ADRIEN BICHET (2008) NICOLAS CLAUSSET (2008) ARNAUD SELLEM (2008)



MONNAIE ÉLECTRONIQUE : QUEL AVENIR POUR BITCOIN ?

Inconnu en août 2013, oublié en juin 2014 : est-ce là le triste sort de bitcoin auprès du grand public ? Très présente dans la presse un certain temps, cette monnaie numérique semble retomber dans l'indifférence médiatique après avoir vu son cours perdre plus de 40 % entre décembre et avril. Pourtant, bitcoin est loin d'être mort car les monnaies « numériques alternatives » révèlent un mouvement de remise en cause profonde des monnaies officielles. Retour sur ces quelques mois agités.

Bitcoin est une monnaie numérique, qui permet de réaliser des transactions *via* Internet, quasi immédiates et totalement irréversibles. Elle est née en décembre 2008, dans le tumulte de la crise financière. Et, depuis, son évolution est marquée par des crises successives. Fin 2013, le cours explosait de 100 dollars le 2 octobre à 1 147 dollars le 4 décembre, plus haut historique à ce jour, suscitant un fort intérêt notamment médiatique auquel une nouvelle chute mit un terme. Simultanément, plusieurs affaires ont ébranlé des acteurs clés, comme la fermeture de la place de marché historique, MtGox, en février 2014.

Si la spectaculaire hausse du cours explique en partie l'attention dont il a fait l'objet, son potentiel d'innovation est indéniable. Dans le cadre de notre formation au corps des Mines, nous avons donc voulu comprendre non seulement le rôle et le fonctionnement de bitcoin, mais surtout les controverses dont il est l'objet et ce qu'il nous apprend sur l'évolution de notre rapport aux monnaies.

« Ce ne sont plus les banques qui traitent les transactions »

UNE VALIDATION DÉCENTRALISÉE COMPENSÉE PAR LA CRÉATION MONÉTAIRE

La validation des transactions de manière décentralisée est l'innovation majeure de bitcoin : ce ne sont plus des institutions – les banques – mais des utilisateurs – dénommés les mineurs – qui traitent les flux de transactions en temps réel.

Figure 1 - Le cours de bitcoin, très variable, reflète notamment les événements qui jalonnent son parcours (CoinDesk Bitcoin Price Index, USD).

UN MODÈLE DÉCENTRALISÉ

Bitcoin est une monnaie numérique qui repose sur un protocole décentralisé : la validation des transactions ne fait appel à aucun tiers de confiance : elle est confiée à des ordinateurs ne se connaissant pas, répartis sur le réseau. Le code des logiciels est public *(open-source).* Les transactions se font en bitcoin (abrégé XBT, ou BTC). Chaque bitcoin est divisé en 10^8 satoshis, permettant ainsi des paiements de montants très faibles (au maximum de son cours 1 satoshi valait environ 10^{-5} USD).

Les transactions sont assimilables à des virements entre des comptes que les utilisateurs gèrent eux-mêmes, sans banque. Dans le protocole bitcoin, les comptes sont appelés adresses bitcoin et permettent de recevoir, stocker et envoyer de la monnaie. Ces adresses sont publiques et connues de tous. Une transaction est un message communiqué à tout le réseau et qui spécifie une adresse d'origine, une adresse de destination et un montant.

S'ASSURER DE L'IDENTITÉ D'UTILISATEURS ANONYMES

Un utilisateur dispose d'une clé privée connue de lui seul pour chacune de ses adresses. Lorsqu'il émet une transaction, il la signe, ce qui permet de vérifier l'identité de l'émetteur et l'intégrité de la transaction au moyen d'un procédé cryptographique. Chacun peut ensuite vérifier que la signature correspond bien à la clé publique et ainsi s'assurer que l'individu à l'origine de la transaction est bien le possesseur de l'adresse.

ÉVITER LA DOUBLE-DÉPENSE

Un des problèmes d'une monnaie numérique non centralisée est celui dit de la double-dépense : comment s'assurer qu'un bitcoin n'est bien dépensé qu'une seule fois et n'est pas la copie d'un autre déjà dépensé ? Bitcoin résout ce problème au moyen d'un livre faisant état de toutes les transactions de bitcoin depuis son origine. Ce livre est partagé par tous les nœuds du réseau, qui en ont chacun une copie. Les transactions sont regroupées par blocs de transactions (formant ainsi une chaîne de blocs, ou *blockchain*). Lorsqu'une transaction est émise sur le réseau, il est donc possible de vérifier quels sont les fonds disponibles sur une adresse en retrouvant dans le livre de compte tous les mouvements réalisés vers et depuis cette adresse. Si les fonds sont bien disponibles, la transaction est dite valide.

