LES MONNAIES VIRTUELLES

PROJET EXPLORATOIRE PREMIER SOUTIEN 2015-2016

Sous la direction de

Madame le Professeur Valérie Malabat

0. INTRODUCTION

Alors que la monnaie virtuelle « *ne connaît pas de qualification certaine, le droit se saisit des opérations d'intermédiation [et] encadre notamment les plates-formes d'échanges* »[1]. Cette description met à jour une réaction spontanée de l'environnement juridique face à un phénomène nouveau. Pourtant, la réalité de cette soumission des opérateurs de monnaie virtuelle aux règles applicables aux prestataires de service de paiement doit être discutée : elle n'est ni systématiquement retenue, ni tout à fait convaincante au regard de la réalité des opérations effectuées[2]. Pire encore, elle est incapable de couvrir l'ensemble des activités et des risques que suscite la monnaie numérique.

Sur un plan plus théorique, il y a de toute façon un paradoxe certain dans cette démarche finaliste poursuivie par les autorités nationales. Cherchant à appliquer des règles juridiques existantes à un objet nouveau, celles-ci font l'impasse sur la certitude généralement attachée à l'opération de qualification. Or, si l'on veut concevoir un régime juridique adéquat, il semble cohérent de le construire à partir d'une réflexion menée en amont, afin d'identifier les risques, les enjeux, et les réponses adaptées.

Cette réflexion est d'autant plus importante que l'irruption des monnaies virtuelles est un facteur de changement, voire de révolution, sur au moins deux plans. Premièrement, sur le plan des principes, elle questionne le lien consubstantiel entre la monnaie et l'Etat. Il est en effet généralement admis, bien que cela ne soit pas indiscutable[3], que l'émission de la monnaie est une prérogative régalienne et donc territorialisée. Sur un second plan, plus pratique, c'est la légitimité et l'efficacité fonctionnelles du système bancaire traditionnel qui sont contestées. Ce système, fondé sur la coopération des banques nationales et des banques privées, est donc amené à réagir face à la faculté de disruption que prétendent posséder les monnaies virtuelles.

Les analyses présentées ci-dessous s'inscrivent donc dans un processus initié par les pouvoirs publics depuis 2013 dans l'optique de mieux connaître des monnaies virtuelles. Elles offrent un regard pluridisciplinaire et scientifique sur un phénomène nouveau, et participent ainsi au débat nécessaire à la réception par le monde économique et juridique des crypto-monnaies.

---

[1] P. Pailler, « Quelles règles pour l'encadrement de la monnaie virtuelle en France ? », *RISF*, 2014, n° 4, p. 40.

[2] T. Bonneau, « Commentaire sous CA Paris, 26 septembre 2013, n° 12/00161, *SAS Macaraja c/ SA Crédit industriel et commercial* », *JCP E*, 2014, p. 1091 : l'auteur considère qu'il aurait été plus pertinent de faire une analogie avec les prestataires de services d'investissement.

[3] Voir par exemple, R. Libchaber, *Recherches sur la monnaie en droit privé*, LGDJ, 1992, n° 60 et s.

1. PRESENTATION DU PROJET DE RECHERCHE

Selon Denis Beau, directeur général des opérations à la Banque de France, « *[c]onsidérer le bitcoin comme une monnaie est un abus de langage, il ne relève pas du code monétaire* »[4]. *De lege lata*, l'affirmation est difficilement contestable[5]. L'enjeu d'un travail de recherche pluridisciplinaire sur les monnaies virtuelles n'est pas là. Il doit au contraire investir une triple interrogation destinée à comprendre la nature des monnaies virtuelles ; à établir moins la ou les qualifications possibles que l'approche souhaitable, au regard des enjeux que soulève leur utilisation ; et à évaluer, en conséquence, le besoin de régulation.

Plus largement, l'irruption des monnaies virtuelles participe et illustre un mouvement qui interroge la place et le fonctionnement de la monnaie et des institutions monétaires dans la société occidentale[6]. Vecteur et marqueur du changement, ces nouvelles monnaies issues du monde numérique ne pouvaient laisser indifférent ni les autorités politiques, ni le monde scientifique[7]. C'est donc avec pour objectif de situer les monnaies virtuelles dans leur environnement réel et d'évaluer le besoin d'adaptation ou de réaction de cet environnement, que ce projet de recherche pluridisciplinaire a été entrepris[8].

---

[4] Position exprimée devant la Commission des finances du Sénat, le 15 janvier 2014 (http://www.senat.fr/ compte-rendu-commissions/20140113/fin.html). Dans le même sens, il a pu être écrit que « *[c]ontrairement au vocable attaché à ce produit, il ne s'agit pas d'une monnaie, puisqu'il n'est pas créé par un Etat* » (H. de Vauplane et S. Cazaillet, « Bitcoin : *money, money, money* », *La lettre juridique*, 17 avril 2014, n° 567, p. 1).

[5] Toutefois, il est à noter que pour « *la Commission luxembourgeoise de surveillance du secteur financier (CSSF), [...] de telles monnaies sont de la monnaie (car acceptées comme moyen de paiement pour des biens et des services par un cercle suffisamment large de personnes)* » (P. Storrer, « Crowdfunding, bitcoin *: quelle régulation ?* », *Dalloz*, 2014, n° 14, p. 833). De même, l'Allemagne leur reconnaît la qualité de « monnaie privée » et la Californie a amendé la Section 107 du *Financial Code* pour clarifier la légalité de l'utilisation des monnaies virtuelles comme moyen de paiement ou de transfert d'argent (voir *infra*).

[6] BCE, *Virtual currency schemes*, Francfort, 2012, p. 48: « *Although in practical terms virtual currency schemes are only an evolution, from a conceptual point of view they do present substantial changes when compared to real currencies and payment systems* ». Voir plus largement, pour une illustration des débats suscités par la monnaie, E. Dacheux et D. Goujon, « Pas de transition sans une nouvelle approche de la monnaie : pour une monnaie délibérée », *The Conversation*, 24 mai 2016 (https://theconversation.com/pas-de-transition-sans-une-nouvelle-approche-de-la-monnaie-pour-une-monnaie-deliberee-59476).

[7] Sur l'intérêt de cette démarche, voir P. Storrer, *op. cit.*, p. 832-834.

[8] On peut même penser que la question de la réglementation des monnaies virtuelles est une question de vie ou de mort pour elles. En effet, si face aux difficultés que rencontrent leur développement, « *[l]e souvenir de la réticence qu'a rencontrée à ses débuts la carte bancaire amène à ne pas affirmer de manière trop péremptoire que le bitcoin n'est pas prêt à convaincre le grand public, [il] y a également fort à parier que sans un engagement des autorités, la question de la confiance pourra constituer une marche infranchissable* » (N. Clausset et A. Sellem, « Le bitcoin, de l'engouement à l'indifférence : L'avenir d'une monnaie qui a dérangé », *La Gazette de la Société et des Techniques*, 2015, n° 82, p. 3).

Traditionnellement une monnaie regroupe trois fonctions économiques :

1) elle est un instrument de mesure de la valeur qui permet aux agents économiques de s'accorder sur une évaluation en fixant un prix. La monnaie constitue en ce sens une unité de compte standardisée. La première des fonctions essentielles est intellectuelle et consiste donc à offrir une unité de valeur. La versatilité des monnaies virtuelles est sur ce point problématique ;

2) la monnaie est ensuite un instrument d'échange, un intermédiaire qui possède un pouvoir libératoire vis-à-vis des dettes et obligations. C'est la seconde fonction essentielle attachée à la monnaie, une fonction matérielle de paiement. Là encore, l'absence de caractère libératoire[9] questionne la nature légale des monnaies virtuelles ;

3) enfin, la monnaie constitue un instrument de réserve de valeur. En tant qu'objet de propriété, elle peut être thésaurisée. La conservation de sa valeur peut toutefois poser des difficultés et elle dépend des actions de l'émetteur, ce qui explique le rôle historiquement prépondérant des Etats dans le statut et le fonctionnement des monnaies.

Ces éléments constitutifs expliquent que la monnaie doive en principe revêtir certaines qualités : « *La fonction de mesure de la valeur suppose la divisibilité de la monnaie (*divisibility*). Son utilisation en tant qu'instrument de paiement implique sa mobilité (*transportability*) et son acceptabilité (*cognizability*). La conversation de la valeur par la monnaie nécessite qu'elle puisse revêtir une certaine durabilité (*durability*)* »[10].

Il apparaît à l'évidence que les monnaies virtuelles ne remplissent pas sans difficulté l'ensemble de ces critères (fonctionnels et qualitatifs)[11] – alors même que certains auteurs ont pu relever la proximité voulue entre les monnaies virtuelles et les monnaies métalliques[12]. On peut noter en ce sens les précautions prises par la conférence des gouverneurs des banques

---

[9] Il semble toutefois que la jurisprudence canadienne pourrait accepter de reconnaître un caractère libératoire à un paiement en Bitcoin (par exemple entre deux utilisateurs habituels des monnaies virtuelles) dans la mesure où depuis les années 30 elle juge que « *tout moyen d'échange qui remplit les fonctions de la monnaie reconnaît généralement un pouvoir libératoire envers le débiteur* ». En conséquence, pour la doctrine libérale canadienne, « *une monnaie qui n'a pas cours légal, mais qui a acquis le statut de monnaie dans une communauté, deviendrait une monnaie officielle* » (M. Lacoursière, « L'encadrement juridique de la monnaie virtuelle au Canada », *RISF*, 2014, n° 4, p. 24, spé. note 33).

[10] R. Bismuth, *Dictionnaire encyclopédique de l'Etat*, Paris, Berger-Levrault, 2014, p. 636.

[11] Voir par exemple, P. Pailler, *op. cit.*, p. 41.

[12] L. Desmedt, « Le bitcoin et les crypto-monnaies : nouveaux modèles, questions persistantes », *RISF*, 2014, n°4, p. 9 : « *Le rapport aux moyens de paiement métalliques est abondamment souligné dans le vocabulaire utilisé et dans l'iconographie [...] Ainsi, les crypto-monnaies apparaissent comme une involution dans l'histoire des instruments de paiements, un retour à une époque pré-bancaire* ».

centrales américaines (*Conference of State Bank Supervisors*) pour définir les monnaies virtuelles[13]. L'évolution du traitement réservé au bitcoin permet cependant de faire des suppositions de portée générale, et de penser que les monnaies virtuelles pourraient, malgré l'absence de certaines caractéristiques des monnaies au sens de la théorie économique, se voir reconnaître juridiquement comme des monnaies *sui generis* – cela ne saurait cependant se faire dans des conditions juridiquement satisfaisantes à droit constant. L'intérêt et la difficulté d'une étude pluridisciplinaire des monnaies virtuelles résident justement dans la confrontation de ces deux univers cognitifs, car elle montre l'originalité de ces dernières, ainsi que le besoin d'adopter une approche et des solutions nouvelles pour appréhender leur fonctionnement. Après une présentation synthétique de l'objet d'étude, seront exposés les objectifs et les méthodes du groupe de travail qui depuis novembre 2015 s'est intéressé, sous la direction du Professeur Valérie Malabat, aux monnaies virtuelles.

1.a Objet

Définition

Selon le rapport Tracfin de 2014, une « *monnaie virtuelle est une unité de compte stockée sur un support électronique[14], créée, non par un Etat ou une union monétaire, mais par un groupe de personnes physiques ou morales, et destinée à comptabiliser les échanges multilatéraux de biens ou de services au sein de ce groupe* »[15]. Dans une définition tout aussi

[13] CSBS, « State Regulatory for Virtual Currency Activities. CSBS Model Regulatory Framework », 15 septembre 2015, p. 2 : « *Virtual Currency is a digital representation of value used as a medium of exchange, a unit of account, or a store of value, but does not have legal tender status as recognized by the United States Government* ».

[14] En conséquence, certains auteurs qualifient les monnaies virtuelles de monnaie électronique. En droit de l'Union européenne se rapprochement ne semble pas permis par la directive 2009/110/CE, qui définit cette dernière 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* » (Article 2). C'est d'ailleurs ce qu'affirment clairement les rapports officiels, tel que celui du groupe de travail du ministère des Finances (*L'encadrement des monnaies virtuelles. Recommandations visant à prévenir leurs usages à des fins frauduleuses ou de blanchiment*, juin 2014, p. 3) ou encore du Conseil fédéral suisse (*Rapport du Conseil fédéral sur les monnaies virtuelles en réponse aux postulats Schwaab (13.3687) et Weibel (13.4070)*, 2014, p. 8).

