Note numéro 6
septembre 2014

Note du CREOGN

Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale

Monnaies virtuelles : nature et risques

Le bitcoin a été l'une des vedettes de l'année 2013 avec l'envolée de son taux de change multiplié par près de 100 en 12 mois, suscitant d'ailleurs la multiplication de monnaies virtuelles concurrentes. Ces monnaies virtuelles se légitiment dans la contestation de l'État et de l'imposante réglementation bancaire et financière. Pourtant, cette réglementation devient indispensable à leur pérennité, pour renforcer la sécurité et la confiance.

La monnaie, une définition plus économique que juridique

Le droit français ne donne aucune définition de la monnaie. Les quelques textes juridiques existants sont contenus dans le Traité de Maastricht qui réserve le monopole de l'émission des billets de banque à la Banque Centrale Européenne, les seuls à avoir cours légal. Ces billets ne peuvent donc être refusés en règlement de dettes libellées en euros, même s'il existe des dispositions stipulant l'obligation de régler par un moyen traçable au-delà d'un seuil déterminé. Le Code monétaire et financier se limite à préciser quel est le pouvoir libératoire des formes monétaires exprimées en euros.

Pour les économistes, les choses sont mieux cernées, depuis longtemps. En effet, dès le IV^{eme} siècle avant notre ère, Aristote dans son « Éthique à Nicomaque » avançait que la monnaie était un instrument d'échange, un étalon de valeur et une réserve de valeur. Le prix Nobel Milton Friedman rappelait qu'au final, « n'importe quel bien susceptible de fournir une garantie provisoire sur le pouvoir d'achat général peut faire office de monnaie ».

L'histoire de la monnaie demeure celle de l'innovation pour une plus grande simplification. Se sont imposés de façon récente les billets de banque, traduisant l'abandon progressif des métaux précieux comme référence, puis la monnaie scripturale, de simples écritures dans les livres comptables des banques[1], et enfin la monnaie électronique[2], des impulsions numériques, détenues sur des supports ad hoc : cartes, clés USB ou disques d'ordinateur. Mais ces monnaies – et ce très tôt dans l'histoire – ont une spécificité forte : elles sont devenues la marque, le symbole du souverain. Battre monnaie est la caractéristique du pouvoir régalien.

Pourtant, la création monétaire est largement un phénomène privé

Dans les faits, la création monétaire est largement privée. En effet, pour l'essentiel, la monnaie naît à l'occasion de l'octroi d'un crédit bancaire, principalement par les banques commerciales, le plus souvent privées. De même, l'or et l'argent n'ont jamais été créés par un État, le souverain se limitant à apporter sa marque.

Le pouvoir régalien s'exprime en fait au travers les actions de contrôle, de réglementation et de régulation de l'activité monétaire. L'activité bancaire aujourd'hui s'effectue sous la surveillance de la Banque Centrale Européenne qui exécute une mission définie par la loi[3], avec des moyens définis par la loi. Elle est ainsi fort proche d'une autorité administrative indépendante. Cette réglementation garantit des droits aux utilisateurs de la monnaie souveraine.

1 En novembre 2013, les pièces et billets représentaient 9 % de l'agrégat monétaire M3, contre 91 % pour les dépôts bancaires.

2 La directive européenne 2009/110/CE du 16 septembre 2009 définit la monnaie électronique comme une « valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique ».

3 Article 108 du Traité de Maastricht et L 141-1 du CMF (pour la Banque de France).

Laissons de côté les monnaies alternatives[4] et regardons la monnaie « cyber ». Il convient ici de clarifier une terminologie qui n'est pas véritablement fixée. On parle ainsi de monnaies virtuelles, le terme « virtuel » correspondant pleinement à l'acception qu'en donne Denis Berthier[5] : « est virtuel ce qui, sans être réel, a, avec force et de manière pleinement actuelle, les qualités du réel ».

Les premières monnaies virtuelles reposaient sur des dispositifs alliant système de paiement centralisé et monnaie. C'est ainsi qu'ont fonctionné « e-gold », de 1996 à 2006, et « liberty reserve » de 2006 jusqu'à son démantèlement par les polices de 17 pays en mai 2013, pour fait de blanchiment.

