Eclairages sur l'obscur des monnaies virtuelles

Elisabeth Omes
Hervé Hansen
Avocats à la Cour
Elvinger Hoss Prussen

Tout progrès donne du fil à retorde aux juristes. Chaque innovation (qu'elle relève du secteur financier ou scientifique) exige une opération d'analyse et de qualification juridiques, qui s'avère souvent délicate car elle risque d'exposer des incohérences dans un ordre juridique donné. Parfois, ces incohérences ne peuvent être réparées que par une réforme normative.

Les monnaies virtuelles sont un phénomène que peu de juristes spécialistes du droit bancaire et financier osaient imaginer il y a encore quelques années. Elles donnent lieu à un certain nombre de questions, dont la réponse dépend d'une opération de qualification juridique. Sont-elles des monnaies électroniques? Sont-elles des monnaies comme les autres, c'est-à-dire analogues aux monnaies étrangères comme le dollar américain ou le yen japonais? S'agit-il peut-être d'instruments financiers ou des biens mobiliers intangibles rendant la désignation de « monnaie » trompeuse?

Le présent éclairage cherche à donner des pistes de réflexion concernant un certain nombre de problématiques liées aux monnaies virtuelles et les solutions qu'on pourrait envisager. Il est certainement trop tôt pour donner des réponses définitives. Sans anticiper sur ce qui suivra, on peut déjà révéler qu'il n'est pas évident de trouver une qualification cohérente des monnaies virtuelles qui offre des solutions satisfaisantes dans tous les domaines de notre droit.

Ce qui est sûr, c'est que les monnaies virtuelles existent. Elles sont un animal juridique inconnu, dont la catégorisation correcte exigera un certain travail, mais il serait une grave erreur de considérer qu'il n'existe pas au regard du droit. L'inconnu n'est pas inexistant. Si on a pu dire dans le contexte d'une infraction pénale dont l'identité des auteurs était incertaine que: « *Et war net keen*. », il convient de constater dans le cadre de la qualification juridique des monnaies virtuelles que: « *Se sin net näischt.* »

Définition

Les monnaies virtuelles, dont l'incarnation la plus connue est le *bitcoin*, sont des unités de compte qui peuvent être utilisées comme intermédiaires d'échange et réserves de valeur, mais qui n'ont pas d'émetteur central et ne sont pas nécessairement liées à une monnaie conventionnelle : « *Le* bitcoin *est une unité de compte virtuelle stockée sur un support électronique permettant à une communauté d'utilisateurs d'échanger entre eux des biens et services sans avoir à recourir à la monnaie légale.* »[1]. Ainsi, le *bitcoin* n'a pas d'émetteur central et n'a aucun lien avec une monnaie conventionnelle.

En pratique, les monnaies virtuelles sont stockées sur un support électronique et échangées de façon électronique. Cependant, on pourrait parfaitement imaginer des monnaies virtuelles fonctionnant à l'aide de supports matériels[2].

Les concepts de monnaie virtuelle et monnaie électronique peuvent paraître semblables, mais ils ne sont pas identiques. L'article 1(29) de la loi du 10 novembre 2009 relative aux services de paiement[3] définit la monnaie électronique comme étant :

« *une valeur monétaire représentant une créance sur l'émetteur, qui est:*

i) stockée sous une forme électronique, y compris magnétique, et

ii) émise contre la remise de fonds aux fins d'opérations de paiement, et

iii) acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique; »

Comme les monnaies virtuelles ne sont pas émises en contrepartie d'une remise de fonds, elles ne constituent pas une créance sur un émetteur. La pos-

1 J. Lasserre Capdeville, « 3 Questions – Le bitcoin », *JCP E*, 25, n°3, 16 janvier 2014.

2 European Banking Authority, *EBA Opinion on 'virtual currencies'*, EBA/Op/2014/08, 4 juillet 2014, § 20, p. 11.

3 Cet article transpose en droit luxembourgeois l'article 2(2) de la directive 2009/110/CE relative aux services de paiement.

sibilité de se passer d'un émetteur central intrigue, mais fait tout leur charme. Le détenteur d'unités de compte (qui ne représentent pas une créance sur un tiers) ne dépend donc pas de la solvabilité d'autrui. La monnaie virtuelle sans émetteur présente l'avantage qu'elle ne peut pas faire l'objet d' « assouplissement quantitatif » par une banque centrale.

