus largement, de reprendre le contrôle de la monnaie. Et c'est, selon eux, ce qui explique l'attrait de la plus célèbre des « cryptos », dont le cours, en hausse depuis la mi-juillet, a dépassé les 50.000 dollars.

Se disant souvent libertariens ou anarcho-capitalistes, les partisans des cryptos imaginent ainsi le développement d'un système monétaire décentralisé, où aucune autorité ne contrôlerait l'évolution de la masse monétaire (et ne pourrait donc la manipuler, expliquent-ils), où le recours à des intermédiaires ne serait plus nécessaire, et où les transactions seraient anonymes.

1

Décentralisé et anonyme : sans belle-mère !

De fait, grâce à la technologie du blockchain, deux personnes privées peuvent échanger directement des bitcoins, sans recourir à un tiers, l'intermédiaire financier, auprès duquel il est obligatoire de s'identifier et qui est généralement soumis à la supervision des autorités publiques.

A l'inverse, les moyens de paiement électroniques courants, carte de débit ou de crédit, Paypal ou appli bancaire sur votre smartphone, ne sont pas anonymes – et ils ne peuvent pas l'être.

Lors du paiement d'un achat en magasin avec une carte – pour prendre l'exemple le plus banal –, la banque doit pouvoir vérifier que le compte du client est suffisamment garni avant d'envoyer la réponse « transaction acceptée », qui indique au commerçant que le paiement sera effectué. Et c'est pourquoi il laisse le client emporter la marchandise, sans vérifier que l'agent est déjà arrivé sur son compte.

Pour les partisans du bitcoin, l'anonymat serait la première bonne raison de privilégier la cryptomonnaie. L'argument, souvent, fait mouche. Or, il repose sur une confusion entre anonymat et confidentialité.

Ce que désirent avant tout M. et Mme Tout-le-Monde, c'est le respect de leur vie privée. Autrement dit : la confidentialité – l'assurance que leur intermédiaire financier ne divulgue pas, sur la place publique ou à des tiers, l'historique de leur compte et des transactions effectuées ; que ces données ne sont pas accessibles à tous les employés de leur banque.

Mais ils souhaitent également pouvoir disposer, au besoin, d'une preuve de paiement – typiquement, l'extrait de compte indiquant que tel jour, à telle heure, tel montant a été transféré de leur compte à tel autre compte, celui de leur fournisseur d'eau ou d'électricité, ou de l'entreprise qui a rénové leur salle de bains.

Certes, on peut vouloir effectuer certains paiements de manière anonyme. Mais nul besoin d'une « crypto » ; il suffit de payer en liquide, c'est bien plus simple. Et c'est une bonne raison de refuser une société sans cash.

Quant aux achats en ligne, on voit mal l'intérêt d'un paiement anonyme, alors que, sur internet, on laisse toujours des traces, de ses déplacements, de ses achats – et, trop souvent sans y réfléchir, on accepte que de nombreuses données personnelles soient collectées.

2

Sécurité : retenir son code d'accès et bien plus encore

Les prosélytes des « cryptos » affirment souvent qu'un portefeuille en bitcoins est très sécurisé, voire… plus sécurisé que l'argent déposé dans une banque.

Cette deuxième affirmation, si elle peut surprendre, n'est pas *a priori* sans fondement. Seuls les billets sont émis et donc garantis par la Banque centrale – et c'est l'une des raisons qui pourrait justifier le lancement, par la Banque centrale européenne (BCE), d'un euro numérique.

En revanche, l'argent déposé sur un compte bancaire, bien qu'il soit libellé en euros, a été émis par la banque. Il s'agit d'une créance sur une institution financière privée, une promesse de paiement faite par la banque – autrement dit : de la « monnaie privée ». Et si la banque devait faire faillite, le titulaire du compte ne serait remboursé qu'à hauteur de la garantie des dépôts de 100.000 euros fournie par l'Etat.

Pour autant, personne ne refuse d'être payé en « monnaie bancaire ». Parce que c'est pratique. Mais aussi parce que les institutions financières, ces intermédiaires dont les partisans du bitcoin disent vouloir se débarrasser, déchargent leurs clients d'une préoccupation essentielle : celle d'assurer la sécurité de leurs comptes et de leurs transactions.

Les consignes de sécurité que doit appliquer l'utilisateur des moyens de paiement électroniques classiques sont élémentaires : garder secret son code PIN et l'encoder discrètement sur le terminal lors d'un paiement ou d'un retrait, prévenir Card Stop dès le constat de la perte ou de la disparition de la carte bancaire, utiliser un digipass pour réaliser les opérations bancaires en ligne… Rien de bien futé.

