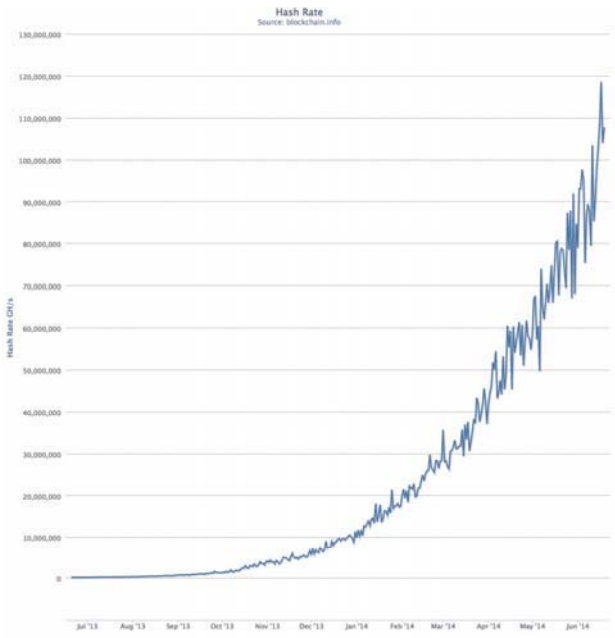
Bitcoin

Par Olivier BORDERIES (1997)

Bitcoin est une nouvelle « monnaie » créée en 2008 par Satoshi Nakamoto (probablement le pseudonyme d'un groupe de cryptographes activistes libertaires; leur papier fondateur, très lisible, présente les grandes lignes du projet: http://bitcoin.org/bitcoin.pdf), qui repose sur un réseau peer-to-peer de serveurs (nœuds) disséminés à travers le monde et communicant entre eux via le protocole bitcoin. Ce réseau opère sans le contrôle d'une autorité centrale. Chacun peut librement créer un nœud et y participer car ce protocole est open source et le client software majoritairement (mais pas nécessairement) utilisé est disponible gratuitement sur internet. La raison d'être du réseau est de garder la trace de tous les transferts de tous les bitcoins, dans l'équivalent numérique d'un registre public, appelé le blockchain. Plus spécifiquement le blockchain est la chaine des enregistrements successifs (horodatés) de l'ensemble des transactions impliquant un (ou une fraction de) bitcoin depuis sa création. Ce blockchain étant public et distribué (dans environ 8000 nœuds aujourd'hui), il est possible pour chaque individu, simplement en interrogeant le réseau, de vérifier indépendamment la propriété d'un bitcoin revendiquée par une contrepartie potentielle avant une transaction.

L'enregistrement des transactions se fait par 'block' (typiquement quelques centaines de transactions), d'où le nom blockchain, que le réseau valide et archive (i.e. ajoute en dernière position du blockchain) environ toutes les 10mn. Le processus de validation (mining) est effectué par les nœuds de manière concurrente. Le critère discriminant est la puissance de calcul. En effet, la validation d'un block consiste à lui trouver et ajouter une signature (un hash au sens cryptographique du terme) ayant des caractéristiques rares (aujourd'hui environ 1/5^{e}19). Par propriété du hash (fonction pseudo aléatoire), cette recherche est assimilable une recherche aveugle. En conséquence, plus la fréquence de génération/test de signatures d'un nœud est grande, plus sa probabilité de valider un block est importante. Pour inciter les nœuds du réseau à dépenser des ressources (machines, électricité, temps) dans la validation des blocks, et par là assurer sa pérennité, le protocole bitcoin prévoit d'attribuer un certain nombre de bitcoins (aujourd'hui 25) au nœud qui valide un block. C'est de cette manière que la monnaie bitcoin est créée.

