

COMMISSION OUVERTE
**MARCHÉS ÉMERGENTS,
AUDIOVISUEL ET DROIT
DU NUMÉRIQUE**

Responsable : GÉRALD BIGLE, AVOCAT À LA COUR



Mardi 16 septembre 2014

**Les monnaies numériques
(Bitcoins et autres
cryptomonnaies)**

Intervenants :

Caroline Laverdet

Avocat à la Cour

Hubert de Vauplane

Avocat à la cour

Philippe Rodriguez

Président de l'Association Bitcoin France
et dirigeant d'Avolta Partners



*Présentes à cette occasion, les éditions Lexbase
vous proposent de retrouver un compte-rendu
de cette réunion.*

Revue

Lexbase Hebdo édition affaires n°406 du 18 décembre 2014

[Internet] Événement

Les monnaies numériques (*Bitcoins* et autres cryptomonnaies) — Compte rendu de la réunion du 16 septembre 2014 de la Commission ouverte Marchés émergents, audiovisuel et droit du numérique du barreau de Paris

N° Lexbase : N5106BUN



par Vincent Téchené, Rédacteur en chef de Lexbase Hebdo — édition affaires

La Commission ouverte Marchés émergents audiovisuels et droit du numérique du barreau de Paris a tenu, le 16 septembre 2014, une réunion sous la responsabilité de Maître Gérald Bigle, Avocat au barreau de Paris. A cette conférence, qui avait pour thème " *Les monnaies numériques (Bitcoins et autres cryptomonnaies)*", sont intervenus Caroline Laverdet avocate à la cour, Hubert de Vauplane avocat à la cour, et Philippe Rodriguez Président de l'Association Bitcoin France et dirigeant d'Avolta Partners.

– **Aspects techniques et économiques du *Bitcoin*** (par Philippe Rodriguez Président de l'Association Bitcoin France et dirigeant d'Avolta Partners)

L'Association Bitcoin France regroupe les acteurs travaillant dans les cryptomonnaies, c'est-à-dire les *start-up* offrant des solutions mais aussi les personnes physiques qui ont des activités autour de ce secteur. Le but premier de cette association est de faire la promotion des cryptomonnaies, de fédérer les entreprises et les individus intervenant dans ce secteur et à protéger du régulateur ces inventions et ces technologies.

L'émergence des cryptomonnaies a engendré un affrontement entre des institutions et le monde des nouvelles technologies qui est en train de créer quelque chose. C'est également une confrontation entre générations.

Le terme "*Bitcoin*" désigne à la fois un système de paiement à travers le réseau internet et une unité de compte utilisée par ce système de paiement. Le *Bitcoin* a été inventé par un cryptographe qui a fait le choix de rester anonyme (connu sous le pseudonyme de Satoshi Nakamoto). En 2008, il a publié un document, expliquant comment créer un système qui permettrait de transférer des valeurs de façon sécurisée d'un point à l'autre d'internet sans utiliser aucune organisation ou autorité centrale. A partir de ce document, Satoshi Nakamoto a programmé un système mettant en application cette invention, transformée en logiciel mis en place début 2009. Ce logiciel a été mis en *open source*, c'est-à-dire qu'il a livré le code à une communauté de développeurs, amenée ainsi à l'améliorer. Aujourd'hui 75 % du code de ce logiciel a été redéveloppé.

Le terme "*bitcoin*" peut être utilisé avec un "B" majuscule ou un "b" minuscule. Employé comme un nom propre (il commence par une majuscule et n'est pas précédé d'un article), il se réfère au système de paiement ; employé comme un nom commun (il commence par une minuscule, est précédé d'un article et peut se mettre au pluriel), il se réfère à l'unité de compte.