[15] Tracfin, *L'encadrement des monnaies virtuelles. Recommandation visant à prévenir leurs usages à des fins frauduleuses ou de blanchiment*, juin 2014, p. 3. La définition proposée par la Commission européenne dans le cadre du projet de modification de la quatrième directive anti-blanchiment est très similaire : « *"virtual currencies" means a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically* » (article 3, 18) du projet de directive présenté *infra*).

La définition adoptée par le *New York State Department of Financial Services* (*NYSDFS*), est par contre plus resctrictive, car elle exclut notamment les monnaies créées dans le cadre de jeux vidéos et qui ne sont pas convertibles en monnaie fiat : « Virtual Currency *means any type of digital unit that is used as a medium of exchange or a form of digitally stored value. Virtual Currency shall be broadly construed to include digital units of exchange that (i) have a centralized repository or administrator ; (ii) are decentralized and have no centralized repository or administrator; or (iii) may be created or obtained by computing or manufacturing*

englobante, le Fond Monétaire International considère que relèvent du concept de monnaie numérique toutes les « *représentations numériques de valeur, émises par des promoteurs privés et libellées dans leur propre unité de compte* »[16]. Du point de vue de leur rapport au pouvoir, les monnaies virtuelles sont donc des monnaies privées qui se développent à l'insu de l'Etat, hors des circuits établis pour la circulation des monnaies ayant un cours légal, sur une aire géographique souvent plus large en utilisant des réseaux ouverts permettant de se passer d'intermédiaire.

On peut ajouter que certaines d'entre elles n'ont pas vocation à ne circuler qu'entre les membres du groupe fondateur, mais au contraire à se répandre comme un outil « normal » d'échange. A cet égard, le système de monnaie virtuelle peut être fermé (les unités se gagnent alors directement par « minage », ou par gain dans le cas des jeux en ligne par exemple), ou ouvert s'il existe une convertibilité avec les monnaies ayant un cours légal selon un taux fixe ou variable. Les systèmes ouverts peuvent être à flux bidirectionnels ou unidirectionnels selon les règles de convertibilité adoptées[17]. Des plateformes internet se sont spécialisées dans l'achat et la vente de monnaies virtuelles, permettant non seulement à ceux qui ne participent pas au minage d'acquérir des unités, mais aussi de déterminer le taux de change avec les monnaies étatiques[18].

Le périmètre ainsi défini est donc très large et inclut aussi bien des coupons de fidélité que des instruments de valeurs plus sophistiqués. Parce que ce sont celles qui posent le plus de difficultés, se sont essentiellement les « crypto-monnaies » qui ont été retenues dans cette étude, et plus précisément celles qui reposent sur un système ouvert, non-étatique,

---

effort. Virtual Currency shall not be construed to include any of the following : (1) digital units that (i) are used solely within online gaming platforms, (ii) have no market or application outside of those gaming platforms, (iii) cannot be converted into, or redeemed for, Fiat Currency or Virtual Currency, and (iv) may or may not be redeemable for real-world goods, services, discounts, or purchases. (2) digital units that can be redeemed for goods, services, discounts, or purchases as part of a customer affinity or rewards program with the issuer and/or other designated merchants or can be redeemed for digital units in another customer affinity or rewards program, but cannot be converted into, or redeemed for, Fiat Currency or Virtual Currency ; or (3) digital units used as part of Prepaid Cards ; » (NYSDFS, Regulatory framework, 24 juin 2015, *New York Codes, Rules and Regulations*, Title 23, Chap. 1, Part. 200, Sect. 200.2).

[16] FMI, *Virtual Currencies and Beyond : Initial Considerations*, 2016, p. 7 (https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf) : « *VCs are digital representations of value, issued by private developers and denominated in their own unit of account.2 VCs can be obtained, stored, accessed, and transacted electronically, and can be used for a variety of purposes, as long as the transacting parties agree to use them. The concept of VCs covers a wider array of "currencies," ranging from simple IOUs of issuers (such as Internet or mobile coupons and airline miles), VCs backed by assets such as gold, and "cryptocurrencies" such as Bitcoin"* ».

[17] Sur les différentes catégories, voir BCE, *Virtual currency schemes*, Francfort, 2012, p. 14 et s.

[18] Banque de France, « Les dangers liés au développement des monnaies virtuelles : l'exemple du bitcoin », *Focus*, 5 décembre 2013, n° 10, p. 2.

décentralisé et à flux bidirectionnel. Elles constituent le seul type de « monnaie » *lato sensu* qui ne soit pas régulé.

Plus exactement, elles constituent le seul type de monnaie – pour autant que ce terme puisse être employé en droit à leur sujet – qui ne relève pas clairement d'une catégorie juridiquement établie et réglementée.

Tableau 7 : Matrice des différents types de monnaie

	Format de la monnaie	
Statut légal	**Physique**	**Digital**
Non régulé	Certains types de monnaies locales	Monnaies virtuelles
Régulé	Billets et pièces	E-monnaies
		Monnaies commerciales des banques (dépôts)

Source : BCE 2012.

Si en France, à la suite notamment de la Banque de France[19], un consensus se fait autour de l'idée que les monnaies virtuelles devraient être distinguées des instruments de paiements[20] et des instruments financiers[21] (définis respectivement par l'article L. 133-4 Code monétaire et financier (CMF) et l'article L. 211-1 CMF), ou encore des monnaies électroniques (visées par la directive européenne 2009/110 (DME2)[22]), des incertitudes persistent en effet quant à la qualification juridique qui doit s'imposer[23].

---

[19] Banque de France, *op. cit.*, p. 5.

[20] Pour un contrepoint, voir P. Pailler, *op. cit.*, p. 41-42 : « *Sur une base conventionnelle et privée, la monnaie virtuelle peut bien remplir le rôle d'instrument de paiement* », au regard de « *l'importance de la finalité dans [la] définition* », de sorte que l'on pourrait la considérer comme « *un système de paiement électronique sans intermédiaire* ». C'est également la position tenue par Gonzague Grandval, fondateur de Paymium.

[21] Voir par exemple, R. Vabres, « Le statut fiscal de la "monnaie virtuelle" en droit français », *RISF*, 2014, n° 4, p. 44 : « *la "monnaie virtuelle" ne constitue ni un titre représentatif du capital d'une société, ni un titre de créance, ni un contrat financier* »). Là encore, Pauline Pailler explore toutefois cette hypothèse, en considérant que la monnaie virtuelle peut encore relever de la catégorie des biens divers soumis à la loi n° 2°14-344 du 17 mars 2014 relative à la consommation (*op. cit.*, p. 42-43).

[22] Cette qualification est exclue dans la mesure où les monnaies virtuelles ne sont pas émises contre la remise de fonds, conformément aux dispositions de l'article L. 315-1 CMF qui transpose les dispositions de la directive.

[23] H. de Vauplane, « L'analyse juridique du Bitcoin », *Rapport Moral sur l'Argent dans le Monde*, 2014, p. 353-355 ; N. Godlove, « Regulatory Overview of Virtual Currency », *Oklahoma Journal of Law and Technology*, 2014, Vol. 10, p. 24-31 (https://www.law.ou.edu/sites/default/files/files/FACULTY/godlove%20revised2.pdf – l'auteur envisage les qualifications de monnaie, de marchandise et de contrat, écarte les deux premières pour conclure que les monnaies virtuelles sont des contrats relatifs à la création et à la détention d'une nouvelle forme de propriété intellectuelle).

L'appréhension des crypto-monnaies en tant que « monnaie » est même contre-intuitive pour le juriste : dans l'imaginaire de l'*homo juridicus*, « *la question du lien entre monnaie et Etat constitue un point de fixation récurrent dans l'histoire et dont les aspects juridiques reflètent de façon assez fidèle le rôle, considérable mais toutefois en déclin, des entités souveraines dans le phénomène monétaire* »[24].

Appréhender les monnaies virtuelles comme des monnaies au sens juridique du terme supposerait donc d'admettre le principe d'une déconnection entre leur existence et le caractère souverain de son créateur, un abandon d'une « *dimension organique* »[25] de l'argent jusque-là essentielle. Autrement dit, il faudrait admettre qu'une monnaie au sens juridique n'a pas nécessairement la qualité de monnaie légale[26], sans pour autant devoir tomber sous la catégorie des monnaies complémentaires locales qui sont tolérées par l'Etat (et dont la légalité est subordonnée, en vertu de l'article L 521-3 CMF, à la condition qu'elles circulent à l'intérieur d'un réseau limité d'accepteurs ou pour un éventail limité de biens ou de services)[27].

Face aux incertitudes quant à la nature du *bitcoin*, une approche alternative a pu être mise en œuvre par la Cour d'appel de Paris lors d'un litige opposant une banque et une société ayant des activités dans le secteur des monnaies numériques désireuse d'ouvrir un compte[28]. Au lieu de s'intéresser à l'objet de ces activités (donc à la monnaie virtuelle en tant que telle), la juridiction s'est simplement intéressée à la nature de ces activités pour considérer qu'il s'agissait de prestations de service de paiement. En conséquence, à défaut d'avoir l'agrément requis en la matière par l'article L 521-2 CMF[29], elle a jugé que la société ne pouvait contester le refus opposé à bon droit par la banque. Si cette approche peut paraître séduisante, car elle emporte un certain nombre d'obligations pour les opérateurs agissant sur le marché des monnaies numériques, d'une part, elle reste insuffisante dans la mesure où elle ne couvre

[24] R. Bismuth, *Dictionnaire encyclopédique de l'Etat*, Paris, Berger-Levrault, 2014, p. 636.

[25] *Id.*

[26] Si la Banque de France considère depuis 2013 que le Bitcoin ne peut être appréhendé ni comme une monnaie légale, ni comme un moyen de paiement au sens du CMF (R. Preda, « Les monnaies virtuelles, enjeux de régulation », in A. Blandin-Obernesser (dir.), *Droits et souveraineté numérique en Europe*, Bruylant, 2016, p. 78), l'Allemagne, via le *Bundesanstalt für Finanzdienstleistungsaufsicht*, a pour sa part considéré le Bitcoin comme une unité de change privée (*Rechnungseinheiten*) afin d'en permettre la taxation à hauteur de 25 % au titre des plus-values immobilières.

[27] C'est dans cette limite que la légalité du projet de Sol violette à Toulouse a été confirmée par la Banque de France en 2011.

[28] Ord. CA Paris, 26 août 2011, *SA Crédit Industriel et Commercial c. S.A.S. Maracaja*, n° 11/15269 ; CA Paris, 26 septembre 2013, *SA Crédit Industriel et Commercial c. S.A.S. Maracaja*, n° 12/00161.

[29] La même position a été adoptée par l'autorité de régulation compétente en ce domaine : Autorité de contrôle prudentiel et de résolution (ACPR), « Position relative aux opérations sur bitcoins en France », *Position 2014-P-01*, 29 janvier 2014 (https://acpr.banque-france.fr/fileadmin/user_upload/acp/publications/registre-officiel/ 201401-Position-2014-P-01-de-l-ACPR.pdf).

pas l'ensemble des activités à risque, et d'autre part, elle ne fait pas l'unanimité. La Banque centrale européenne (BCE) comme l'European bank authority (EBA) considèrent par exemple que les activités relatives aux monnaies virtuelles ne sont pas couvertes par les directives relatives aux prestations de service de paiement[30]. Thierry Bonneau émet aussi des doutes quant au bien-fondé de cette solution au regard des opérations effectuées par les plateformes[31] – dont la portée est de toute façon trop incertaine à ce stade contentieux.