Plus élaborées, sont venues ensuite les « cryptomonnaies », dont le parangon est le bitcoin. Ce dernier a été inventé en 2009 par un Japonais, Satoshi Nakamoto, vraisemblablement le pseudonyme d'un groupe d'informaticiens sur lequel on sait peu de chose. Il fonctionne en « peer to peer », c'est-à-dire en échange direct et décentralisé entre internautes, sous forme cryptée (d'où sa dénomination). Autrement dit, le dispositif « bitcoin » est aussi système de paiement. Les transactions financières se dispensent de plates-formes de compensation, ce qui, selon ses partisans, réduit très fortement les coûts de fonctionnement. Elles restent traçables mais demeurent anonymes... du moins tant que le détenteur du portefeuille n'est pas identifié.
Il n'existe pas non plus d'autorité gérant le dispositif, l'équivalent d'une banque centrale. Cette dernière est d'autant plus inutile que la création monétaire est programmée pour atteindre un nombre fini de bitcoins (environ 21 millions) vers 2040. Les bitcoins naissent ex nihilo selon un rythme décroissant par l'exécution d'un algorithme complexe (le minage). Une masse monétaire indépendante de l'action des États est supposée leur éviter la tentation de jouer avec sa valeur.
Cerise sur le gâteau, le bitcoin est convertible en monnaies souveraines. Des plates-formes en permettent l'achat ou la vente, la valeur de change se formant selon l'offre et la demande. A cet égard, l'envolée folle de la fin de l'année 2013, jusqu'à 1200 $ en novembre - contre 100 en septembre, 15 en janvier 2013 et 0 en 2009 – puis la chute de 50 % à la mi-décembre sont imputée respectivement à la demande chinoise puis aux mesures restrictives prises alors par la Banque Populaire de Chine.
Le succès du bitcoin a attiré de nouvelles offres similaires. Selon François Paget, chercheur en cybermenaces chez Mac Afee, une centaine de monnaies similaires aurait été créée depuis 2009 – dont quelques-unes ont déjà disparu !
En tout état de cause, les monnaies virtuelles traduisent clairement la remise en cause de la mainmise régalienne sur la monnaie.

Des avantages espérés qui sont autant de risques réels
Le bitcoin apparaît comme une belle innovation technologique. Sa masse évolue conformément aux prévisions. Est-ce véritablement un souci qu'il échappât à toute instance de contrôle ? Ses promoteurs font valoir qu'il offre ou offrira à terme plusieurs avantages :

- la stabilité des prix ;
- un faible coût de transaction ;
- la discrétion des transactions.

En fait, ces avantages avancés sont à moduler en raison soit de risques de nature économique, soit de comportements déviants qui, à terme, constituent une menace pour la confiance que l'on peut placer dans le bitcoin, la pire des choses qui puisse arriver à une monnaie. Les Banques centrales[6] n'ont d'ailleurs pas manqué d'alerter.

Tout d'abord, la stabilité des prix n'est pas garantie par une masse monétaire fixée. Pour que les prix restent stables, il faut, au moins en première approximation, que la masse monétaire croisse au même rythme que l'offre de biens et services, ce que la conception d'une monnaie

4 Monnaies privées émises sur une aire géographique donnée, qui restent néanmoins émises sous le contrôle des autorités monétaires.
5 Ingénieur polytechnicien ; la citation est tirée de « méditations sur le réel et le virtuel » L'Harmattan, 2004.
6 Après la BCE, en 2012, les Banques centrales de nombreux pays ont d'une façon générale alerté sur les risques liés aux monnaies virtuelles, allant jusqu'à imposer des mesures restrictives (Inde, Chine) voire à interdire les transactions en bitcoin (Thaïlande).

P2P exclut – en tout cas aujourd'hui -.
Cette monnaie présente même des motifs d'instabilité structurelle, faute de garde-fous :

- absence de banque centrale pour réguler les changes ;
- absence d'économie nationale attachée au bitcoin, ne permettant pas de bénéficier d'un effet « compétitivité » en cas de baisse du taux de change ;
- absence de valeur intrinsèque du bitcoin, à la différence de l'or pour lequel il existe un marché non monétaire assurant une valeur minimale au métal ;
- parfaite substituabilité par des monnaies souveraines, voire des monnaies virtuelles concurrentes[7] : malgré sa rareté programmée, la demande de bitcoin sera extrêmement variable selon que les consommateurs souhaiteront l'utiliser ou lui préféreront les monnaies souveraines qui rendront les mêmes services.