L'absence d'émetteur central permet aux parties à un transfert de monnaie virtuelle d'éviter le contrôle d'un tiers. C'est pour cette raison que le *bitcoin* a pu être utilisé à des fins illicites (p.ex. trafic de stupéfiants, rémunération de tueurs à gage, blanchiment d'argent), ce qui lui a valu une certaine réputation. Voilà également pourquoi, les autorités nationales et internationales ciblent leurs analyses sur les risques d'utiliser les monnaies virtuelles à des fins frauduleuses.

Les monnaies virtuelles sont-elles des monnaies ?

Le qualificatif de « monnaie » pour les monnaies virtuelles pose problème à certains dans la mesure où « *leur fonction d'échange et leur effet libératoire ne sont que purement conventionnels et non légaux, ceux-ci n'étant effectifs qu'entre les seuls membres de la communauté d'utilisateurs de ces monnaies, d'autre part, la trop grande volatilité de leurs cours n'en fait pas des réserves de valeur satisfaisantes*. »[4]

L'argument concernant la volatilité est de nature empirique. Si le *bitcoin* a subi de violentes fluctuations par le passé, force est de constater que la volatilité a diminué ces derniers mois. De toute manière, l'évolution du cours du *bitcoin* ne permet pas d'arriver à des conclusions concernant toutes les monnaies virtuelles. Conceptuellement, rien ne permet de dire que les monnaies virtuelles seraient en soi plus volatiles que des monnaies émises par les banques centrales des Etats.

L'argument concernant l'effet libératoire purement conventionnel est plus sérieux.

L'effet libératoire d'un paiement n'est imposé par la loi que si la monnaie en question a cours légal.

Celui qui refuserait un paiement par une monnaie ayant cours légal au Luxembourg commettrait même une infraction pénale (article 556[5] du Code pénal).

4 J. Dubois, « La régulation des crypto-monnaies et de leurs plate-formes de conversion », *Revue internationale des services financiers*, 2014/2, pp. 77-82, voir p. 78.

5 Art. 556 Code pénal : *Seront aussi punis d'une amende de 25 euros à 250 euros:*[…] *4° Ceux qui, à défaut de convention contraire, auront refusé de recevoir les monnaies non fausses ni altérées, selon la valeur pour laquelle elles ont cours légal dans le Grand-Duché.*

Au Luxembourg, seul l'euro a cours légal. Comparé à l'euro, le *bitcoin* a donc l'inconvénient de ne pas avoir cours légal et partant de pouvoir être refusé par un créancier sans que ce dernier ne contrevienne à l'article 556 du code pénal précité.

Cela dit, le *bitcoin* a cette caractéristique en commun avec le dollar, le yen, la livre sterling et toutes les autres monnaies étatiques autres que l'euro. Or, personne ne conteste que ces monnaies sont des « vraies » monnaies.

C'est donc à raison que la Commission de Surveillance du Secteur Financier (CSSF) reconnaît dans son communiqué du 14 février 2014 que les monnaies virtuelles sont de la monnaie «*puisqu'elles sont acceptées comme moyen de paiement pour des biens et des services par un cercle suffisamment large de personnes*. », tout en insistant dans le même communiqué sur le fait que les monnaies virtuelles n'ont *« à l'évidence pas cours légal »*.

Fonctionnement du *bitcoin*

Sans vouloir prétendre fournir des explications techniques exhaustives, il paraît utile d'expliquer de façon simplifiée le fonctionnement de la monnaie virtuelle la plus connue, le *bitcoin*, créé en 2009 par Satoshi Nakamoto.

Le *bitcoin* fonctionne sur base d'un réseau *peer-to-peer* dont les participants sont ceux qui ont activé un programme informatique à cet effet (un « *bitcoin client* »). Chaque participant dispose d'au moins une clé publique (diffusée à tout le réseau), qui peut être comparée à un portefeuille (le « *bitcoin wallet* ») ou un coffre en banque. Afin de pouvoir faire des paiements en utilisant des *bitcoins* associés à cette clé publique, c'est-à-dire afin d'extraire le contenu du coffre, il faut une clé privée (gardée secrète) qui est détenue par le seul « propriétaire » du coffre en question.