Aucune proposition énumérée jusqu'ici ne fait donc l'unanimité, et ce ne sont pas les seules à avoir été formulées. En effet, pour certains auteurs les monnaies virtuelles devraient – par défaut – être considérées comme de simples biens – ce que leur traitement fiscal en France semble par ailleurs confirmer. Mais pour terminer le tour d'horizon des qualifications possibles, il convient d'ajouter que la Cour de justice, raisonnant par analogie, a considéré qu'au regard de la directive TVA les bitcoins sont des devises[32]. L'énumération des options envisagées par la doctrine ou les autorités publiques montrent qu'en la matière c'est bien l'incertitude qui règne. Incertitude d'autant plus grande que le périmètre pertinent de l'interrogation ne peut en réalité se réduire à la France, dans la mesure où les monnaies virtuelles sont a-nationales. Faut-il donc admettre que cet « *objet juridique non identifié* »[33] doit répondre de qualifications différentes non seulement selon les usages dont on voudrait que le droit se saisisse, mais aussi selon l'origine de ce droit ou la nationalité des utilisateurs ?

Présentation

Origine

Il est possible de voir les monnaies virtuelles, telles qu'elles ont été définies en amont, comme le résultat d'un processus allant « *de systèmes fermés de paiement propres vers des univers ludiques aux modes de paiement universels basés sur les devises virtuelles* »[34].

Les jeux vidéo en ligne, reposant sur la création et la vie d'univers numériques, ont en effet constitué une étape particulièrement importante dans le développement de moyens de

[30] Directive n° 2007/64 du 13 novembre 2007, et directive n° 2015/2366 du 25 novembre 2015 concernant les services de paiement dans le marché intérieur.

[31] T. Bonneau, « Le Bitcoin, une monnaie ? », in *Banque et Droit*, 2015, n° 159, p. 8.

[32] CJUE, 22 octobre 2015, *Skatteverket c. David Hedqvist*, Aff. C-264/14.

[33] *Ibid.*, pt. 48 et s.

[34] R. Preda, *op. cit.*, p. 73.

paiement virtuels[35]. Ainsi, *World of Warcraft*[36] ou *Second life* ont constitué des terrains d'expérimentation pour des monnaies virtuelles centralisées[37], fermée ou du moins unilatérale pour le premier (jeton *WoW*) et ouverte pour le second (*Linden Dollar*). Au-delà d'un débat juridico-éthique sur la notion de propriété virtuelle, ces expériences ont donné la possibilité – au moment des différentes crises financières qu'a connues le monde économique à partir de 2007[38] – d'extrapoler et de proposer un nouveau modèle monétaire dégagé de la tutelle étatique avec le *bitcoin*.

Alors que les circonstances de la naissance de cette « *monnaie alternative dérégulée* »[39] attestent de la dimension a-étatique, voire libertarienne[40], des monnaies virtuelles, il semble cependant qu'elles n'ont jamais eu dans l'esprit de leur inventeur pour destinée de se substituer complètement au système traditionnel.

Satoshi Nakamoto[41], son créateur[42], voulait plus simplement offrir à ceux qui le désiraient un instrument de paiement indépendant des politiques monétaires étatiques et du système

---

[35] Voir pour une étude des comportements économiques des utilisateurs de Norrath, le tout premiers univers virtuel créé en 1999 : E. Castronova, « Virtual Worlds: A First-Hand Account of Market and Society on the Cyberian Frontier », *CESifo Working Paper Series No. 618*, 2001 (disponible en ligne : http://papers.ssrn.com/sol3/ papers.cfm?abstract_id=294828).

[36] Il existe, en hongrois, des travaux de recherche doctorale sur ce lien : E. Dániel, *From World of Warcraft to Bitcoin: Analysis of the Status of Individuals, Economy and Property in Virtual Societies from the Point of Civil and Criminal Law* (trad. par l'auteur), 286 p., résumé en anglais p. 239-256 (disponible en ligne : http://ajk.pte.hu/files/file/doktori-iskola/eszteri-daniel/eszteri-daniel-muhelyvita-ertekezes.pdf).

[37] Selon Raruca Preda, la centralisation, sous l'égide des développeurs, des monnaies fut instaurée pour éviter le développement d'un marché noir dans *World of Warcraft* (à propos du développement de ces marchés d'échange parallèles sur Ebay, voir E. Castronova, « Chapter 6 : The Almost Magic Circle », in *Synthetic World. The Business and Culture of Online Games*, The University of Chicago Press, 2005, p. 149 et s. . Le créateur de *Second Life*, Philip Rosedale a pour sa part conçu le *Linden Lab* comme une banque centrale en charge de réguler le cours de la monnaie virtuelle de manière à assurer aux utilisateurs des profits potentiels – et taxables (R. Preda, *op. cit.*, p. 74).

[38] Cette naissance en période de crise n'est pas une donnée propre aux monnaies virtuelles. Le CESE souligne à cet égard qu'il s'agit d'une caractéristique que partage toute création de monnaie nouvelle – ce fut par exemple le cas du *WIR*, créé en Suisse après la crise de 192 – qui interviendra généralement pour faire face à un problème d'hyper inflation de la monnaie souveraine, d'indisponibilité du crédit, du défaut de liquidités, ou encore d'inefficacité du système traditionnel de paiement (P. A. Gailly, « Nouvelles monnaies : les enjeux macro-économiques, financiers et sociétaux », *Avis du CESE, Section de l'économie et des finances*, 2015, p. 18).

[39] N. Clausset et A. Sellem, *op. cit.*, p. 3.

[40] Voir en ce sens, W. Dai, « B-money », 1998 (http://nakamotoinstitute.org/b-money/) où l'auteur se revendique d'un courant « *crypto-anarchique* » : « *in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary* ».

[41] Le projet développé par Satoshi Nakamoto s'appuie pourtant sur les contributions antérieures d'autres programmateurs, au premier rang desquels figurent Wei Dai et Nick Szabo (leurs travaux sont accessibles en ligne à l'adresse suivante : http://nakamotoinstitute.org/literature/ ; voir en particulier, N. Szabo, « Bit Gold », 2005, http://nakamotoinstitute.org/bit-gold/#selection-7.7-11.10) et qui sont associés au mouvement Cypherpunks.

[42] Il s'agit d'un pseudonyme utilisait pour diffuser en 2008 le document « Bitcoin : a Peer-to-Peer Electronic Cash System » *via* une *mailing list* de programmateurs. Depuis 2010, l'alias n'a plus été utilisé pour

bancaire traditionnel[43] – reposant sur l'action conjuguée des banques centrales et des banques privées[44]. Un instrument de paiement rendant inutile la participation et la rémunération de tiers de confiance, qui permettrait grâce à Internet de procéder à des micro-paiements jusqu'alors impossibles en raison des coûts de la médiation des institutions financières[45]. Pour éviter le risque de double-dépense[46], Satoshi Nakamoto propose donc de remplacer ce système reposant sur un tiers de confiance (*Trust*) par un système rendant les paiements identifiables et irréversibles, grâce à l'utilisation de la cryptographie (d'une primitive cryptographique plus exactement) et à l'existence d'un *ledger* (« livre ouvert ») partagé et librement consultable[47]. Dans un tel environnement – une architecture distribuée – la confiance n'est plus institutionnelle, mais intrinsèque. Cette technologie tend par ailleurs à assurer une confidentialité – au moins relative[48] – des paiements et les faibles coûts de transaction.

---

communiquer et l'identité du ou des créateurs restent toujours inconnues (en 2016, l'australien Craig Steven Wright a prétendu être Satoshi Nakamoto toutefois cette affirmation a été récusée rapidement).

[43] Marqueur de cette volonté, un message a été encodé dans le premier block miné par son fondateur faisant allusion aux seconds plans de sauvetage des banques : « *The Times 03/Jan/2009 Chancellor on brink of second bailout for banks* ». Sur l'impact de la crise économique dans le projet de Satoshi Nakamoto, voir Odile Lakomski-Laguerre et Ludovic Desmedt, « L'alternative monétaire Bitcoin : une perspective institutionnaliste », *Revue de la régulation*, 2015, n° 18, § 25 et s. (https://regulation.revues.org/11489#bodyftn15).

[44] Ce substrat idéologique constitue assurément une différence fondamentale par rapport aux projets de création de la « monnaie d'internet » qui, tel que *Beenz*, ont vu le jour à la fin des années 90 pour s'interrompre avec l'éclatement de la bulle internet en 2001 (http://www.theregister.co.uk/2001/08/16/beenz_is_dead_official/ ; http://money.usnews.com/money/personal-finance/slideshows/6-virtual-currencies-that-went-bust).

[45] S. Nakamoto, *Bitcoin : A Peer-to-Peer Electronic Cash System*, 2008, §1 (http://nakamotoinstitute.org/bitcoin/#selection-45.414-45.732).

[46] Il s'agit d'éviter qu'un « *utilisateur puisse "copier" un bitcoin pour le dépenser plusieurs fois*. *Bitcoin apporte une solution innovante : pour pouvoir ajouter un bloc de transactions à la* blockchain*, un "mineur" doit non seulement vérifier la validité de ces transactions, mais aussi trouver la solution à un problème arbitrairement complexe à résoudre mais dont la solution est facile à vérifier. Le premier "mineur" à achever le calcul peut alors inscrire ce nouveau bloc dans la* blockchain*, et recevoir une rémunération, dès lors que les autres "mineurs" ont reconnu l'exactitude de son calcul. Pour tromper le système, un "mineur" malveillant devrait à lui seul trouver en moyenne les solutions à tous les problèmes successifs plus rapidement que l'ensemble des "mineurs" bienveillants réunis. En pratique, le coût serait prohibitif puisque cela nécessiterait de rassembler une puissance de calcul supérieure au reste des utilisateurs* » (N. Clausset et A. Sellem, *op. cit.*, p. 2).

[47] Chaque nouvelle transaction est inscrite dans ce registre, qui peut être consulté à l'adresse suivante : http://blockchain.info/fr.

[48] Si l'ensemble des paiements sont enregistrés et visibles dans le registre ouvert (*ledger*) que constitue la Blockchain, les deux parties à une opération ne sont identifiées que par la clef publique correspondant à leur compte. Il reste toutefois possible avec les *Bitcoins* de retrouver l'identité de ces parties à partir de cette information (F. Reid et M. Harrigan, « An Analysis of Anonymity in the Bitcoin System », *Cornwell University Librairy*, p. 15-25, http://arxiv.org/pdf/1107.4524.pdf). Ce n'est pas le cas de toutes les monnaies virtuelles. Par exemple, *Darkcoin*, devenu *Dashcoin* en Mars 2015, protège totalement l'anonymat en recourant à une sur couche appelée *PrivateSend* puis *Dashsend*. Le même résultat est aujourd'hui proposé par plusieurs extensions (« *cryptocurrency mixing services* »), tel que *Zerocoin* devenu *Zerocash*, qui sans être une monnaie autonome transforment des bitcoins en des « jetons » anonymes le temps d'effectuer les transactions voulues (pour plus de détails, voir E. Ben Sasson e.a., « Zerocash : Decentralized Anonymous Payments from Bitcoin », 56 p., disponible en ligne : http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf).

Dans un premier temps, le *bitcoin* reste une invention relativement confidentielle. Après le minage du premier bloc le 3 janvier 2009, et la première transaction entre Satoshi Nakamoto et Hall Finney le 12 janvier, il faut attendre mars 2013 (au moment de la crise chypriote) pour voir le cours de change décoller. Il passera alors de 0,001 – sa valeur initiale – à plus de 100 dollars[49].

Technologie[50]

Les monnaies virtuelles peuvent apparaître à première vue comme un ensemble hétéroclite sur le plan technologique en raison du développement d'une multitude d'espèces différentes[51]. Toutefois, ce développement c'est fait sous la forme d'un foisonnement dont le *bitcoin* et son programme open-source constituent la branche originelle. En conséquence, malgré des variations multiples dans les détails du fonctionnement, les monnaies virtuelles reposent sur un certain nombre de caractéristiques communes. Par ailleurs, le choix de s'intéresser à celles qui fonctionnent dans un circuit ouvert et qui sont à flux bidirectionnel réduit l'intérêt des divergences techniques et l'on s'intéressera pour l'essentiel aux principes structurels sur lesquels repose le caractère disruptif de telles monnaies virtuelles. Ces principes, qui sont la transparence et la confiance distribuée, sont donc à l'origine des modalités techniques fondamentales régissant le fonctionnement des monnaies virtuelles[52]. Ils sont en quelques sortes les valeurs à partir desquelles ont été designées les caractéristiques destinées à garantir la confiance intrinsèque et à un offrir un outil de « *désintermédiation* »[53].