VALIDER LES TRANSACTIONS

Toutes les dix minutes en moyenne, un nouveau bloc de transactions est validé par le réseau et est inscrit dans la *blockchain.* La validation inclut, outre la vérification que les transactions sont valides, une preuve de calcul : un calcul arbitrairement compliqué mais facile à vérifier, qui permet de s'assurer qu'un utilisateur malveillant ne pourra pas valider de transactions frauduleuses. Le premier mineur (un utilisateur qui a accepté de mettre de la puissance de *calcul* au service du réseau) à finir ce calcul complexe gagne le droit d'inscrire ce nouveau bloc dans la *blockchain.*

Pour faire fonctionner le système, les mineurs mettent à sa disposition de la puissance de calcul. Or cela représente un coût pour ces derniers, dont le matériel, développé spécialement à cet effet et très rapidement obsolète (figure 2), peut valoir jusqu'à plusieurs milliers de dollars. La solution apportée par bitcoin consiste à rémunérer les mineurs, en plus d'une commission prélevée sur les transactions qu'ils valident, par de la création monétaire (de nouveaux bitcoins leur sont distribués).

Cette création monétaire, connue à l'avance, décroît avec le temps de sorte à faire converger la masse monétaire vers une limite arbitraire de 21 millions de bitcoins. Cette « politique monétaire », minimaliste par sa gestion rigide de l'offre de monnaie, ne manque pas d'interroger, tant sur ses conséquences économiques que sur les motivations qui ont conduit à l'adopter. Bien qu'il soit impossible de répondre avec certitude à ces questions, il est souvent avancé que bitcoin serait ainsi structurellement déflationniste. De plus, la prédictibilité de cette création monétaire est souvent présentée comme protection contre d'éventuelles dérives. En effet, certains croient y voir une application des idées de Milton Friedman qui, dans un entretien, s'était déclaré « favorable à remplacer la Fed par un ordinateur » pour gérer l'émission monétaire indépendamment des pressions politiques. Ces innovations sont mises en musique par un mécanisme dont le fonctionnement est détaillé dans l'encadré.

L'ÉCOSYSTÈME BITCOIN

Tout un écosystème s'est progressivement développé autour de bitcoin. Eléments centraux, des plates-formes d'échange assurent la conversion bitcoin-devises nationales à travers un mécanisme de marché. Les plus actives sont aujourd'hui OkCoin en Chine, Bitfinex et Bitstamp en Europe et aux États-Unis. Des plates-formes alternatives voient également le jour, comme Paymium, développé par notre camarade Pierre Noizat (80), dans le respect des contraintes réglementaires et prudentielles françaises. Des gestionnaires de porte-monnaie proposent aux utilisateurs de gérer leurs comptes pour leur garantir une sécurité plus élevée, voire de bénéficier d'assurances sur les dépôts (Elliptic Vault). L'heure est maintenant au développement de plates-formes de *trading* de produits dérivés ou de services de paiement.

« L'opacité du système a contribué à attirer certaines activités illégales »

Les mineurs ont rapidement fait le choix de majoritairement s'associer en *pools* pour mutualiser leurs revenus, afin d'en réduire la variabilité. Ces associations regrouperaient aujourd'hui plus de 80 % de la puissance de calcul. Les programmeurs, enfin, se sont fédérés autour de la *Bitcoin Foundation,* créée fin 2012, qui dispose d'un double rôle (autoproclamé) de standardisation et de porte-parole de bitcoin.

Ce système d'une complexité croissante se traduit par une gouvernance de plus en plus complexe, évoluant au gré des rapports de forces entre ces différents acteurs. Ce fonctionnement particulier, inédit pour une monnaie, ne manque pas de susciter certaines réticences.

ANONYMAT *VS* CONTRÔLE

L'impossibilité pour un utilisateur d'identifier le propriétaire d'une adresse est souvent prise comme argument contre bitcoin, car facilitant des usages illicites (évasion fiscale, blanchiment, achat de drogue, financement du terrorisme, etc.). Cet anonymat, nécessaire pour préserver la vie privée des utilisateurs, constitue néanmoins un sujet d'attention légitime pour les autorités nationales. En imposant aux plates-formes d'échange les mêmes contraintes qu'aux banques – connaître leurs clients, signaler les transactions suspectes, etc. – il est déjà possible aux autorités françaises d'identifier l'origine et la destination d'un flux entrant ou sortant du système à travers ces plates-formes. Par ailleurs, la recherche de traces laissées sur Internet par un utilisateur permet, dans certains cas, de remonter à son identité. Des solutions d'anonymisation plus efficaces sont toutefois en développement, comme DarkWallet. Elles peuvent devenir particulièrement préoccupantes.