La quantité de *bitcoins* associée à une clé publique est diffusée au réseau. En d'autres termes, le coffre a la particularité d'être transparent. Chacun peut voir ce qui se trouve dans mon coffre, mais je suis le seul à pouvoir l'ouvrir au moyen de la clé privée.

La transparence du coffre importe peu, car son « propriétaire » peut rester anonyme. Afin de s'identifier, il doit simplement détenir la clé privée.

La raison pour laquelle chacun peut voir ce qui se trouve dans un coffre en particulier est que la chaîne de toutes les opérations effectuées depuis que le *bitcoin* existe est sauvegardée dans le réseau. Chaque participant au réseau est le dépositaire d'un segment de la chaîne de sorte que le réseau pris en son intégralité contient la chaîne entière. Afin d'éviter qu'un segment soit manipulé, le même segment est déposé auprès de plusieurs participants. Ainsi, lorsque deux participants fournissent des infor-

mations contradictoires sur un même segment, il suffit de faire appel au réseau pour déterminer le contenu correct du segment sur base des informations fournies par la majorité des participants dépositaires du même segment.

Ce travail de comparaison, qui permet de consolider la chaîne des opérations, exige une puissance de calcul considérable. Il ne peut être accompli qu'à l'aide de matériel informatique coûteux et un investissement de temps considérable. Afin d'inciter à ce travail, le réseau récompense ceux qui s'y adonnent en leur permettant de créer un nombre prédéterminé de *bitcoins*. C'est par cette opération de calcul cryptographique permettant à son auteur de créer des *bitcoins* (dénommée « *mining* ») que sont « émis » les *bitcoins*.

Afin d'éviter une émission à effet inflationnaire, la quantité de *bitcoins* émis par unité de travail diminue avec le temps et un nombre maximum de *bitcoins* a été fixé par avance (à 21 millions d'unités). Le dernier *bitcoin* sera émis environ en 2140.

Le *bitcoin* peut ainsi être utilisé comme unité de compte, intermédiaire de change et réserve de valeurs par ceux qui le souhaitent. Il n'est lié à aucune monnaie conventionnelle et ne connaît pas d'émetteur central.

Qualification juridique des activités liées aux monnaies virtuelles

Les autorités de contrôle du secteur bancaire et financier, nationales et internationales, se sont intéressées relativement tôt au phénomène des monnaies virtuelles, principalement pour avertir les consommateurs et investisseurs des dangers liés au développement de ces nouvelles monnaies et établir des recommandations visant à prévenir leur usage à des fins frauduleuses ou de blanchiment. De nombreuses analyses ont été publiées ces deux dernières années[6].

Au vu de l'identification de ces risques, certaines autorités essaient de soumettre les monnaies virtuelles à un certain contrôle en qualifient les services qui les entourent d'activités soumises à un agrément de prestataire de services de paiement voire d'entreprise d'investissement.

Le régulateur luxembourgeois rapproche les services liés aux monnaies virtuelles des services de paiement soumis à la loi du 10 novembre 2009 relative aux services de paiement voire d'une activité de PSF au sens de la loi du 5 avril 1993 relative au secteur financier. Ainsi, dans son communiqué du 14 février 2014[7], la CSSF invite ceux qui souhaitent émettre des moyens de paiement libellés en monnaies virtuelles, ceux qui veulent offrir des services de paiement utilisant des monnaies virtuelles et ceux qui ont l'intention d'installer un marché (une plateforme) pour négocier des monnaies virtuelles à lui décrire en détail les activités envisagées. Sur base de cette description, la CSSF déterminera le statut pour lequel une autorisation devra être demandée. En fonction des activités envisagées, il est certainement envisageable qu'un agrément d'établissement de paiement soit requis.

En France l'ACPR (Autorité de contrôle prudentiel et de résolution) se prononce comme suit : *« 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 »*[8]. Ce faisant, l'ACPR est en ligne avec une décision rendue le 26 septembre 2013 par la Cour d'appel de Paris, ayant retenu que la société qui, lors de négociation de Bitcoins sur une plateforme d'échange gérée par une société étrangère, reçoit les fonds des acheteurs et les transfère aux vendeurs, déduction faite de ses frais et commissions et de ceux dus au gestionnaire de la plateforme, fournit un service de paiement pour lequel elle a besoin d'un agrément[9].