La vie n'est pas aussi facile pour le détenteur de cryptomonnaies. S'il perd son ou ses codes d'accès, il est marron. Surtout, il a intérêt à mettre en place des procédures de sécurité exigeantes, dont Bitcoin.org, un projet « open source » indépendant qui vise à soutenir le développement du bitcoin, dresse une longue liste. Notamment : chiffrer le portefeuille et les terminaux, smartphone et ordinateur ; effectuer régulièrement des sauvegardes ; signer les transactions hors ligne (en utilisant deux ordinateurs, dont l'un est déconnecté de tout réseau) ; stocker son portefeuille « à froid » (portefeuille hors-ligne), etc., etc.

Et penser déjà à rédiger son testament pour y inscrire les informations qui permettront à ses héritiers de récupérer le magot, ajoute encore bitcoin.org.

3

L'intermédiaire rentre par la fenêtre

Pour la plupart des gens, le choix est vite fait : laisser les intermédiaires financiers s'occuper de la sécurité. C'est d'ailleurs ce qui explique le succès des plateformes d'échange et de conservation de cryptomonnaies, notamment de Coinbase fondée en 2012 et qui a fait son entrée en Bourse à Wall Street à la mi-avril.

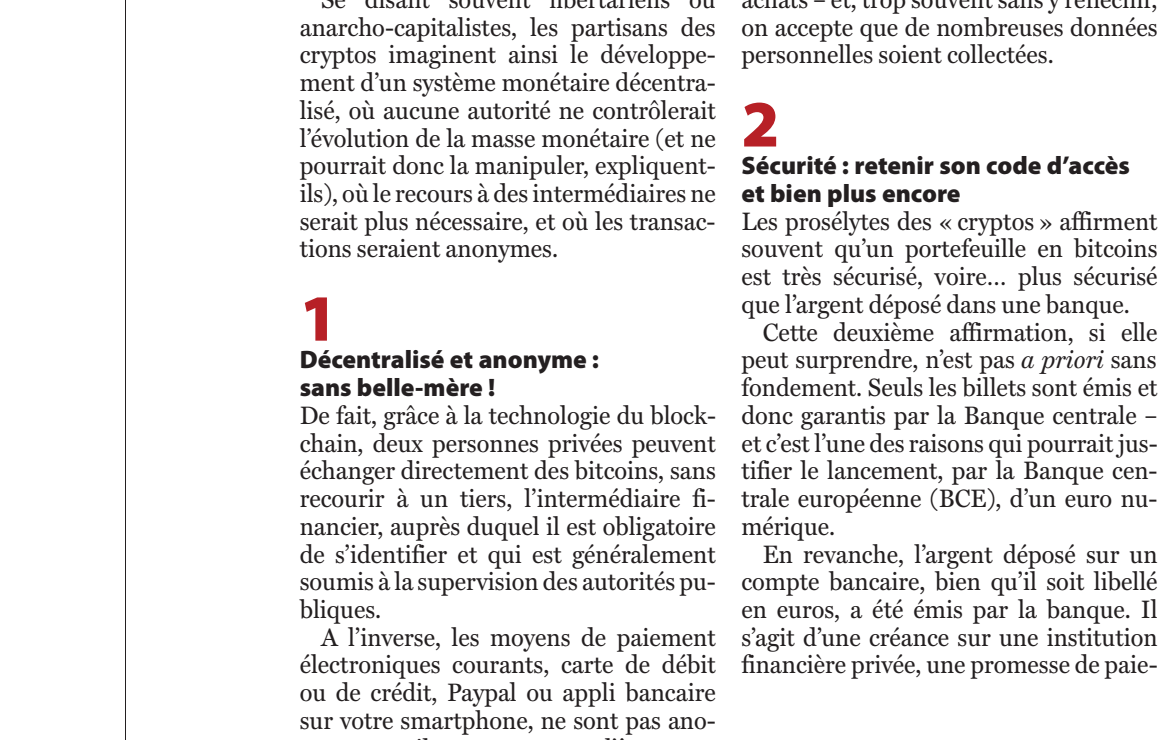
« Si vous allez voir ma mère et lui dites : "Voici ton compte, mais si tu égares le mot de passe, tout est perdu", ce n'est pas une bonne manière de commencer », expliquait ainsi l'un de ses fondateurs, Brian Armstrong, comme le rappelaient récemment nos confrères du *Monde*. Coinbase propose donc à ses clients de conserver leurs cryptodevises, en leur garantissant une double sécurité : le stockage « off line » et la possibilité de retrouver les codes de sécurité si, d'aventure, le client les oublie.