Si le cours du change du bitcoin est passé de quelques euros en début d'année 2013 aux alentours de 900 à la fin de l'année, cela s'explique certes par la montée en régime de son usage. Mais aussi par le caractère fortement spéculatif que lui confère son essence volatile. Le risque de change[8] est considérable, avec des fluctuations parfois de 10 % en quelques heures, de 20 % en quelques jours … Des produits dérivés – options ou contrats de différence, avec de forts effets de levier – sont apparus, qui sont moins des instruments de couverture que de spéculation.
Enfin, la détention des bitcoins apparaît très concentrée : moins de 50 personnes possèdent 30 % des bitcoins, moins de 1000 en conservent la moitié. L'étroitesse du marché peut faire craindre des manipulations de cours.

Évoquer des coûts de transactions faibles dans ces conditions est excessif. Certes, le système de paiement « bitcoin » se passe d'intermédiaire. Mais c'est sans la prise en compte des risques, de change comme évoqué supra, voire d'erreurs – par le caractère irréversible des opérations – et de vol.

On ne peut sous-estimer en effet l'ampleur du « cyberbrigandage[9] ». Les cas de vol de porte-monnaie se multiplient en raison de la profitabilité du cybercrime. En 2011, la plate-forme d'échanges MtGox annonce le vol de 1000 bitcoins (et la leçon n'a guère porté – cf. infra). C'est alors une somme limitée... A la même époque, un particulier découvre le piratage de son ordinateur et le vol de 25 000 bitcoins, soit à l'époque la bagatelle de 350 000 euros (mais 17 millions d'euros aux cours de janvier 2014). A l'automne 2013, le site Inputs.io subit un vol de 4 100 bitcoins – 1,2 millions de dollars – et la plate-forme d'échange danoise est piratée pour un préjudice d'un million d'euros.
Les hackers ont parfaitement compris que les coûts de ces « cyber hold-up » sont modestes pour des rentabilités fortes. Rappelons que l'une des raisons originelles des banques était la protection des valeurs de la rapacité des criminels... Le prix Nobel d'économie Paul Krugman évoquait à propos du bitcoin une régression monétaire[10]. On peut certes en débattre mais sur ce point précis, c'est effectivement une marche en arrière.

Ce sont deux qualités majeures avancées par les promoteurs du bitcoin qui en révèlent néanmoins toute l'ambivalence : la discrétion et la convertibilité. Faire circuler l'argent de façon (presque) anonyme, et pouvoir le transformer à tout instant en monnaie souveraine représente le nec plus ultra du système de paiement. Ce sont deux facilités extraordinaires que la criminalité organisée ne pouvait négliger.
Des sites internet offrent des produits totalement illicites de toute nature : numéros de cartes bancaires, stupéfiants, armes, pédopornographie... Ce sont les marchés noirs du « darkweb ». L'anonymat des monnaies virtuelles, doublé du recours à un réseau spécifique qui brouille les traces sur la toile, permet de réaliser des emplettes criminelles dans la plus grande discrétion. Au début du mois d'octobre 2013, le FBI fermait Silk Road, site mettant en relation acheteurs et vendeurs, se rémunérant par commission, où les paiements ne s'effectuaient qu'en bitcoin.

7 Sauf peut être sur les sites du « darkweb ».
8 Le risque de change est le risque de perte due à une évolution défavorable du taux de change d'une devise détenue (ou d'un actif libellé en devise).
9 N'est pas abordé ici le « botnet de minage » qui consiste en la prise de contrôle illicite d'ordinateurs afin de les utiliser pour bénéficier de la création de nouveaux bitcoins.
10 http://www.rtbf.be/info/chroniques/detail_des-bits-et-de-la-barbarie?id=8164268 – Paul Krugman a obtenu le prix Nobel d'économie en 2008.

Ce « cyber-supermarché » (ou plus exactement « cyber-courtier ») du produit criminel, ouvert en 2011, aurait généré un chiffre d'affaires total de 9,5 millions de bitcoins, à comparer aux 12 millions actuellement en circulation, pour 600 000 bitcoins de commissions. Il a été très vite remplacé par d'autres et d'ailleurs un nouveau « Silk Road » a ouvert un mois plus tard. Il s'agit ici d'une criminalité pleinement économique : s'il y a une demande et un profit à réaliser, il y aura une offre. L'internet et les monnaies virtuelles sont des moyens d'accroître la profitabilité du crime par des gains de productivité et la réduction des coûts ...