USAGES ILLICITES

L'opacité du système a contribué à attirer certaines activités illégales qui, à leur tour, ont engendré une certaine méfiance vis-à-vis de bitcoin. Le site de vente en ligne de substances et services illicites *Silk Road,* fermé en novembre 2013 par le FBI, et rouvert depuis, exige par exemple des paiements en bitcoin. Cependant, la conservation dans la *blockchain* de l'intégralité de l'historique des transactions dans le système bitcoin constitue un risque d'identification des utilisateurs, même après de nombreuses années. Enfin, les volumes d'échange en bitcoin restent pour l'instant faibles par rapport aux estimations des montants des transactions illégales comme le blanchiment (entre 800 et 2 000 milliards de dollars par an[1] contre 14 milliards de dollars de transactions bitcoin en 2013), ce qui rend bitcoin peu adapté à ce genre d'activités pour le moment. Ainsi, bitcoin n'est

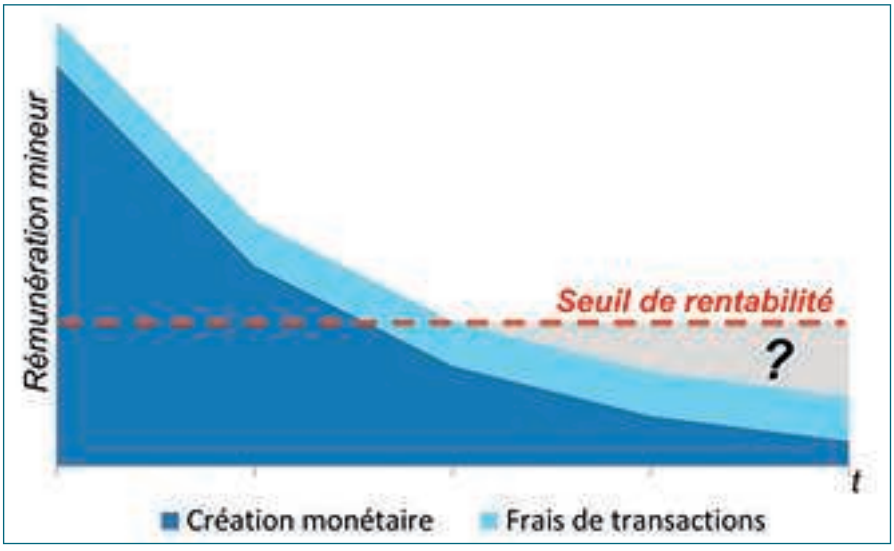

Figure 2 - L'évolution de la création monétaire devrait conduire à une évolution de la rémunération des mineurs.

guère la monnaie idéale pour les transactions illégales, pour lesquelles le « cash » reste une manière probablement aussi sûre de procéder.

DES TRANSACTIONS PEU COÛTEUSES... POUR LE MOMENT

Bitcoin se propose également de réduire les coûts de transactions en s'affranchissant d'un intermédiaire. L'atteinte de cet objectif mérite toutefois d'être nuancée. Tout d'abord, l'utilisateur de bitcoin paye souvent de faibles frais de transactions. Cependant ceux-ci ne forment qu'une part minime de la rémunération des mineurs (moins de 0,5% en 2013), le reste provenant de la création monétaire. À terme, il est très probable que le modèle économique actuel soit remis en cause par le ralentissement progressif de la création monétaire, conduisant vraisemblablement à des coûts de transactions nettement plus élevés, ou à une diminution de la puissance dédiée au minage, se traduisant par une baisse de la sécurité du système. Les services bancaires pourraient ainsi se révéler plus compétitifs que bitcoin, l'architecture décentralisée de bitcoin se révélant intrinsèquement plus chère à maintenir qu'un système centralisé.

BITCOIN, DEMAIN

Trop volatil pour servir d'unité de compte ou de réserve de valeur, encore peu reconnu par les commerçants comme moyen de paiement, bitcoin est encore loin d'être une monnaie à part entière. Pour survivre, bitcoin devra toutefois consentir à des évolutions. Or, celles-ci sont incertaines, notamment du fait d'une gouvernance complexe. De là le développement, dans le sillage de bitcoin, de nouvelles monnaies numériques cherchant à corriger ces imperfections.

C'est surtout le poids des réglementations que bitcoin se verra imposer à terme, en particulier en matière de fiscalité, qui détermineront son avenir. Une position claire des États en la matière est attendue, mais ces derniers hésitent à s'engager et donc à abandonner, tacitement, leur monopole en matière de création monétaire.

« Bitcoin est encore loin d'être une monnaie à part entière »

L'enthousiasme suscité chez certains peut aussi révéler un mouvement profond de remise en cause des monnaies officielles. La défiance à l'égard du système bancaire de réserve fractionnaire et des banques centrales, jugées incapables de mener une politique monétaire indépendante, a pu provoquer chez d'autres un glissement progressif de la confiance envers les institutions vers un algorithme comme bitcoin. Braudel voyait les monnaies comme « à la fois des moteurs et des indicateurs ; elles provoquent, elles signalent le changement. Elles en sont aussi la conséquence. » L'avenir dira ce qu'est bitcoin. ■

PRINCIPAUX MARCHÉS

La Chine est d'ores et déjà le premier marché en termes de volume de transactions (56 % des échanges en mai 2014), notamment parce que bitcoin permet de détourner les contraintes imposées sur les flux de capitaux. L'Afrique semble être un marché prometteur. Ses lacunes en infrastructures de paiement, ainsi que les flux monétaires qu'elle reçoit de sa diaspora – 32 milliards d'euros en 2013 à un coût de transaction moyen de 12 % selon la Banque mondiale – en font un client de choix pour la nouvelle monnaie.

1. Source : United Nations Office on drugs and crimes.