Auparavant, l'échange de monnaie passait soit par un système à quatre points, soit par un système à deux points. L'invention du *Bitcoin* offre la capacité de passer par un ensemble de points qui, par consensus, permet d'expliquer si cette opération existe ou non. L'organisation centrale est donc remplacée par cet ensemble d'organisations qui décident si l'opération peut avoir lieu. Transférer de l'argent ne nécessite pas de connaître la monnaie, la banque, l'organisation centrale...etc. L'adresse *Bitcoin* est la seule information nécessaire pour recevoir des *bitcoins*. Une adresse *Bitcoin* est gratuite et est générée par un programme informatique soit par des sites internet, soit par des fournisseurs de place de marchés... Elle est constituée d'une clé publique et d'une clé privée. Une transaction correspond à l'envoi d'une certaine somme d'une adresse vers une autre adresse, sans l'intervention d'un intermédiaire. En fait, l'ensemble des ordinateurs (environ 300 000 dans le monde) effectuant des calculs pour déterminer la véracité d'une transaction gère un livre de compte partagé ; c'est un système de *peer to peer*. Le système est donc horizontal. Lorsque la transaction part dans le réseau, les ordinateurs vérifient la transaction et effectuent un calcul extrêmement compliqué. Ce calcul est rendu difficile par l'utilisation d'une preuve de travail, c'est-à-dire la preuve que l'entité qui vient de signer ces calculs est bien un ordinateur. Il faut en moyenne 9-10 minutes pour que l'un des ordinateurs trouve la réponse à l'énigme, enregistre l'opération et la partage avec les autres ordinateurs. Ce système est donc particulièrement sécurisé puisque pour l'attaquer, il faudrait disposer, selon les experts, d'une puissance de calcul permettant de prendre le contrôle de plus de 51 % des nœuds du réseau (attaque dite des 50 %), ce qui en pratique s'avère techniquement impossible et financièrement inintéressant. Le système octroie à l'ordinateur qui a trouvé la solution à l'énigme une partie de la valeur monétaire : 50 *bitcoins* par opération les quatre premières années, 25 *bitcoins* les quatre années suivantes, 12,50 *bitcoins* ensuite, etc., sachant qu'1 *bitcoin* vaut environ, aujourd'hui, 300 euros. La puissance informatique du réseau est de plus en plus importante, ce que le protocole avait prévu dès son origine si bien que l'équation mathématique est de plus en plus compliquée à résoudre. Tous les 15 jours l'équation change de façon à pouvoir ajuster la puissance informatique du réseau. Ceux qui effectuent ces calculs sont appelés les "mineurs". La transaction en *bitcoins* n'est pas répudiable, ce qui est contre intuitif puisque l'ensemble des lois actuelles tend à protéger les transactions en s'assurant de pouvoir revenir en arrière en cas de litige ou de malversation.

La possession des *bitcoins* est matérialisée par une suite de chiffres et de lettres qui constituent un porte-monnaie virtuel (ou compte). Une personne peut détenir plusieurs porte-monnaie. Le porte-monnaie comporte le montant en *bitcoins* de l'argent qu'il contient, une clé publique qu'on peut laisser circuler et une clé privée qui doit rester secrète, car son détenteur peut dépenser l'argent du porte-monnaie. Tout support convient pour conserver la suite de symboles constituant le porte-monnaie : papier, clé USB, la mémoire, etc. Grâce à des logiciels adéquats, il est également possible de gérer son porte-monnaie sur son ordinateur ou son téléphone.

Ce système est réellement utilisé puisqu'une transaction d'un montant équivalent à 160 millions de dollars a été récemment réalisée. Alors qu'une telle transaction coûterait entre 600 000 et 900 000 dollars pour être effectuée par une banque, elle a coûté 8 cents, a mis 1 seconde pour être exécutée et a été totalement vérifiée en 50 minutes pour devenir irrépudiable. Ce système est puissant ; il permet de réaliser des choses jusqu'alors impossible et engendre nécessairement un certain nombre d'enjeux.

Une grosse partie des *bitcoins*, est conservée par ses acheteurs comme une valeur spéculative. Ils peuvent être utilisés sur des sites de commerce électronique qui acceptent cette monnaie électronique, pour effectuer une transaction (une maison a été achetée en *bitcoins*), pour rémunérer quelqu'un en *bitcoins* (c'est le cas d'un avocat canadien)... Les possibilités offertes par cette technologie qui, en outre, permettrait de réduire considérablement le coût des transactions, sont immenses.

Bitcoin est un *challenge* à la fois pour les Etats et les Banques centrales et notamment pour leur souveraineté.