---

[49] Le 10 juin 2011, la parution des premiers articles dans les médias est à l'origine d'une première bulle spéculative, durant laquelle la valeur du bitcoin passe de 1 à 28 dollars. La crise chypriote fera grimper celle-ci à 248 dollars le 9 avril 2013 avant qu'il ne retombe à seulement 38 dollars le 11 avril ! On notera aussi comme date importante, le 28 novembre 2013 où le cours atteindra les 1 000 dollars et où plus de 100 000 transactions auront été effectuées.

[50] Sur l'ensemble des aspects techniques, on consultera avec profit l'ouvrage réalisé par les membres de Princeton Université : A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, « Bitcoin and Cryptocurrency Technologies. A comprehensive Introduction », 2016, Princeton University Press, 336 p. (draft disponible à l'adresse suivante :

[51] Une approche quantitative amène cependant à relativiser cette diversité, puisqu'aujourd'hui les seules monnaies virtuelles ayant une capitalisation significatives sont Bitcoin et Ethereum. Ripple, Litecoin, Steem, Ethereum Classic et Dash, qui sont les plus importantes parmi celles qui restent, ne dépassent pas les 220 000 dollars et n'ont pas toutes adopté un fonctionnement décentralisé.

[52] Pour J. Bonneau e.a., les principales caractéristiques du Bitcoin sont d'être un registre de transactions, un protocole de consensus, et un réseau de communication (« SoK : Research Perspectives and Challenges for Bitcoin and Cryptocurrencies », *2015 IEEE Symposium on Security and Privacy*, 2015 p. 2 et s., disponible en ligne : http://www.ieee-security.org/TC/SP2015/papers-archived/6949a104.pdf).

[53] Pour reprendre la formule de J. Bonneau e.a., *op. cit.*, p. 15 : les auteurs soulignent que la possibilité de se passer de tiers de confiance dépasse la question de la réalisation d'un paiement sécurisé pour englober des hypothèses variées tels que la réalisation de paiements conditionnels, des conversions automatisées de crypto-devises, des dépôts de garanties, ou encore l'établissement de la fiabilité d'une partie contractante.

Concrètement, le système repose sur un réseau de pair à pair (*Peer-to-Peer* ou *P2P*) dans lequel il n'y a pas de serveur ou de nœud central[54], mais où chaque participant est censé supporter le réseau en partageant directement l'information détenue sur son installation informatique[55]. En conséquence, tout utilisateur de monnaie virtuelle doit normalement posséder un exemplaire du logiciel commun et une version à jour du registre des transactions.

C'est grâce à cette décentralisation de l'information que fonctionne le mécanisme de consensus inventé pour valider les transactions en absence d'autorité centrale jouant le rôle de tiers de confiance. Le système repose donc sur le fait que l'ensemble des participants possèdent en mémoire l'ensemble des messages relatifs aux transactions déjà émises et sont d'accords pour reconnaître une nouvelle transaction comme valide au regard des informations qu'ils possèdent[56]. Ainsi si Alice veut envoyer à Bob une certaine somme (au minimum un Satoshi, c'est-à-dire un cent millionième [$1e^{-8}$] de bitcoin), elle enverra un message décrivant qui elle est, à qui et combien elle veut envoyer de l'argent. Afin de valider la transaction, les membres du réseau vérifieront si l'historique des transactions réalisées depuis l'origine (*Genesis Block*) permet d'établir qu'Alice à bien en sa possession la somme requise. Le mécanisme de consensus empêche Alice d'envoyer simultanément les mêmes bitcoins à différents destinataires. Le système prévient donc le double-paiement grâce à la non-fongibilité des unités de monnaie et à la validation par l'ensemble des participants (qui sont autant de nœuds du système) de chaque opération. Pour des raisons de sécurité, ce processus de consensus repose également sur l'utilisation d'un procédé cryptographique (on parle de primitives cryptographiques) destinée à vérifier que la demande a bien été émise par Alice. On parle de transaction *pay-to-pub-key-hash*.

Sur le réseau bitcoin, aucune donnée n'est pourtant chiffrée – conséquence de l'exigence de transparence. Le registre des transactions est donc librement consultable pour qui est capable d'en comprendre le langage. La cryptographie n'intervient que pour deux choses,

---

[54] Il existe cependant des nœuds permanents, appelés « *seed nodes* », dont l'adresse IP est communiquée aux nouveaux entrants, et qui sont dédiés au téléchargement des données nécessaires à l'installation de la Blockchain.

[55] L'information est partagée de façon à optimiser le flux de la manière suivante : « *New blocks and pending transactions are broadcast to the entire network by flooding. Nodes send INV messages to all of their peers containing the hashes of new blocks or pending transactions whenever they first hear of them. Peers can respond by requesting the full contents of these blocks or transactions if they have not yet seen them (*via *a GETDATA message). By default nodes will only forward new data once, preventing infinite propagation; only relay transactions and blocks that are valid; only relay the first block they hear of when two blocks are found in a temporary fork; and will not broadcast pending transactions which conflict (double-spend) with pending transactions they have sent* » (J. Bonneau e.a., *op. cit.*, p. 5).

[56] Pour certains observateurs, Bitcoin se réduit à ce registre distribué sur lequel sont inscrites les transactions sous forme de tableaux d'entrées et de sorties communiqués par message hachés (*ibid.*, p. 3).

premièrement « *pour créer des signatures non falsifiables* » et ainsi pouvoir certifier l'identité des parties dans une transaction, deuxièmement pour « *implémenter des fonctions à sens unique* »[57] rendant infalsifiable l'horodatage et le contenu des blocs intégrés à la Blockchain. La cryptographie à laquelle recourt le protocole doit donc simplement permettre d'établir la confiance dans le système, et n'est pas destinée à rendre anonymes les échanges. Elle recourt à l'algorithme de hachage SHA-256.

Sur le premier point, la suppression des tiers de confiance imposait effectivement de trouver le moyen de pouvoir prouver, à l'ensemble des participants du réseau, son « identité » et la possession des unités de monnaie pour effectuer une transaction[58] (ce que l'historique de la Blockchain permet de vérifier). La solution trouvée repose tout d'abord sur la discrimination entre les informations à diffuser et celles qui doivent rester secrètes : il s'agit de la clef publique (ou adresse publique[59]) et de la signature digitale des parties à la transaction d'une part, et de la clef privée d'autre part. Grâce à un algorithme de vérification, le réseau va pouvoir vérifier facilement l'authenticité de la signature digitale[60], c'est-à-dire le fait que l'émetteur de la transaction possédait bien au moment de l'opération la clef privée associée aux *bitcoins* dont le transfert est demandé. La signature est unique, et elle changera pour chaque nouvel ordre de paiement. L'intérêt d'utiliser la cryptographie lors de l'envoi d'une transaction est de mettre en œuvre un processus à sens unique : alors qu'une signature digitale

---

[57] S. Mignot, « Le Bitcoin : nature et fonctionnement », *Banque & Droit*, 2015, n° 159, p. 11.

[58] L'identité ne doit pas être entendue au sens de l'état civil, elle est simplement la qualité de celui qui sera reconnu, par le processus de consensus, comme en capacité d'utiliser un certaine somme de Bitcoin. Techniquement, *« [o]wnership simply means knowing a private key which is able to make a signature that redeems certain outputs—an individual owns as many bitcoins as they can redeem. Public key hashes, as specified in pay-to-pub-key-hash transactions, effectively function as pseudonymous identities within the system and are referred to as addresses. No real-world name or identifying information are required* » (J. Bonneau e.a., *op. cit.*, p. 3).

[59] En réalité, l'adresse publique est générée à partir de la clef publique et adopte un format plus simple afin de pouvoir plus aisément la préciser dans le message qui décrira la transaction à opérer.

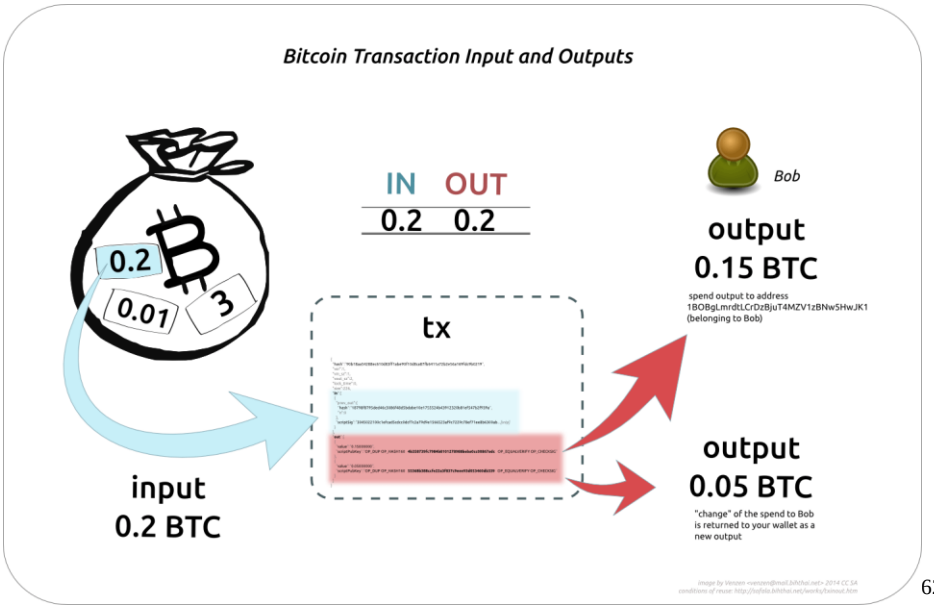
[60] G. Marin-Dagannaud, « Comprendre la blockchain Ethereum – Article 1 : Bitcoin, première implémentation de la blockchain (1/2) », 3 juin 2016 (https://www.ethereum-france.com/comprendre-la-blockchain-ethereum-article-1-bitcoin-premiere-implementation-de-la-blockchain-12/) : « *De manière synthétique, la signature digitale est une fonction* F *prenant en paramètre la clé privée de l'émetteur (*p*) et le message émis (*m*). Pour vérifier si la signature est valide, chaque nœud applique une autre fonction* V *prenant en paramètre l'adresse publique de l'émetteur (*a*), le message (*m*) et la signature digitale (*s*), et qui renvoie vrai ou faux. Il est important de noter que la fonction* F *est à sens unique, de sorte qu'il est impossible de deviner la clé privée à partir de la signature. Cela implique également une interdépendance entre la signature et le message :* F *donnera toujours la même signature pour un message et une clé privée donnés, mais le moindre changement de l'un des deux paramètres aura pour effet d'altérer radicalement la signature. Ainsi, une signature digitale ne pourra jamais être réutilisée. Cela empêche également les nœuds qui relaient la transaction de la modifier au passage. En effet, si l'intégrité du message est corrompue (*m *devient* m*'),* V *renverra faux car le message en entrée n'est plus le même que celui qui avait été passé en paramètre de* F ».

est générée systématiquement à partir de la clef privée[61], il est impossible de retrouver cette dernière à partir de la première. Ceci permet d'utiliser sa clef privée – et de prouver que l'on a bien utilisé cette clef –, tout en évitant d'avoir à la communiquer au réseau et de risquer ainsi d'être détroussé de ses bitcoins.

Une fois l'identité établie, il faut encore pouvoir vérifier que le « compte » est « crédité » (et que son détenteur ne procède pas à un double paiement avec les unités de monnaie qu'il possède). Pour ce faire, bitcoin a écarté la solution adoptée par les banques traditionnelles, c'est-à-dire l'enregistrement en continu de la balance des comptes (mais ce n'est pas une caractéristique partagée par toutes les monnaies virtuelles, et parmi les contre-exemples on compte Ether, son principal concurrent sur le marché actuel, puisqu'Ethereum fonctionne grâce à plusieurs serveurs centraux). Dans un système décentralisé, et étendu sur le monde entier, ce mécanisme était en effet inadapté. C'est la Blockchain qui permet de résoudre cette difficulté. Au moment où la demande de transaction est formée, un nœud va vérifier les « sorties de transaction non dépensées » (*Unspent Transaction Output* ou UTXO) associées au compte en remontant l'ensemble de la chaîne des transactions.