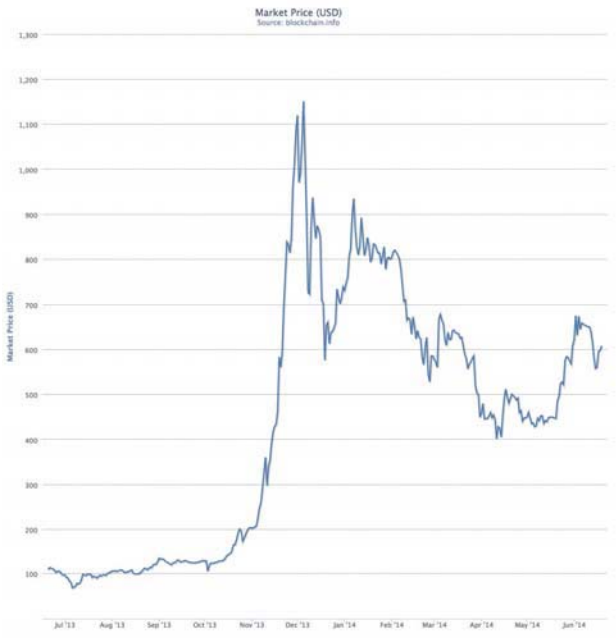


Hash Rate

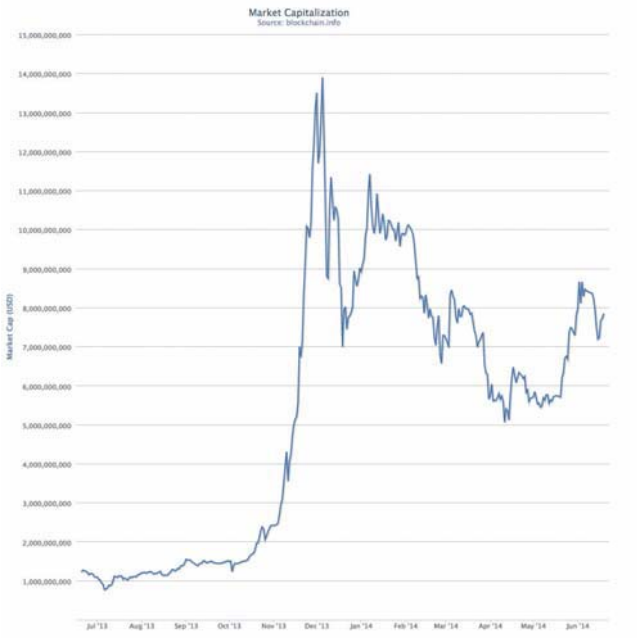
La compétition entre les nœuds pour la validation des blocks pousse ceux-ci à augmenter leur puissance, à tel point qu'aujourd'hui les nœuds utilisent souvent du hardware dédié (ASICS) et représentent en agrégé une puissance supérieure à plusieurs centaines de super ordinateurs. Une fois qu'un bloc a été ajouté au blockchain avec sa signature, il ne peut être modifié sans provoquer une incohérence dans la chaine des signatures (par propriété du hash). D'autre part une copie du blockchain est présente dans chaque nœud du réseau. Ce qui le rend infalsifiable. Cependant il existe un danger reconnu : Si un nœud concentre plus de 50% de la puissance de calcul totale du réseau, celui ci a alors le pouvoir de valider/bloquer n'importe quelle transaction. Ce cas limite, bien que hautement improbable étant donné la très grande fréquence de génération de signatures du réseau (aujourd'hui environ 1^{e}17/s) et sa croissance exponentielle, fait l'objet d'une grande attention de la part des nœuds principaux, c'est à dire ceux qui ont le plus d'intérêt à la survie du réseau. Tout le monde peut voir l'état du réseau en tant réel sur https://blockchain.info/ ou http://blockr.io/ par exemple.

Ainsi le réseau bitcoin se propose de remplacer le rôle traditionnel des banques commerciales et quasi supprimer tout frais de transaction (par comparaison: une transaction par carte bancaire est typiquement facturée 2-3% du montant), et aussi de se soustraire aux banques centrales qui décident souverainement de la quantité de monnaie en circulation, et donc dans une certaine mesure de sa valeur.