– **Aspects juridiques du *Bitcoin* (par Caroline Laverdet et Hubert de Vauplane, avocats à la cour)**

Pour Caroline Laverdet, l'anonymat inhérent au *Bitcoin* risque de conduire certaines personnes à mener des activités illicites. Le rapport de Tracfin, remis le 11 juillet 2014, prévoit ainsi de limiter l'anonymat en imposant une prise d'identité lors de l'ouverture par un professionnel d'un compte en monnaie virtuelle pour un tiers, et une vérification d'identité pour les retraits et dépôts aux "distributeurs" de *bitcoins*.

L'exemple le plus flagrant sont les nombreux sites présents sur le réseau TOR (acronyme de *The Onion Router*, littéralement "le routeur oignon") qui est une sorte d'internet parallèle, composé de routeurs organisés en couches, appelés nœuds de l'oignon, qui transmettent de manière anonyme des flux. Les sites internet se terminent en ".onion".

Ces sites proposent pour la plupart des produits (notamment des stupéfiants, des produits contrefaits, des faux papiers, des armes, de la monnaie contrefaite) et des prestations de services illicites (hacker un ordinateur pour s'introduire dans une boîte mail, laisser penser qu'une personne consulte des sites pédo-pornographiques...) payables en *bitcoins* et ressemble à un site de commerce en ligne classique avec des avis de consommateurs, des CGV, des FAQ, etc.. L'un des sites les plus connus est "Silk Road". D'ailleurs, le FBI a mis fin et fermé le site "Silk Road" en octobre 2013, estimant que ce site permettait d'acheter avec des *bitcoins* des biens ou services illégaux.

Ces risques ne proviennent donc pas directement des mineurs et des utilisateurs des *bitcoins* qui ont recherché une confiance dans une monnaie et un moyen d'échange en s'écartant des autorités, mais son utilisation peut faciliter la réalisation d'activités illicites. Et, même si les autorités n'ont aucune prise sur le *Bitcoin*, certains faits peuvent entraîner la chute du cours des *bitcoin*.

Il existe ainsi un risque financier : récemment, la faillite de "Mtgox", plate-forme d'échange de monnaie virtuelle *bitcoin*, à la suite vraisemblablement d'une faille sécuritaire, a entraîné la perte de l'équivalent de 500 millions de dollars (800 000 *bitcoins*).

En outre, l'anonymat soulève la question du traçage des transactions, la monnaie transférée pouvant provenir ou servir à des activités illégales.

Enfin, il existe un risque en ce qui concerne le cours du *bitcoin*, en raison de sa volatilité particulièrement forte du cours relativement peu corrélé à la plupart des actifs traditionnels et qui repose notamment sur la confiance de ses utilisateurs dans la sécurité du système. Juridiquement, le *bitcoin* peut-il être considéré comme une unité de compte, un actif, une créance, une monnaie électronique, une monnaie d'échange ? De véritables incertitudes existent qui ont pu conduire la cour d'appel de Paris en 2013 (CA Paris, Pôle 5, 6ème ch., 26 septembre 2013, n° 12/00 161 N° Lexbase : A7474KLE) à décider que les intermédiaires devaient obtenir un agrément de l'ACPR ou encore l'administration fiscale à estimer que les plus-values réalisées sur le *bitcoin* étaient imposables.

Hubert de Vauplane rappelle que l'un des principaux problèmes des banques est la fraude à la carte bancaire, alors que la fraude au *bitcoin* semble inenvisageable aujourd'hui en raison de son caractère sécurisé. Une grosse partie du produit net bancaire émane des commissions sur cartes bancaires. Les banques doivent donc prendre en compte que ce "système" nettement plus sécurisé viendra concurrencer en quelque sorte les paiements par cartes bancaires entraînant donc une baisse significative de leur chiffre d'affaires généré par cette activité. Ceci est une vraie question. D'où le point de savoir comment réguler le *Bitcoin*. Si la question revêt un véritable intérêt théorique, la manière d'appréhender le sujet doit être pragmatique ; il faut laisser l'innovation se développer et ne pas l'encadrer trop strictement pour ne pas la tuer. Un contrôle à l'entrée sur les mouvements de fonds et un régime fiscal adéquat semblent suffisants.

La définition juridique du *Bitcoin* est compliquée car l'innovation touche à plusieurs champs : celui des moyens de paiement, celui de l'unité de réserve, mais aussi celui de la régulation de la monnaie, si l'on considère que c'est une quasi-monnaie. Il est donc compliqué de faire entrer le *Bitcoin* dans les cadres juridiques existants.