Ce n'est qu'en Allemagne que le régulateur s'éloigne des services de paiement pour se rapprocher des services d'investissement. Cette différence d'orientation s'explique par le fait que la BaFin qualifie les monnaies virtuelles d'instruments finan-

6 On peut notamment citer les suivantes : European Central Bank, Virtual Currency Schemes, October 2012; Banque de France, Les dangers liés au développement des monnaies virtuelles: l'exemple du Bitcoin, Focus n°10, 5 décembre 2013 ; EBA, Avertissement aux consommateurs concernant les monnaies virtuelles, 12 décembre 2013 ; BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht), Bitcoins : Aufsichtliche Bewertung und Risiken für Nutzer, 19 décembre 2013 ; ACPR, Banque de France, Position de l'ACPR relative aux opérations sur les Bitcoins en France, 29 janvier 2014 ; CSSF, Communiqué de presse relatif aux monnaies virtuelles, 14 février 2014 ; Groupe de travail « Monnaies virtuelles » piloté par Tracfin, l'encadrement des monnaies virtuelles, recommandations visant à prévenir leurs usages à des fins frauduleuses ou de blanchiment, juin 2014 ; GAFI, Monnaies virtuelles: Définitions clés et risques potentiels en matière de LBC/FT, juin 2014 ; EBA, EBA Opinion on « virtual currencies », 4 juillet 2014.

7 Communiqué de presse de la CSSF du 14 février 2014 relatif aux monnaies virtuelles : « les intéressés potentiels qui souhaitent s'établir au Luxembourg pour exercer une activité du secteur financier (comme par exemple l'émission de moyens de paiement libellés en monnaies virtuelles ou autres, l'offre de services de paiement utilisant des monnaies virtuelles ou autres, l'installation d'un marché (« plateforme ») pour négocier des monnaies virtuelles ou autres) doivent définir leur objet social et leur activité de façon suffisamment concrète et précise pour permettre à la CSSF de déterminer le statut pour lequel ils devront obtenir l'agrément ministériel ».

8 ACPR, Banque de France, Position de l'ACPR relative aux opérations sur les Bitcoins en France, 29 janvier 2014

9 CA Paris, 26 septembre 2013, n°12/00161; L'essentiel - droit bancaire, n°4 Avril 2014, p.5, note J. Lasserre Capdeville.

ciers[10]. Même si la CSSF ne qualifie pas le *bitcoin* d'instrument financier, il ne faut pas oublier que le *bitcoin* pourrait être lié à un instrument financier tel un contrat de différence (CFD) ou un contrat d'option. Dans ce cas, les professionnels prestant des services liés à ce type d'instrument financier devront disposer de l'agrément de PSF (entreprise d'investissement et/ou PSF spécialisé) couvrant les services qu'ils proposent.

Quand le virtuel rencontre le réel : Peut-on voler ou saisir les monnaies virtuelles ?

Deux questions se sont spontanément imposées : quid du vol ou de la saisie des *bitcoins* ? Il est certain que la problématique de la qualification juridique des monnaies virtuelles se posera dans d'autres contextes (p.ex. liquidation d'une communauté en cas de divorce, apport de *bitcoins* au capital d'une société), mais à ce stade, deux questions feront l'objet d'une brève analyse: celle du vol et celle de la saisie-arrêt de ces monnaies.

La question du vol engendre nécessairement celle de savoir si les monnaies virtuelles peuvent être qualifiées de « chose » au sens de l'article 461 du Code pénal. La réponse est loin d'être évidente[11]. Pour prendre le contrôle des *bitcoins* d'autrui, il suffit d'appréhender la clé privée (une sorte de mot de passe très complexe) des *bitcoins* en question. Cette clé privée peut être sauvegardée sur un disque dur local, un serveur ou répartie dans le *cloud* (c'est-à-dire sur plusieurs serveurs sous forme cryptée). Celui qui copie une clé privée se rend-il déjà coupable de vol ? Ou le vol n'a-t-il lieu qu'au moment où celui qui a copié la clé privée l'utilise pour faire une opération en utilisant les *bitcoins* d'autrui ? Ou n'y a-t-il pas de vol du tout ? Dans ce cas, les infractions de « *hacking* » incriminées aux articles 509-1 à 509-7 du Code pénal sont-elles d'application ?