Bitcoin est arrivé aux oreilles du grand public au cours de l'année 2013, pendant laquelle son cours a été multiplié par près de 100, avant de retomber sensiblement. Il tourne aujourd'hui autour de 600 USD, et la valeur de marché de



Bitcoin Market Price USD



Bitcoin Market Capitalization

l'ensemble des bitcoins créés à ce jour est environ 8 milliards de USD. La fièvre spéculative qui a accompagné cette hausse a souvent produit des titres de presse sensationnalistes mais peu explicatifs, prédisant la fin proche des monnaies traditionnelles, ou bien alertant contre une très dangereuse illusion.

La récente débâcle de Mount Gox en février 2014, un des premiers et pendant un temps principaux échanges de bitcoins, sur fond de fraude, a encore augmenté l'attention des médias, et la tension dramatique, sur le sujet.
De grands noms, comme Warren Buffett et Marc Andreessen (célèbre capital risqueur de la Silicon Valley) se sont publiquement et résolument opposés sur l'avenir de ce phénomène, le premier le considérant comme un mirage, le second comme révolutionnaire.

En fait, comme dans tout débat médiatique, les choses sont rarement définies avant d'être débattues. Or le cas bitcoin est particulièrement sujet à confusion. En effet, la très brève description ci-dessus montre que le nom bitcoin désigne au moins 4 entités distinctes : un protocole, un réseau, un client software, une monnaie (qui peut être considérée comme un moyen de paiement et/ou une réserve de valeur).

En tout cas, le cours explosif et volatile du bitcoin et l'excitation médiatique associées rappellent un peu les premiers émois du public face à internet et les aventures chahutées des premières sociétés dot com, à la fin des années 90. Si le parallèle est juste, il y a fort à parier que le concept du bitcoin, essentiellement un registre de transactions public et distribué à travers internet, murisse en terme d'applications, et se renforce en terme de sécurité, quelque soit le sort de sa première implémentation.

En matière d'applications, on peut imaginer l'intérêt immédiat pour les nombreux travailleurs migrant typiquement modestes qui renvoient une bonne partie de leur salaire à leur famille et paient actuellement jusqu'à 10% de frais pour le transfert. Plus généralement, le réseau bitcoin peut offrir un substitut au système bancaire dans les pays où celui ci est embryonnaire et/ou peu fiable.

Dans les pays développés, la possibilité de faire des micros paiements (un bitcoin est divisible jusqu'à 1^{e}-8) créerait une zone de prix nouvelle entre la gratuité totale et le montant minimum de transaction viable compte tenu des frais fixes du système bancaire. La presse, et plus généralement tout fournisseur de contenu, pourrait probablement en bénéficier. Le spectre d'applications potentielles est très large, et les étudiants des universités américaines, chaudrons d'innovation et d'imagination, s'organisent en club pour explorer le sujet (e.g. http://bitcoin.mit.edu/, http://bitcoin.stanford.edu/)

Au cours des 20 dernières années, avec une accélération récente, de nombreux domaines ont déjà été essentiellement transportés sur - et radicalement transformés par - internet (e.g. sans objectif d'exhaustivité, le courrier, les encyclopédies/atlas, les réservations de vol/train/voyages, le tourisme, le commerce, les rencontres, les réseaux sociaux, la télévision, le développement software, et assez récemment l'éducation avec les MOOCs)
Dans cette perspective longue, il n'est finalement pas surprenant que le réseau génère quelque idée alternative nouvelle pour concurrencer les moyens de paiement/monnaies traditionnels.

L'AUTEUR

Olivier BORDERIES (1997), est directeur dans le département Cross Asset Solutions de la banque d'investissement de la Société Générale, qu'il rejoint en 2003. Après un début de carrière dans l'industrie des télécoms, suivi d'un MBA (INSEAD), il s'oriente vers la finance. Il s'occupe aujourd'hui de concevoir/promouvoir des solutions d'investissement/couverture à destination d'investisseurs institutionnels en Europe. Le sujet avant-gardiste de cet article n'est cependant pas (encore ?) directement lié à son activité professionnelle.