De façon simple, le blanchiment qui consiste à dissimuler l'origine illicite de capitaux en est facilité : les flux criminels sont convertis en monnaie virtuelle, transférés là où on veut les dissimuler puis « transformés » à nouveau en monnaie officielle (propre!).
Tracfin décrit ainsi dans son rapport 2011 comment une société en France opérait de multiples transactions vers l'étranger de façon totalement dissimulée. Le site Liberty Reserve, autre cyber-supermarché de l'illicite, aurait blanchi 6 milliards de dollars en utilisant la monnaie virtuelle éponyme. En janvier 2013, Charlie Shrem, un des pontes du monde du bitcoin - vice-président de la Fondation Bitcoin – connaissait des démêlés avec la Justice américaine, pour avoir contribué à fournir des bitcoins à des acheteurs chez Silk Road.
Deux éléments peuvent encore freiner l'ardeur des blanchisseurs dans l'utilisation du bitcoin : sa traçabilité et sa forte volatilité. Mais des solutions « correctrices » apparaissent : le zerocoin est un avatar du bitcoin qui offre un réel anonymat, sous couvert du respect de la vie privée … Et un Russe a lancé le wishcoin au début de 2014, dont la valeur est indexée sur le rouble, tout en garantissant l'anonymat.

La confiance passe par la réglementation
Faut-il interdire les monnaies virtuelles ? Outre que cela reviendrait à condamner toute forme d'innovation, une telle interdiction risque fort d'être illusoire, le cyberespace étant international. En revanche, il est temps de sortir du brouillard juridique, ne serait-ce que pour créer les conditions nécessaires au maintien de la confiance. L'ACPR[11] impose, depuis janvier 2014, aux sociétés effectuant « à titre habituel » des opérations de change avec des bitcoins, de disposer d'un agrément de prestataire de service de paiement, les soumettant ainsi à la dense réglementation financière.

Ce pourra éviter des désastres. Ainsi celui causé par MtGox ! En février 14, cette plate-forme de change – l'une des premières dans le monde - dépose le bilan, qu'elle impute à des malversations informatiques Le préjudice est évalué alors à 350 millions d'euros, pour l'essentiel au détriment des clients qui n'ont aucun recours. Par comparaison, la réglementation française impose désormais à cette nature d'activité – quand elle porte sur des monnaies officielles – de respecter notamment des règles de sécurité.
L'AMF[12] en juillet 2014 souligne l'importance des risques juridiques et criminels, « sur fond de transparence limitée, d'asymétrie d'information et de flou juridique ». Les conditions ne sont pas réunies pour un fonctionnement sain des marchés financiers, en raison de l'absence de règles et de contrôleurs, ouvrant la porte à de multiples fraudes. Aussi TRACFIN[13], dans une analyse au final très proche, propose de limiter l'anonymat et de plafonner les paiements par monnaie virtuelle.

D'une façon plus générale, les Banques centrales et l'Autorité Bancaire Européenne alertent depuis 2012 sur les risques inhérents aux monnaies virtuelles, autour de deux grands thèmes : la dérive criminelle et le manque de protection des utilisateurs. Des États les ont interdites[14], la France s'oriente plutôt vers un renforcement de la réglementation. Il reste que le système a été conçu pour se dispenser de contrôleurs… Cette réglementation est nécessaire à la confiance indispensable pour la pérennité du bitcoin, mais ce sera sans doute au détriment de ses atouts concurrentiels.

11 Autorité de Contrôle Prudentiel et de Résolution, en charge de la surveillance des banques et assurances ; sur le rôle attendu de l'ACPR, voir article de Jean-Luc Delangle dans la Revue du CREOGN, avril 2014, p41 & 42 (disponible sur le site du CREOGN).
12 Autorité des Marchés Financiers, en charge de la surveillance des activités financières ; le document ici évoqué s'intitule « Cartographie 2014 des risques et tendances sur les marchés financiers et pour l'épargne »
13 Rapport sur l'encadrement des monnaies virtuelles
14 La position des différents Etats est présentée dans le document de l'AMF cité supra page 68.