Exemple : *Ainsi, si Alice possède 10 bitcoins, son compte est composé de la manière suivante : UTXO A(n) + UTXO B(n) + etc.* (*chaque UTXO correspondant à un montant positif de bitcoin).*
Si elle souhaite envoyer 1 bitcoin à Bob, alors le UTXO A(n) qui jusqu'alors avait une valeur de 2 – ce que l'on sait en observant l'ensemble des transactions antérieures jusqu'à (n) – va pouvoir être utilisé : il sera entièrement dépensé, une partie revenant à Bob et l'autre retournant au compte d'Alice. Une fois le paiement effectué, il deviendra UTXO A(n+1) et aura une valeur de 1 bitcoin. En faisant la somme des UTXO associés au compte d'Alice, il apparaîtra alors qu'elle a un « solde » virtuel de 9 bitcoins.

[61] Il en va d'ailleurs de même pour la clef publique, qui elle aussi est issue de la clef privée. Cette dernière est choisie par l'utilisateur (parmi les 2^{160} combinaisons possibles) au moment de son entrée dans le système, et elle ne peut être générée par celui-ci afin que personne d'autre que son propriétaire ne puisse en avoir connaissance.



62

L'avantage d'un tel système est que « *[l]a chaîne de transaction a une propriété fondamentale : une transaction peut référencer de multiples UTXOs en entrée et en sortie, mais un UTXO spécifique ne peux être utilisé qu'une fois en tant qu'entrée. Cela permet d'empêcher que la même somme d'argent ne soit dépensée deux fois. Les UTXOs sont stockés dans une base de données dont chaque nœud possède une copie. À chaque transaction validée, la base de données est mise à jour* »[63].

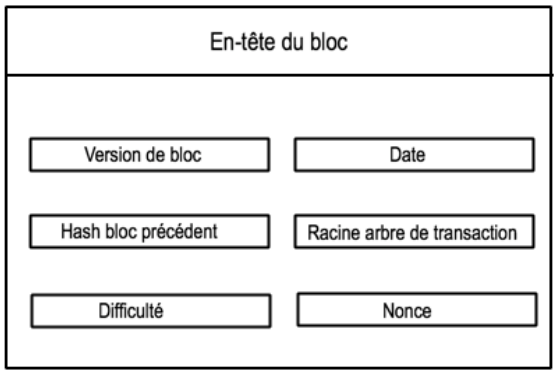
Système d'échange et de paiement, bitcoin est aussi un mécanisme de création monétaire. Sur ce point, il met en présence deux types d'utilisateurs. Tout d'abord les utilisateurs « simples », qui se contentent de recourir à l'infrastructure pour effectuer des transactions avec les *bitcoins* qu'ils ont soit achetés *via* une plate-forme d'échange, soit obtenus au moment de la vente d'une marchandise ou d'un service. Ensuite, un second groupe d'environ 6000 utilisateurs participe activement au fonctionnement de l'infrastructure. Ce sont les mineurs, dont le travail permet de vérifier la validité des transactions grâce au mécanisme de consensus et de construire ainsi la Blockchain par l'ajout de nouveaux blocks.

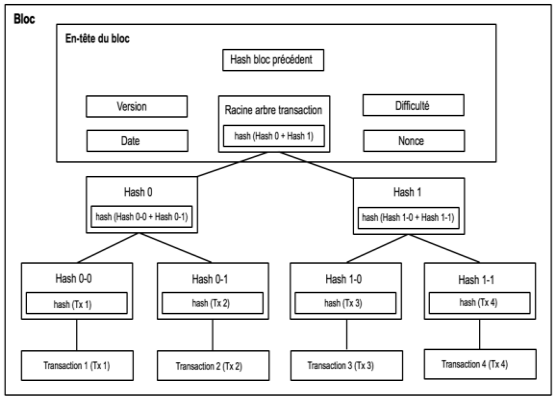
Le processus de construction de la chaîne de block met en concurrence l'ensemble des mineurs de la manière suivante. Les nœuds emmagasinent les transactions en attente de validations. A partir du dernier block existant sur la Blockchain, un mineur va agréger les transactions qu'il aura vérifiées puis s'attaquer à la résolution du problème mathématique imposé par la *proof of work* pour la constitution de l'en-tête du nouveau bloc. C'est en effet la

[62] Source : ©Shutterstock (https://www.cryptocoinsnews.com/bitcoin-transaction-really-works/)
[63] G. Marin-Dagannaud, *op. cit.*

résolution de ce problème qui conditionne sa validation par le système et *in fine* l'attribution d'une récompense[64].

Composition de l'en-tête d'un bloc et d'un bloc[65] :





Le problème mathématique consiste à trouver un *nonce* dont la valeur du hash (une fois appliquée la fonction SHA-256) soit inférieure au seuil défini par le système en fonction du niveau de difficulté voulu (et comme pour la signature digitale, l'algorithme utilisé empêche de partir de la valeur demandée pour trouver un nonce satisfaisant la *proof of work*). Le hash est écrit en hexadécimal et comporte 64 chiffres qui sont donc compris entre 0 et 15. Sa valeur en base décimale est déterminée de la manière suivante : « *il faut multiplier chaque chiffre par* 16^i*, i étant la position du chiffre dans le hash, en partant de la droite et à partir de 0. Exemple :* $2ba5 = 2*16^3 + 11*16^2 + 10*16^1 + 5*16^0 = 8192 + 2816 + 160 + 5 = 11\ 173$ »[66].

Plus le niveau de difficulté sera élevé, plus il imposera de trouver un hash dont la valeur soit basse. Pour remporter la récompense, un mineur doit être le premier à trouver un nonce dont le hash remplira cette exigence. Dans ce système, les chances de succès sont donc proportionnelles à sa puissance de calcul[67].

---

[64] Voir pour une présentation des rares expérimentations fondées sur un système de *proof of stake* : L. Lee, (« New Kids on the Blockchain : How Bitcoin's Technology Could Reinvent the Stock Market », *Hastings Business Law Journal*, 2016, Vol. 12, n° 2, p. 109-116 (disponible en ligne : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2656501=).

[65] Source : G. Marin-Dagannaud, « Comprendre la blockchain Ethereum – Article 1 : Bitcoin, première implémentation de la blockchain (2/2) », 13 juin 2016 (https://www.ethereum-france.com/comprendre-la-blockchain-ethereum-article-1-bitcoin-premiere-implementation-de-la-blockchain-22/).

[66] *Id.* : « *Un hash est composé de 64 chiffres, sa valeur est donc majorée par* 16^{64}*. Le seuil fixe une limite inférieure à* 16^{64}*, afin que la recherche de hash ne soit pas triviale (en d'autres termes, qu'elle demande un effort de calcul à l'ordinateur). Par exemple, si on place un seuil à* 16^{58}*, l'ordinateur devra calculer des hash en incrémentant le nonce à chaque échec, jusqu'à en trouver un inférieur à* 16^{58} ».

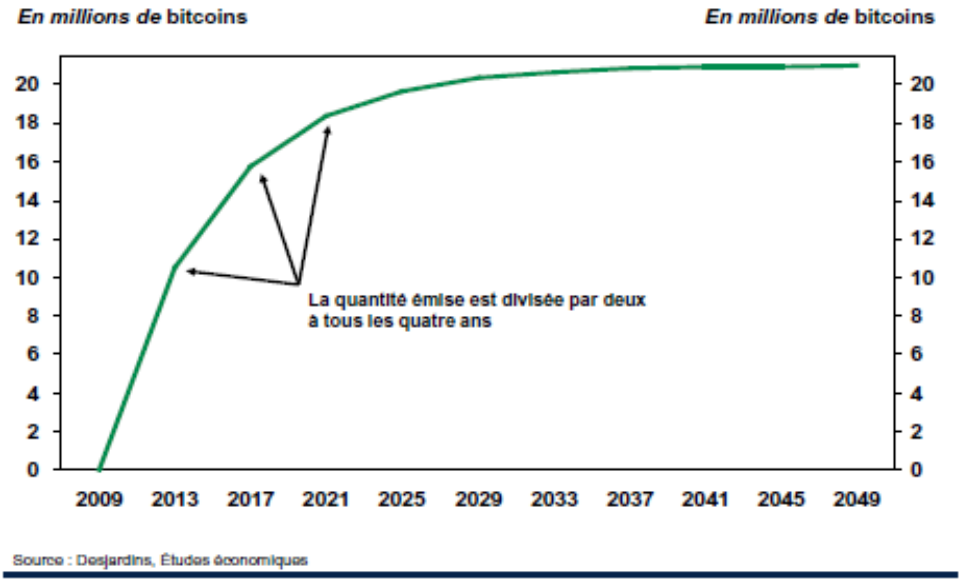
[67] J. Bonneau e.a., *op. cit.*, p. 4-5.

En raison de la structure décentralisée, il existence un temps de latence de 12,6 secondes en moyenne entre la découverte d'un nouveau bloc et sa prise en compte par l'ensemble des nœuds. Il n'est donc pas impossible que deux mineurs trouvent au même moment un nouveau bloc, satisfaisant au niveau de difficulté exigé mais regroupant des transactions différentes. Dans cette hypothèse, la Blockchain se divise momentanément et les mineurs travaillent sur l'une ou l'autre des versions, jusqu'à ce que l'une des branches soit plus longue que l'autre. A ce moment là, la seconde sera effacée et les transactions présentes sur celle-ci ne seront plus considérées comme validées. A court terme, l'unité de la chaîne de bloc est donc toujours maintenue.

La participation des mineurs doit donc être récompensée, puisque c'est leur investissement qui permet au réseau de fonctionner. Le minage leur permet d'acquérir des *bitcoins* sans avoir à les acheter, avec ce système de rémunération destiné à compenser les dépenses élevées requises par les opérations de hachage (équipement informatique spécifique [carte ASIC créée spécialement pour obtenir un « *Hashrate* » élevé] et facture énergétique).

Toutefois, l'offre de monnaie est limitée dans le cas du *bitcoin*. Le monnayage y relève d'un schéma prédéterminé : il est conçu comme un mécanisme temporaire dans la mesure où la production ne doit pas dépasser 21 millions d'unités. Pour ce faire, la récompense attribuée au mineur ayant proposé un nouveau block est divisée par deux tous les 210 000 blocs (soit à peu près tous les quatre ans).

Graphique 1 – Progression programmée de la quantité de *bitcoins*



Source : Desjardins, Études économiques

Le second « *Halving* » (division par deux du nombre de *bitcoins* émis en récompense du minage) a eu lieu le 9 juillet 2016. Depuis le 28 novembre 2012, la récompense était de 25 *bitcoins* et passe donc à 12,5 (l'évènement est concomitant à une légère baisse du cours). Une fois le volume maximum d'unités atteint, il faudra donc passer à un nouveau système de rémunération des mineurs[68], certainement fondé sur des frais de transactions qui risquent d'exploser au fur et à mesure que le nombre d'utilisateurs croîtra[69] (et de détruire *in fine* ce qui fait l'intérêt des monnaies virtuelles ?) – car proposer un *fee* élevé sera la garantie de voir sa transaction validée rapidement. Pour éviter ce risque, et plus largement pour garantir une croissance harmonieuse des paiements virtuels, doit être trouvée une solution permettant de réduire le coût technique du maintien du système et/ou d'accroître sa rentabilité en termes de capacité de transaction.

Bitcoin connaît, en effet, un problème technique vital pour son avenir. Celui de la scalabilité, qui touche à la question de savoir comment accroitre les capacités opérationnelles du système tout en garantissant le bon fonctionnement du mécanisme de consensus décentralisé. En clair, c'est la rapidité de validation des transactions qui est l'enjeu majeure des prochains mois[70]. En l'état de son fonctionnement, la diffusion du *bitcoin* connaît plus précisément deux obstacles techniques majeurs : un nombre de transactions maximum qui est largement inférieur aux systèmes de paiement traditionnel, et une taille croissante de la Blockchain[71].