Il est intéressant de relever les symétries du *Bitcoin* avec l'or. Comme Hubert de Vauplane l'a écrit (1) " Si l'on met de côté le caractère immatériel du bitcoin, celui-ci, tout comme l'or, est un bien qui a une valeur en soi conduisant à une fluctuation quotidienne de son cours ; mais il est aussi une unité d'échange (non légale) permettant d'acheter ou de vendre d'autres biens. Si l'or, comme toute marchandise, fait l'objet d'un droit de propriété, on peut aussi considérer que la détention d'un bitcoin conduit son détenteur à disposer des caractéristiques de la propriété sur celui-ci. Pourtant, il existe une différence entre les deux : le bitcoin est par nature non fongible puisque chaque bitcoin est individualisé. L'or peut être fongible (le minerai bien sûr, mais aussi les pièces métalliques) ou non (les

lingots sont tous numérotés)". On pourrait être tenté de voir dans le *bitcoin* une monnaie électronique : il s'agit bien d'unité monétaire (c'est-à-dire qui sert à mesurer la valeur de l'échange), stockée sous forme électronique, aux fins d'opérations de paiement accepté par des personnes physiques ou morales. Mais, par rapport à la définition juridique de la monnaie électronique, deux éléments essentiels font défaut pour le *bitcoin* : il n'y a pas d'"émetteur" proprement dit, mais surtout la remise initiale de *bitcoins* ne correspond pas à un versement de fonds initial. En outre, une monnaie légale se caractérise par son pouvoir libératoire absolu qui permet à un débiteur d'éteindre une dette vis-à-vis de son créancier par règlement à celui-ci d'une quantité déterminée d'unités monétaires à leur valeur nominale. Le *bitcoin* n'a pas force légale dans un espace géographique déterminé. Il n'a donc pas d'effet libératoire légal et ne peut, de ce seul fait, prétendre à la qualification juridique de monnaie.

Néanmoins, il n'est pas souhaitable à ce stade d'apporter une réponse sur la qualification juridique. C'est la réglementation qui doit apporter les réponses aux interrogations posées par ce système. Déterminer le cadre juridique avant le cadre normatif, n'est pas la bonne option. Considérer, par exemple, que l'échange d'une monnaie ayant cours légal contre une monnaie virtuelle comme le *bitcoin* peut être qualifié de service de paiement permet d'appliquer un corps de règles, telles que celles sur la lutte contre le blanchiment, la nécessité d'un agrément de prestataire de services de paiement, etc., assurant ainsi une sécurité juridique. C'est la position de l'ACPR et de la Banque de France, la première considérant que "*dans le cadre d'une opération d'achat/vente de bitcoins contre une monnaie ayant cours légal, l'activité d'intermédiation consistant à recevoir des fonds de l'acheteur de bitcoins pour les transférer au vendeur de bitcoins relève de la fourniture de services de paiement*". Le fondement sous-jacent de cette position du régulateur est que l'activité de paiement est une activité trop sérieuse pour être exercée par n'importe qui. Cette approche très pragmatique est retenue par la plupart des régulateurs. Cette "analyse" en un service de paiement a aussi été reprise dans une jurisprudence récente opposant une plate-forme d'échange de *bitcoins* (la société Macaraja) au Crédit industriel et commercial (CA Paris, Pôle 5, 6ème ch., 26 septembre 2013, n° 12/00 161, préc.) Du point de vue théorique, cette analyse est critiquable. D'une part, le *bitcoin* n'est pas une monnaie ayant cours légal. D'autre part, pour qu'il y ait service de paiement, encore faut-il pouvoir rattacher cette activité à l'un des services de paiement prévus par la "DSP" (Directive 2007/64 du Parlement européen et du Conseil du 13 novembre 2007, concernant les services de paiement dans le marché intérieur N° Lexbase : L5478H3B).

Ni la Banque de France, en tant que banque centrale ou de membre du système européen des banques centrales, ni la BCE, en tant qu'émetteur de l'euro ne se sont intéressés au *Bitcoin*, mais ce sont bien les régulateurs en tant que superviseurs des activités bancaires et de paiement qui se sont saisis de la question. Autrement dit, ce n'est pas sous l'angle de la monnaie et macroéconomique que les banquiers abordent le problème mais bien sous celui des opérations et de la régulation des opérations, car leur tropisme bien normal est la lutte contre le blanchiment de capitaux.