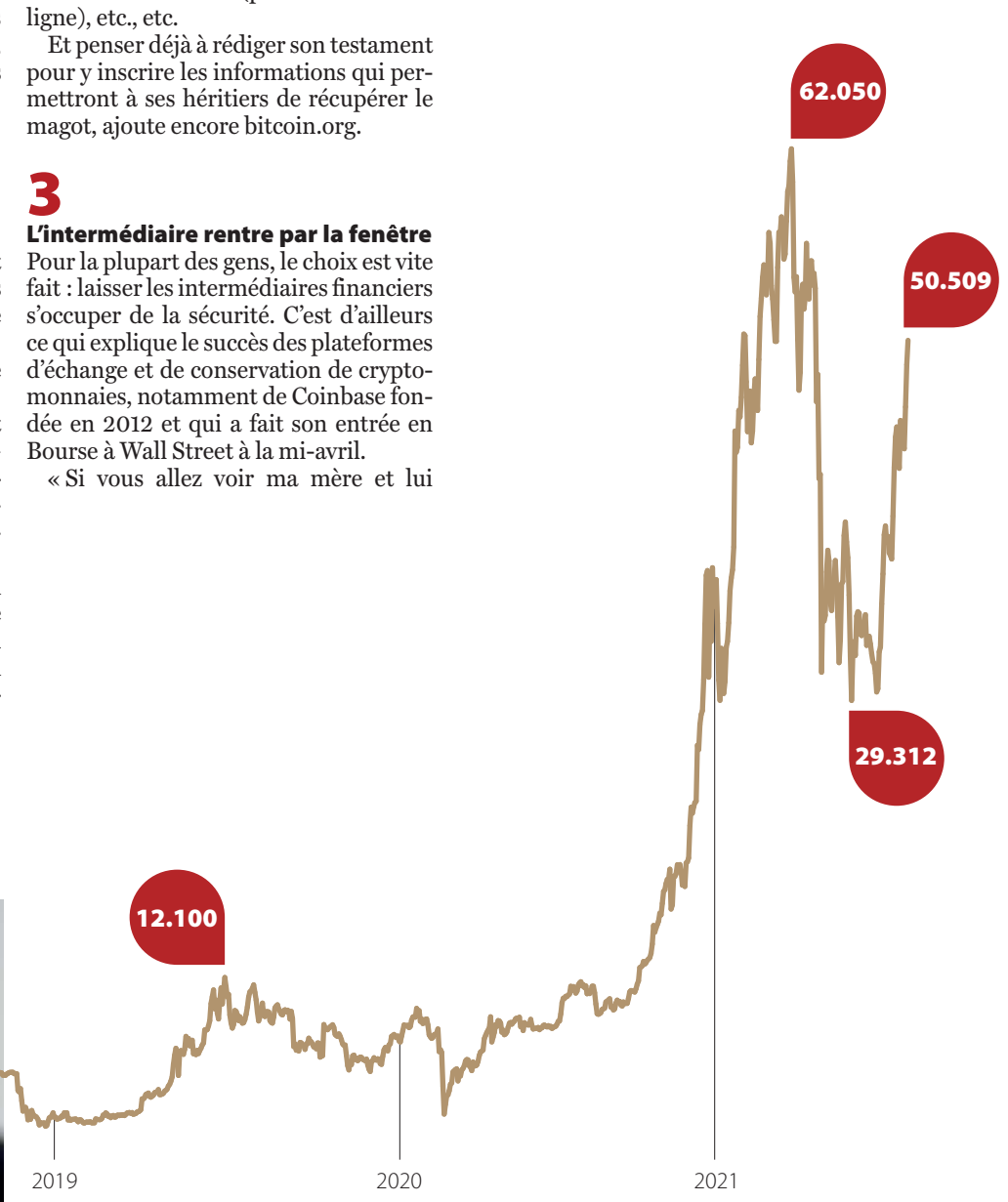
Mais voilà : l'intermédiaire, qu'on a voulu fait sortir par la porte, rentre par la fenêtre. Et s'il est également enregistré auprès des autorités de contrôle des marchés financiers – ce qui implique qu'il respecte tout un tas de règles –, l'Etat retrouve son rôle de belle-mère. Le serpent se mord la queue. Il ne reste plus rien du rêve libertaire.

Quant à l'idée que le monde irait beaucoup mieux si la monnaie n'était plus sous le contrôle de l'Etat – s'il n'y avait plus de Banque centrale, si les agents économiques avaient le choix entre différentes monnaies privées en concurrence les unes avec les autres –, elle relève d'une croyance en l'autorégulation des marchés régulièrement démentie par les crises.

S'il s'agit de reprendre le contrôle de la monnaie, il n'y a qu'un moyen : la prise de contrôle démocratique des Banques centrales.

En vogue dans la Silicon Valley, l'anarcho-capitalisme – cette doctrine selon laquelle une société capitaliste sans Etat serait à la fois économiquement efficace et moralement désirable – ou le libertarisme – qui prône un Etat minimal – reposent sur une vision simpliste de l'économie et de la société.





Le bitcoin en dollars

Pour les partisans du bitcoin, l'anonymat serait la première bonne raison de privilégier la cryptomonnaie. Mais c'est confondre anonymat et confidentialité. © REUTERS.