---

[68] Jusqu'à présent les frais de transaction restent marginaux, et relève d'une forme de bonne pratique librement adoptée par les utilisateurs. Selon Fabienne Pinos, « *Entre le 3/01/2009 et le 3/10/2015, les frais moyens par transaction ont oscillé entre 0 et 0,07 BTC soit entre 0 et 0,6 USD* » (« Monnaies virtuelles et intérêt général : quelles perspectives de convergence ? », draft disponible à l'adresse suivante : https://www.dropbox.com/s/vhxmw4y06u9xssu/2016_03_Projet_Article%202_%20F%20PINOS.pdf?dl=0). Toutefois, la saturation du réseau pousse ces derniers à accorder plus systématiquement une récompense au mineur qui validera leur transaction (techniquement, il suffit de ne pas indiquer d'adresse où renvoyer les UTXO excédentaires une fois le paiement effectué), au risque sinon de ne pas voir leur message traiter suffisamment rapidement.

[69] La hausse des coûts de transaction va être nécessaire au fur et à mesure que la rétribution des mineurs va baisser, alors que la sécurité du système repose sur la capacité de l'ensemble des mineurs à s'équiper des outils informatiques les plus performants (au risque sinon de laisser un groupe particulier prendre le pouvoir sur la Blockchain (N. Clausset et A. Sellem, *op. cit.*, p. 3). Pour se maintenir dans cette course à l'équipement les mineurs n'auront pas d'autre choix que de se rémunérer sur les utilisateurs.

[70] N. Godlove, *op. cit.*, p. 21 : « *Bitcoin is far less efficient than our current banking and credit card system for most trades. No transfer can take place without the brute force computations to verify the transfer, which means they must always take more time than a single-point transfer will. Lowering the time it takes to make such a transfer would be untenable, as it would open the Bitcoin up to several vulnerabilities that would render them useless* ».

[71] Elle dépasse les 75 Go depuis le 10 juillet 2016. La longueur de la chaîne est une garantie contre toute tentative de falsification, c'est pourquoi elle est conservée dans son intégralité dans chacun des nœuds du système. En raison du fonctionnement distribué, pour pouvoir modifier cette chaîne à son profit, il faudrait être capable de créer une chaîne plus « longue ». Puisque le système impose aux mineurs de travailler sur la chaîne ayant la valeur computationnelle la plus grande, il faudrait donc que cet attaquant soit capable d'atteindre et de dépasser la puissance de calcul cumulée depuis l'origine du Bitcoin.

Selon les données disponibles, la validation d'une transaction demande aujourd'hui une dizaine de minute (ce qui correspond au délai de création d'un nouveau bloc[72], induit par le niveau de difficulté de la *proof of work*[73] – une heure est même nécessaire pour que l'opération soit considérée comme irréversible, c'est-à-dire comme ayant une profondeur suffisante dans la chaîne[74]), et la capacité d'enregistrement du système est volontairement limitée à sept transactions par seconde (contre un maximum théorique de 56 000 pour visas et une moyenne de 2 000 transactions par second en pratique). « *Le temps de validation est une vraie problématique de la Blockchain appliquée au monde réel. Les deux principes de "*Proof of work*" et de profondeur de bloc nécessaires pour s'assurer que la transaction ne peut être renversée rendent ce temps incompressible dans une implémentation comme celle du Bitcoin* »[75].

L'une des solutions envisageable, développée sous le nom de *Bitcoin XT*, par Mike Hearn et Gavin Andresen, consistait à augmenter massivement la taille des blocks au-delà des 1 Go actuels (ce qui permettrait d'enregistrer toutes les dix minutes davantage de transactions). Cette proposition (« *bitcoin improvement proposal* » ou *BIP*) a cependant été écartée par la communauté, qui craignait que cela ne réduise le nombre d'acteurs en capacité technique de participer au minage en raison des disparités mondiales dans l'accès à Internet[76]. Une autre possibilité est offerte par l'*add-on* Lightining Network[77]. Cette surcouche permet, lorsque des parties opèrent de multiples transactions entre-elles de ne pas procéder à leur enregistrement

---

[72] Ce délai de dix minutes a été choisi dans le système Bitcoin pour éviter la récurrence des *forks* qui se produisent lorsque deux blocs sont minés en même temps. Cette « sécurité » n'est pas systématique. Litecoin par exemple permet un minage beaucoup plus rapide des nouveaux blocs (et le nombre d'unités qui seront produites à terme est également quatre fois plus important).

[73] La difficulté de la preuve de travail est ajustée par le système tout les 2016 blocks afin de maintenir cet intervalle.

[74] En réalité, ce délai de dix minutes est insuffisant pour garantir de manière absolue la transaction, car le registre distribué est susceptible d'enregistrer deux nouveaux blocs simultanément en raison de la multiplicité des mineurs. Il se crée alors ce que l'on appelle un *fork* : la chaîne des transactions se divise en deux branches qui continuent de croître séparément. Toutefois le protocole a prévu une contre-mesure pour éviter la persistance de cette divergence, en ne laissant survivre que la branche la plus longue – celle qui se développera le plus rapidement. La première des deux fourches qui aura un bloc de plus sera considérée comme la branche valide. Les transactions inscrites dans le ou les blocs abandonnés seront alors effacées et devront être relancées pour intégrer la chaîne survivante. On considère qu'un délai d'une heure est en pratique nécessaire pour obtenir la certitude que le paiement est devenu irréversible. La transaction aura en effet une « profondeur » suffisante dans la chaîne, puisqu'il devient mathématiquement improbable que les deux *forks* se soient développées simultanément au-delà de six blocks à partir de la divergence.

[75] K. Palop, « Le temps de validation de la transaction et la sacabilité du système », *Les défis de la Blockchain dans le monde réel – Partie 2*, 5 avril 2016 (http://www.arsiamons.fr/dossier-blockchain-partie-2-defis-de-blockchain-monde-reel-23/).

[76] Les mineurs chinois qui ne bénéficient pas d'un débit Internet suffisant serait particulièrement handicapé dans cette hypothèse.

[77] J. Poon et T. Dryja, « The Bitcoin Lightning Network : Scalable Off-Chain Instant Payments », 14 janvier 2016, 59 p. (https://lightning.network/lightning-network-paper.pdf).

systématique sur la Blockchain (on parle d'opération *trustless*), mais d'inscrire dans cette dernière le solde selon une temporalité déterminée. Dans une logique similaire, le projet *Rootstock* propose de faire fonctionner une *side-chain* en dehors du système de consensus décentralisé en se servant de *bitcoins* comme dépôt de garantie.

Enfin, certains développeurs proposent de couper la chaîne, pour ne pas imposer la reprise de l'ensemble de l'historique des transactions, quand d'autres encore pensent qu'il sera possible de l'alléger grandement avec les progrès des algorithmes de hachage et qu'il n'est donc pas nécessaire dans l'immédiat d'intervenir.

La solution qui semble se dessiner est l'adoption de *Segregate Witness*, un nouveau protocole qui actuellement testé et qui pourrait être adopté lors d'un *hard fork*[78]. Il permettrait, notamment, en séparant les informations relatives à l'identification des signatures de celles relatives à la transaction proprement dite, d'accroitre légèrement la capacité de stockage des blocks tout en réduisant les besoins de bande passante pour le transfert d'informations entre les nœuds du réseau.

L'évocation de l'évolution à venir du système appelle une remarque sur les conditions dans lesquelles le code peut être modifié. Toute proposition de modification doit rencontrer un consensus suffisant pour s'imposer[79]. En pratique, la différence de positions parmi les mineurs peut être à l'origine de *forks* (il ya en conséquence dans la chaîne des blocs répondant à des protocoles différents, mais compatibles, qui sont le fruit de ces *soft forks*), voire de la création de nouvelles monnaies dérivées du système originel que l'on nomme *Altcoins* (comme *Litecoin* par exemple). Ceci montre que les monnaies virtuelles décentralisées peuvent connaître des problèmes importants de gouvernance[80].

---

[78] A la différence des *soft fork*, qui sont simplement adoptés par la majorité des mineurs et qui permettent aux utilisateurs de l'ancienne version de continuer à utiliser la Blockchain, un *hard fork* implique l'adoption par l'ensemble des utilisateurs du nouveau code : une transaction opérée sous l'ancienne version ne sera pas reconnue par les mineurs et ne pourra pas intégrer un nouveau bloc. Le premier *hard fork*, appelé *BIP 16*, fut adopté le 15 février 2012.

[79] Sur les difficultés à atteindre ce consensus en raison des divergences qui opposent les « *Bitcoin Core developers* » (dont la liste est disponible à l'adresse suivante : https://bitcoin.org/fr/developpement) sur les évolutoins à apporter au code originel, voir B. Reutzel, « Is Bitcoin For the Masses or Against the State ? », 21 janvier 2016 (http://www.coindesk.com/is-bitcoin-for-the-masses-or-against-the-state/).

[80] N. Clausset et A. Sellem, *op. cit.*, p. 3 : « *Jusqu'à présent, le protocole* open source *est géré par la* Bitcoin Foundation*, porte-parole autoproclamé de la communauté Bitcoin. Si elle a dans un premier temps joué un rôle prépondérant pour le développement informatique et les actions de promotion, sa réputation a été entachée depuis fin 2013 par une série de scandales, parmi lesquels la condamnation d'un membre du* board *pour blanchiment d'argent, et par de récentes rumeurs sur une situation financière proche de la faillite* ». Sur les liens entre l'architecture des systèmes informatiques et les questions de gouvernance, voir P. De Filippi, et

S'agissant du bitcoin, son succès est la source d'un dissensus entre les « *core developpers* », qui ont plus ou moins officiellement repris la main après le départ de Satoshi Nakamoto, ce qui montre les limites d'une gouvernance décentralisée lorsque le système rencontre le besoin d'évoluer. La transparence des interventions et la régularité du processus de délibération ne sont aucunement garanties. Mike Hearn, qui fut à l'origine du projet *Bitcoin XT* – destiné à modifier le protocole originel par un accroissement de la taille des blocks, afin de garantir un temps de validation des transactions raisonnable –, a ainsi cessé toute participation dans le projet bitcoin en accusant les tenants de *Bitcoin Classic* de non seulement l'avoir censuré sur les espaces de discussion, mais d'avoir attaqué tout système informatique utilisant sa version du protocole[81].

L'idéal d'un système ouvert et décentralisé est également « dévoyé » par le constat que tous les participants ne jouent pas le même rôle à raison de leur degré d'implication variable, et que tous n'accèdent pas de la même façon au système *bitcoin*. En principe, dans la logique originelle, chaque ordinateur constitue un nœud équipollant du système décentralisé (et devrait donc avoir droit à une voix dans le processus décisionnel[82]) – même s'il ne participe pas nécessairement au minage.

En pratique, la longueur de la chaîne actuelle implique qu'il n'est plus possible pour tous les utilisateurs, ni pour tous les supports (on pense en particulier à l'utilisation sur smartphone), d'en conserver un exemplaire complet et de faire fonctionner *Bitcoin core*. Se développent alors dans le système des nœuds légers (*light nodes*) et des nœuds lourds (*full nodes*). Les premiers ne conservent de la chaîne que ce qui permet d'authentifier une transaction (c'est-à-dire de vérifier qu'elle a été introduite dans un bloc ayant une profondeur suffisante) et recourt au protocole appelé *Simple Verification Payment* (*SVP*). Cette possibilité est ouverte grâce au « *concept d'*arbre de Merkel » (*Merkel Tree*), que l'on retrouve dans les blocs et qui permet « *dans ces structures mathématiquement liées [comme la Blockchain qui résulte d'opérations de hachage], de pouvoir identifier une modification de l'intégrité d'un tout selon ses parties* »[83]. En clair, la modification d'une transaction retranscrite dans les

---

D. Bourcier, « Réseaux et gouvernance. Le cas des architectures distribuées sur internet », *Pensée plurielle*, 2014/2, n° 36, p. 37-53, spé. p. 41 et s.

[81] M. Hearn, « The resolution of the Bitcoin experiment », 14 janvier 2016 (https://medium.com/@octskyward/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.6u2n6v46w).

[82] En fonction de la version du logiciel bitcoin installée, un utilisateur pourrait témoigner son accord ou son désaccord lorsqu'un *BIP* est présenté à la communauté.