Nous ne connaîtrons la réponse définitive à ces questions qu'une fois que les tribunaux luxembourgeois auront eu à connaître d'une soustraction d'unités de monnaies virtuelles. Cependant, il est probable qu'ils s'inspireront d'un récent arrêt de la Cour de cassation dans lequel il a été décidé que : « *Attendu que les données électroniques enregistrées sur le serveur de la banque et qui sont juridiquement sa propriété exclusive constituent des biens incorporels qui peuvent faire l'objet d'une appréhension par voie de téléchargement* »[12].

Ainsi, si des données électroniques sont une « chose » au sens de l'article 461 du Code pénal, il devrait en être de même des clés privées *bitcoin*. Concernant les *bitcoins* eux-mêmes, la question est plus épineuse car ils ne consistent pas en des données électroniques enregistrées sur un support, mais en des unités de compte virtuelles.

Le créancier qui veut faire une saisie-arrêt sur les monnaies virtuelles de son débiteur est confronté à un problème similaire[13]. L'article 693 du Nouveau code de procédure civile dispose que : « *Tout créancier peut, en vertu de titres authentiques ou privés, saisir-arrêter entre les mains d'un tiers les sommes et effets appartenant à son débiteur, ou s'opposer à leur remise*. »

Comme expliqué plus haut, les monnaies virtuelles sont conservées dans une sorte de « coffre transparent ». Or, on sait que le contenu d'un coffre-fort donné en location par une banque ne peut pas faire l'objet d'une saisie-arrêt « *non en raison de l'insaisissabilité des effets qui y sont entreposés et qui font l'objet de la saisie, mais en raison de l'inexistence d'une condition tenant à la qualité du tiers saisi*. »[14]

L'unité de monnaie virtuelle elle-même n'est stockée nulle part puisqu'elle n'est représentée que par une inscription en compte virtuel (la clé publique). Ce compte virtuel ne peut être utilisé que par le détenteur de la clé privée correspondant à la clé publique pertinente. Il est donc difficilement concevable de saisir les unités de monnaie virtuelle elles-mêmes (sauf si elles sont déposées auprès d'une « banque » de monnaies virtuelles). Quant à la clé privée, celle-ci ne pourrait faire l'objet d'une saisie-arrêt que si elle a été remise entre les mains d'un tiers. Or, si la clé privée est stockée sur un serveur, le propriétaire de la clé ne l'a pas remise au propriétaire du serveur en vertu d'un contrat de dépôt, mais fait simplement usage du serveur comme le client d'une banque ferait usage d'un coffre-fort en vertu d'un contrat de location.

Donc, une saisie-arrêt sur des *bitcoins* (ou autres monnaies virtuelles) nous paraît à ce stade difficile en l'absence d'une inscription en compte auprès d'un dépositaire.

* * *

Les quelques explications qui précèdent n'ont pas l'ambition d'être exhaustives et ne donnent qu'un

10 BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht), Bitcoins : Aufsichtliche Bewertung und Risiken für Nutzer, 19 décembre 2013: « die BaFin hat BTC rechtlich verbindlich als Finanzinstrumente in der Form von Rechnungseinheiten gemäss §1 Absatz 11 Satz 1 Kreditwesengesetz (KWG) qualifiziert ».

11 La question de la localisation de l'infraction est à dessein ignorée.

12 Cour de cassation, 3 avril 2014, n° 17/2014, n° 3304 du registre.

13 La localisation des monnaies virtuelles est un problème qui devra être résolu au préalable.

14 F. Kremer et C. Mara-Mahuenda, « Le banquier face à la saisie-arrêt civile de droit commun : développements récents » dans *Droit bancaire et financier au Luxembourg 2014*, Volume II, p. 1174, n° 28.

bref aperçu d'un nouveau phénomène qui est susceptible d'occuper le secteur bancaire et financier dans un futur proche et des problématiques juridiques qui en découlent et découleront. A voir si le phénomène s'installe et continue à se développer (après les « Art funds », verra-t-on les « Bitcoin funds » ?) ou si le *bitcoin* sera un casse-tête passager tel le cube de Rubik dans les années 1980.