D'ailleurs, la définition précisée par le site du ministère de l'Economie et des Finances reflète cette approche : "*une monnaie virtuelle est une monnaie non-officielle émise sous forme numérique. Elle n'a pas de matérialisation physique. Une monnaie virtuelle n'est donc pas juridiquement une monnaie, ni un instrument de paiement mais c'est un moyen de transaction qui peut permettre d'effectuer des paiements en ligne.*"

La réglementation des opérations bancaires et financières semble suffire. Ainsi, les placements en *bitcoins* peuvent entrer dans la catégorie des biens divers de l'AMF. Ce n'est pas un instrument financier mais offrir des placements sur des "biens" autres que des instruments financiers est aussi régulé

Des propositions d'"amélioration" ou plutôt de précisions du cadre juridique ont été faites par l'Association Bitcoin France :

- un non-assujettissement de ces monnaies virtuelles à la TVA ;
- la mise en place d'une *flat tax* pour l'imposition des plus-values sur les cessions de *bitcoin*, à l'image de ce qui existe pour les matières premières et l'or ;
- des propositions sur le paiement des salaires en *bitcoins* ;
- une régulation des plate-formes.

Il est à noter qu'au niveau européen, la Commission européenne s'est saisie du sujet des monnaies virtuelles et a demandé à l'EBA de se pencher sur le sujet. L'Histoire est déjà presque écrite car cela devrait conduire à considérer que l'opération d'échange est un service de paiement.

Les personnes souhaitant intervenir en tant qu'entrepreneur dans le système du *Bitcoin*, se pose la question du traitement fiscal des "clients" de l'utilisateur. Et, le développement des activités liées au *Bitcoin*, dépendra bien en-

tendu de son traitement fiscal. Récemment, l'Administration fiscale a indiqué que les gains tirés de la vente d'unités de compte virtuelles stockées sur un support électronique (notamment les "*bitcoins*"), lorsqu'ils sont occasionnels, sont soumis à l'impôt sur le revenu dans la catégorie des bénéfices non commerciaux (BNC). Si l'activité est exercée à titre habituel, elle relève du régime d'imposition des bénéfices industriels et commerciaux (BIC). Par ailleurs, les unités de compte virtuelles stockées sur un support électronique entrent dans l'assiette de l'impôt de solidarité (ISF) définie par l'article 885 E du Code général des impôts (N° Lexbase : L8780HLR) et doivent ainsi figurer dans la déclaration annuelle d'ISF des redevables qui en possèdent. Les transmissions à titre gratuit d'unités de compte virtuelles stockées sur un support électronique sont également, en vertu des dispositions de l'article 750 ter du CGI (N° Lexbase : L9528IQX), soumises aux droits de mutation à titre gratuit, sous réserve de l'application de conventions internationales. Par ailleurs, et conformément aux préconisations de l'Association Bitcoin France, le rapport de Tracfin sur les monnaies virtuelles prévoit de soutenir au niveau européen un non-assujettissement de ces monnaies virtuelles à la TVA en raison notamment des risques de fraude liés au caractère remboursable de la TVA sur des actifs immatériels, comme l'a montré l'expérience des quotas carbone. Le Gouvernement est sur cette ligne.

S'il semble possible de prévoir, dans un contrat, un "paiement" en *bitcoins*, cette option trouve sa limite dans les règles fiscales puisqu'il sera nécessaire de prévoir une évaluation en euros pour le traitement fiscal de l'opération (ex. : cession de fonds de commerce).

En outre, de vraies questions de territorialité sur le lieu de la transaction se posent : où est exécuté ce service de paiement, dès lors que tout est dématérialisé ? L'un des critères caractéristiques essentiels en matière monétaire est le lieu de paiement ; or avec le *bitcoin*, il n'y a pas de lieu de paiement. Il est donc extrêmement compliqué de déterminer le droit territorialement applicable.

(1) Lire, H. de Vauplane et S. Cazaillet, Bitcoin : money, money, money ?, Lexbase Hebdo n° 567 du 17 avril 2014 — édition fiscale (N° Lexbase : N1872BUU).