[83] K. Palop, « Le poids de la Blockchain », *Les défis de la Blockchain dans le monde réel – Partie 2*, 5 avril 2016 (http://www.arsiamons.fr/dossier-blockchain-partie-2-defis-de-blockchain-monde-reel-23/).

« feuilles » de l'arbre de Merkel serait identifiable en examinant seulement les « racines », les *Merkel roots*, présentent dans l'en-tête du bloc. Il est ainsi possible de vérifier l'intégrité d'une transaction (c'est-à-dire son appartenance à un bloc, qui appartient lui-même à la Blockchain) sans posséder la Blockchain dans sa totalité.

Toutefois, cela suppose l'existence dans le système de nœuds lourds, qui deviennent des points de concentration dans un réseau supposé être *Peer-to-Peer*. Même les plateformes proposant les portefeuilles électroniques, qui permettent aux usagers *lambda* d'utiliser la monnaie virtuelle sans avoir à investir lourdement dans un équipement informatique, sont parfois des nœuds légers (on parle de *SPV-clients*). Lorsque ces nœuds légers voudront effectuer une transaction, le protocole *SVP* sollicitera les informations nécessaires à la certification de l'opération auprès des *full nodes*. La multiplication de ces nœuds légers est de nature à affaiblir la sécurité du système, dès lors qu'ils ne participent pas réellement au mécanisme de confiance décentralisée. Corrélativement les nœuds lourds apparaissent comme des points de centralisation dans le système, dont en pratique les voix sont les seules à compter lorsqu'une modification du logiciel est envisagée.

Ce fonctionnement, vital pour que les monnaies virtuelles constituent un système de paiement à dimension « universelle », est de nature à minimiser voire à anéantir l'influence que peut penser avoir un utilisateur individuel et anonyme sur les mécanismes de gouvernance. Il devient moins un participant qu'un usager du réseau[84] (selon Vitalik Buterin[85], cette situation de dépendance des plus « petits » serait même aggravée dans un environnement fondé non plus sur la *proof of work* mais sur la *proof of stake*[86]) et perd ainsi sa qualité

[84] Etant un « client léger », l'usager ne participe pas au processus de minage. Or, lorsqu'il faut voter pour valider ou rejeter une évolution du protocole, c'est par le biais de « tags » intégrés dans les blocks minés que les positions sont exprimées.

[85] V. Buterin, «Light Clients and Proof of Stake » (https://blog.ethereum.org/2015/01/10/light-clients-proof-stake/).

[86] Voir, sur les variations possibles de *Proof of Stake*, J. Bonneau e.a., *op. cit.*, p. 13. Dans un système de *Proof of Stake*, explique Kévin Palop (*op. cit.*) « *[l]'idée est de fonder la répartition aléatoire du droit à validation d'un bloc, non plus une course à la résolution d'un puzzle mathématique, mais sur la preuve d'engagement économique de chaque mineur* ». Bien que mon énergivore, la viabilité de ce système fait débat – il n'a pour l'heure été adopté que par des monnaies virtuelles marginales, car « *l'une des problématiques principales liées à la* "Proof of Stake" *dans une implémentation où les mineurs élisent un collège de potentiels validateurs (voir Bitshares) est qu'un biais d'immobilisme peut apparaître : puisque aucune puissance de calcul n'est nécessaire, le coût d'exploitation de fourches de chaîne est marginal* ». Il devient alors moins risqué économiquement d'essayer d'attaquer le registre des transactions en falsifiant les blocs. « *C'est le paradoxe du* "Nothing at Stake" *[…] les attaques* "Sybil", *avec leur capacité de nuisance sur la performance et de fraudes à la double-dépense, deviennent plus probables, car presque gratuites* ». De même, Larissa Lee souligne l'existence de risques pour les mécanismes de gouvernance, si certains acteurs acquièrent une position de quasi-monopole : « *Where proof-of-work weighs votes based on the amount of CPU devoted to the system, a proof-of-stake system weighs votes based on the number of Bitcoins a user owns. Therefore, a person holding one percent of the total Bitcoins could mine one percent of the blocks* » (*op. cit.*, p. 108).

d'acteur du système[87]. Que ce soit au stade de la présentation des propositions d'évolution ou au stade de leur acceptation, la décentralisation du système apparaît donc menacée par le fait que seuls les programmeurs[88] et les mineurs participent effectivement à sa pondération[89].

Avenir

Pour une partie du moins des observateurs, « *[l]e succès qu'a rencontré le bitcoin depuis 2013 est indiscutable : la masse monétaire de plusieurs milliards de dollars qu'il représente, le volume journalier des transactions, l'intérêt médiatique et les investissements qu'il suscite en sont autant de preuves* »[90]. Bien que son avenir reste toujours un objet de débat[91], celui-ci répond effectivement à un certain nombre d'attentes aussi bien pratiques qu'idéologiques.

Permettant – au moins jusqu'à ce que les capacités de minage soient saturées et que les frais de transactions augmentent significativement – d'effectuer des virements à moindre frais, le bitcoin est aussi une monnaie a-étatique et antisystème. Pour autant peut-on parler de « *monnaie dérégulée* » comme le font Nicolas Clausset et Arnaud Sellem ? S'il est vrai qu'en tant que monnaie décentralisée, celui-ci repose sur une gouvernance difficile à identifier, il n'en est pas moins vrai qu'un mécanisme de consensus existe et qu'il détermine son fonctionnement. Surtout, les promoteurs des monnaies virtuelles contestent le besoin d'une réglementation juridique d'origine étatique en affirmant que c'est dans le code de la Blockchain – qu'un consensus peut justement faire évoluer – que se retrouvent les règles nécessaires. Ils se revendiquent pour ce faire du célèbre aphorisme de Lawrence Lessig, « *Code is law* »[92] – sans s'encombrer, il faut le noter, des subtilités du raisonnement qui l'accompagne... Cette solution serait toutefois dangereuse si le bitcoin, et plus largement le

---

[87] Exception faite du mineur qui travaille dans une coopérative, qui peut n'être qu'un nœud léger dès lors que le pool comprend par ailleurs des nœuds lourds.

[88] On signalera à cet égard que l'un des *core developpers* est dans une situation bien particulière : Gavin Andresen s'est en effet vu remettre par Satoshi Nakamoto une « clé d'alerte », clé cryptographique privée et unique destinée à limiter les effets d'une attaque 51% sur le système bitcoin. En définitive, au regard du rôle et de l'influence exercés par les *core developpers*, il est possible de penser qu'il existe une forme de hiérarchie ou de comité de pilotage au sein de cette communauté décentralisée.

[89] On peut parler à cet égard d'une « *gouvernance de fait* », puisque ce sont les mineurs qui vont pouvoir acter le changement de logiciel, en reconnaissant ou non les blocs adoptés aux nouvelles règles (J. A. Kroll, e.a., « The Economics of Bitcoin Mining – or Bitcoin in Presence of Adversaries », *The Twelfth Workshop on the Economics of Information Security (WEIS 2013)*, Juin 2013, p. 18).

[90] N. Clausset et A. Sellem, *op. cit.*, p. 4.

[91] Voir par exemple l'interview vidéo de L. H. Summers, ancien Secrétaire du Trésor aux USA, qui voit simplement les monnaies virtuelles et la technologie sur laquelle elles reposent comme le futur du monde financier et non comme un facteur de disruption pour le système traditionnel : https://coindesk.wistia.com/medias/rtitd3kev2.

[92] L. Lessig, « Code Is Law. On Liberty in Cyberspace », *Harvard Magazine*, 2000 (disponible en ligne : http://harvardmagazine.com/2000/01/code-is-law-html).

secteur des monnaies virtuelles, évolue vers une situation d'oligopole. Le pouvoir de modifier le code par consensus, qui appartient théoriquement à l'ensemble utilisateurs, se trouverait gravement compromis par la capacité d'un petit groupe en position dominante d'imposer sa loi et de poursuivre ses seuls intérêts[93].

Pour évaluer le besoin de réglementation juridique, il faut donc faire le point sur la situation actuelle du marché des monnaies virtuelles et sur les évolutions prévisibles. Parmi d'autres angles d'approche possibles, on peut notamment s'interroger sur la capacité du bitcoin à garder captifs ses utilisateurs, sur l'existence en d'autres termes d'alternatives au sein des monnaies virtuelles.

Depuis début 2015, le marché est *a priori* pléthorique puisque l'on dénombre plus de 500 monnaies virtuelles[94]. Cependant, à l'examen, il s'avère que « *[s]eul un petit nombre d'entre elles apporte quelques nouveautés : certaines corrigent des "défauts", d'autres proposent de nouvelles fonctionnalités, d'autres encore reposent sur de nouveaux systèmes de validation* ». Et même face à ces dernières, « *le bitcoin bénéficie toujours d'une longueur d'avance grâce au réseau qu'il a constitué* »[95].

Pourtant, certains observateurs pensent qu'un véritable marché concurrentiel est en train de s'installer[96]. En effet, les problèmes techniques rencontrés par le *bitcoin* ne sont pas nécessairement partagés par les autres monnaies virtuelles. En ce sens, Ether, qui prétend avoir reposé sur une technologie plus performante[97], connaît effectivement un développement

---

[93] L. Lessig, *op. cit.* : « *when government steps aside, it's not as if nothing takes its place. It's not as if private interests have no interests ; as if private interests don't have ends that they will then pursue. To push the antigovernment button is not to teleport us to Eden. When the interests of government are gone, other interests take their place. Do we know what those interests are ? And are we so certain they are anything better ?* ».

[94] Même si elles ne répondent pas toutes à la définition restrictive que l'on a adopté précédemment, elles sont 695 recensées sur le site coinmarketcap.com au 20 août 2016.

[95] N. Clausset et A. Sellem, *op. cit.*, p. 4.

[96] N. Gandal et H. Halaburday, « Competition in the Crypto currency Market », 30 janvier 2015, 32 p. (disponible en ligne : http://www.law.northwestern.edu/research-faculty/searlecenter/events/internet/documents/Halaburda_ cryptocurrency.pdf) : les auteurs constatent que le phénomène appelé « winner takes all », en vertu duquel dans une économie de réseau les premiers arrivants conservent une position dominante sur les nouveaux acteurs, ne caractérise plus désormais ce marché qui s'ouvre de plus en plus.

[97] Selon ses promoteurs, Ether bénéficie avec le système Ethereum d'un langage plus accessible et plus attractif pour les développeurs travaillant à créer des applications en lien avec les monnaies virtuelles. Fred Ehrsam, cofondateur de Coinbase, souligne l'importance de cette différence pour des monnaies dont la valeur est soutenue par l'attractivité fonctionnelle : « *Developer mindshare is the most important thing to have in digital currency. The only reason these networks (Bitcoin, Ethereum) and their tokens (bitcoin, ether) have value is because there is a future expectation that people will want to acquire those tokens to use the network. And developers create the applications which drive that demand. Without a reason to use the network, both the network and its currency are worth nothing* » (« Ethereum is the Forefront of Digital Currency », 24 mai 2016, https://medium.com/the-coinbase-blog/ethereum-is-the-forefront-of-digital-currency-5300298f6c75#.4qnoe2utg).

remarquable – devenant en six mois d'existence la deuxième monnaie virtuelle la plus utilisée[98]. Il est en définitive difficile aujourd'hui d'évaluer la substituabilité entre les différentes offres, et un effort en direction d'une analyse concurrentielle mériterait d'être développé.

Dans un second temps, on peut s'interroger non pas simplement sur la viabilité des monnaies numériques, mais sur l'intérêt économique qu'il peut y avoir à assurer cette viabilité – *via* un encadrement juridique adéquat. De ce point de vue, et malgré les incertitudes et les difficultés qu'elles soulèvent, il ne faudrait pas négliger le fait que les monnaies virtuelles présentent des opportunités pour la sphère économique – au-delà même des potentialités de la Blockchain[99]. Ceux-ci « *sont principalement liés aux transferts de fonds transfrontaliers et aux échanges au sein de communautés virtuelles* »[100]. Pour Larissa Lee, « *[t]his disruptive technology has done for money transfers what email did for sending mail* »[101]. Les monnaies numériques sont effectivement des concurrents certains pour les services de type Western Union[102], mais elles interrogent également la pertinence du fonctionnement des virements bancaires internationaux. En dehors des virements *SEPA* (*Single European Payement Areas*), les frais bancaires s'avèrent toujours largement dissuasifs (frais d'émission et de traitement, commission et marge de change, frais de réception, et frais de commissions prélevés par les banques intermédiaires). Plus largement, dans une économie numérique, on comprend intuitivement qu'un moyen de paiement direct est souhaitable[103]. Les monnaies numériques constituent sur ce point une alternative intéressante aux services proposés, par exemple, par Paypal. Elles devront pour rester compétitives continuer à fonctionner avec des frais de transactions nuls ou restreints (pour comparaison ils sont de 1,4 % à 3,4 %, + 0,25 € par transaction à la charge du vendeur pour Paypal). « *Par ailleurs, le bitcoin pourrait constituer une alternative intéressante dans des pays au système bancaire peu développé* »[104]. Cette perspective du rapport entre la monnaie (virtuelle en l'occurrence) et le lien social a été

[98] https://www.letemps.ch/economie/2016/02/15/monnaies-virtuelles-ether-s-impose-aux-cotes-bitcoin

[99] Pour une analyse des potentialités pour le marché financier, voir L. Lee, *op. cit.*, p. 114 et s. ; AEC, l'Agence aquitaine du numérique, « Blockchain : un disrupteur né ? », *Note de veille*, décembre 2015, n° 2 (http://www.aecom.org/Vous-informer/La-veille-AEC/Dossiers-de-veille/Dossier-de-veille-Block-chain-un-disrupteur-ne) ; ainsi que le panorama produit par FirstPartner reproduit en annexe 2.

[100] N. Clausset et A. Sellem, *op. cit.*, p. 4.

[101] L. Lee, *op. cit.*, p. 82. L'auteur s'interroge sur les conditions juridiques dans lesquelles la technologie Blockchain pourrait être employée pour les marchés financiers.

[102] En termes de masses monétaires, le Bitcoin est aujourd'hui passé devant les virements Western Union.

[103] J.-M. Figuet, « Vers l'émergence de monnaies digitales ? L'exemple du Bitcoin », septembre 2015, p. 3 : « *En tant que moyen de paiement, le bitcoin peut être considéré comme un corollaire du e-commerce* » (draft disponible à l'adresse suivante : https://www.dropbox.com/s/kefn7usbk3ti9zh/PEPS%20Monnaie%20Virtuelle%20JM%20Figuet.pdf?dl=0).

[104] *Id.*

envisagée par Fabienne Pinos, membre du groupe de travail et fera donc l'objet de développements dans l'ouvrage à paraître[105]. L'auteur développe notamment une analyse comparative entre le bitcoin, les monnaies électroniques implémentées sur téléphone mobile et les monnaies locales complémentaires. Enfin, même si cet usage est encore peu développé, les monnaies virtuelles pourraient également permettre de se passer de tiers de confiance dans le cadre d'opérations conditionnelles. En effet, « *[l]es transactions en bitcoins peuvent être assorties de conditions et rendre ainsi des services plus évolués que les moyens de paiement traditionnels, sans même recourir à des tiers de confiance (caution, transaction sous séquestre)* »[106].

Si cela n'entre pas dans le champ de l'étude, il faut redire à nouveau que l'expérience des monnaies virtuelles, et plus particulièrement de *bitcoin*, a surtout suscité l'intérêt du monde économique en raison des possibilités qu'offre la technologie Blockchain[107] – mieux comprendre le fonctionnement des monnaies virtuelles constitue donc un enjeu important : cela doit permettre d'anticiper les problématiques à venir, car un certain de questions se poseront à nouveau (déterritorialité, responsabilité dans une gouvernance décentralisée, transparence et données personnelles, etc.). Le projet portée par la communauté d'Ethereum semble aujourd'hui le plus avancé[108]. Il consiste à promouvoir une nouvelle forme d'association digitale de partenaires porteurs de fonds. La « *decentralized autonomous organization* » est toutefois conçue comme un conseil d'administration géant, au sein duquel la prise de décision est ouverte et transparente (« auditable ») grâce à l'utilisation du registre d'Ethereum[109]. La structure se comporte ensuite comme un fond d'investissement ouvert (il est possible d'y entrer librement), qui répond aux offres présentées par des membres ou des tiers (*TheDAO*, premier essai, a été mis en œuvre à très grande échelle puisqu'il aurait réuni

---

[105] F. Pinos, « Monnaies virtuelles et intérêt général : quelles perspectives de convergence ? », 18 p. (draft disponible à l'adresse suivante : https://www.dropbox.com/s/vhxmw4y06u9xssu/2016_03_Projet_Article%202_%20F%20PINOS.pdf?dl=0). Des travaux explorent déjà cette thématique, comme par exemples ceux de Matthews E. Gladden sur une *autonomous ethically guided cryptocurrency* : « *it is possible to design artificially intelligent cryptocurrencies that are not ethically neutral but which autonomously regulate their own use in a way that reflects the ethical values of particular human beings – or even entire human societies* » (« Cryptocurrency with a Conscience: Using Artificial Intelligence to Develop Money that Advances Human Ethical Values », *Annales. Ethics in Economic* Life, 2015, Vol. 18, n°. 4, p. 85-98).

[106] *Id.*

[107] On signalera que les débouchés ne sont toutefois pas réservés à la sphère des activités lucratives. Une Blockchain pourrait par exemple s'avérer profitable pour le domaine de la santé (N. Deviller, « Quelle Blockchain pour la santé ? », *The Conversation*, 2 mai 2016 (https://theconversation.com/quelle-blockchain-pour-la-sante-58519).

[108] Le *White Paper* qui accompagne ce projet est disponible à l'adresse suivante : https://slock.it/dao.html

[109] Il est possible de faire des liens entre ce projet et le mouvement « *democracy by design* » (P. de Filippi et D. Bourcier, *op. cit.*, p. 48).

jusqu'à 130 millions d'euros) ou elle peut avoir été créée afin de répondre à un objectif spécifique (projets de *Slock.it* et de *Freeftopia*). Cette entité est supposée être dépourvue de statut juridique : elle serait davantage un programme qu'un organisme susceptible de se voir reconnaître une personnalité morale (la position des initiateurs de ce projet sur ce point mériterait toutefois d'être discutée, car la qualification de société de fait semble difficilement pouvoir être exclue et il en va de même pour la notion d'entreprise retenue en droit de l'Union européenne). Les participants sont liées entre eux et avec leurs cocontractants par des *smart-contracts*, intégrés à Ethereum, et dont la bonne exécution pourrait être certifiée par des tiers. Le projet connait toutefois une crise majeure depuis le 16 juin 2016, à la suite d'un vol de tokens (c'est-à-dire de parts des associés de *TheDAO*) pour un montant de 3,6 millions d'Ether. Les 11,6 millions restants ont été bloqués à la suite d'un *soft fork*, de sorte que ni *TheDAO*, ni les participants ne pouvaient les utiliser. Après un débat difficile, il a été convenu de réécrire le registre d'Ethereum, à la faveur d'un *hard fork*, afin de reprendre les Ether volés au pirate et de les restituer à leurs détenteurs initiaux. Cette solution, en apparence la plus juste, fut difficile à accepter dans la mesure où elle remettait en cause un principe fondateur de la technologie Blockchain : l'immuabilité[110]. Cet épisode montre que l'immuabilité ne tient que dans la mesure où elle bénéficie du consensus de la communauté. Quiconque possède ou parvient à réunir 51% de la puissance de calcul du réseau peut bel et bien réécrire des transactions. Par ailleurs, il illustre les dangers de l'investissement dans ces nouvelles technologies. Les porteurs de *TheDAO* ont mis en place une procédure de remboursement pour les participants qui souhaiteraient se retirer, et craignent désormais que les régulateurs comme l'*AMF* (*Autorité des Marchés Financiers*) ou la *SEC* (*Securities Exchanges Commission*) américaine ne s'intéressent à la régulation des projets adossés à une Blockchain – venant ainsi couper l'élan d'innovation.

Les craintes vis-à-vis de toute intervention des autorités publiques ne sont toutefois pas partagées par l'ensemble du monde des monnaies numériques, et certains des acteurs appellent à un encadrement juridique[111]. Il est donc possible de penser que les monnaies virtuelles se trouvent en réalité à un stade de croissance paradoxal. Espace crypto-anarchique

[110] Un désaccord a conduit à une scission avec la création d'une chaîne minoritaire (*Etheruem classic*), dans laquelle les tokens volés n'ont pas été retournés. Elle se présente donc comme réellement immuable et affirme faire une exacte application de la maxime « *code is law* » en partant du principe que les investisseurs auraient dû être plus vigilants et découvrir la faille dans le code de *TheDAO*. Cet épisode a plus largement été l'occasion de revivifier le débat sur la portée de cette doctrine (voir, par exemple, http://www.coindesk.com/code-is-law-not-quite-yet/).

[111] C'est par exemple la position défendu par Gonzague Grandval, cofondateur de la plateforme Paymium, lors du salon *PayForum* qui s'est tenu à Paris du 16 au 17 mars 2016.

ou plus simplement a-étatique au départ, le développement du monde de Satoshi paraît devoir dépendre, au-delà des défis technologiques, de la clarification de son environnement juridique. Ce changement de paradigme se fait au fur et à mesure que les investisseurs s'intéressent aux opportunités ouvertes par les crypto-monnaies. Facteur de confiance, une régulation adaptée permettrait de convertir de nouveaux adeptes et de favoriser simultanément les retours sur investissement. Or, force est de constater sur ce point que l'idéal de la sécurité juridique est loin d'être atteint : comme cela a été rappelé à titre introductif, des difficultés difficilement surmontables se rencontrent dès le stade de l'opération de base que constitue la qualification juridique.

1.b Equipe et méthodologie de travail

L'opportunité des recherches relatives aux monnaies virtuelles a pu être mise en doute, tant par leurs tenants que par leurs adversaires[112]. Pourtant, des études paraissent régulièrement au point que la littérature scientifique puisse aujourd'hui être considérée comme conséquente, aussi bien dans le champ de l'informatique et de la cyber-sécurité que dans celui de l'économie[113]. Les analyses juridiques restent cependant relativement peu nombreuses en dehors de celles que produisent les autorités administratives nationales[114]. Au regard des risques important que les rapports publics ont pu identifier, de l'absence de solution adéquate en droit positif, on peut penser qu'une étude de science juridique relative aux monnaies virtuelles était donc en soi tout à fait justifiée.

Cependant, le propre de ce sujet est de se situer à la croisée des champs de compétences, puisqu'en tant qu'innovation technologique les monnaies virtuelles restent difficiles à saisir pour l'économiste comme pour le juriste. Or, dans la littérature parcourue, les approches croisées du phénomène elles sont quasiment inexistantes. C'est dans l'objectif de combler cette lacune qu'une équipe pluridisciplinaire a été mise en place.

---

[112] J. Bonneau e.a., *op. cit.*, p. 1.

[113] Selon une liste exhaustive, établie par Brett Scott, il y aurait en 2016 plus de 600 publications scientifiques (disponible à l'adresse suivante : https://docs.google.com/spreadsheets/d/1VaWhbAj7hWNdiE73P-W-wrl5a0WNgzjofmZXe0Rh5sg/edit#gid=0).

[114] Voir en ce sens, H. de Vauplane, « L'analyse juridique du Bitcoin », *op. cit.*, p. 351.

Pluridisciplinarité

Autour du Professeur Valérie Malabat, une équipe pluraliste a donc été constituée de manière à assurer une compréhension globale du phénomène à l'étude. Elle compte en outre un participant allemand, ce qui lui assure une vision transnationale sur les problèmes soulevés par les monnaies numériques.

Composition du groupe de travail :

• *Sciences dures (mathématique et informatique) :*

- **Gilles Zémor**, Professeur, spécialiste de la théorie des nombres, d'algorithmique et d'arithmétique, membre de l'Institut de Mathématique de Bordeaux ;

- **Emmanuel Fleury**, Prof. associé, spécialiste en cryptographie et en sécurité informatique, membre du LaBri de l'Université de Bordeaux ;

• *Science économique :*

- **Jean-Marc Figuet**, Prof., spécialiste d'économie monétaire et bancaire et finance internationale, membre du Larefi de l'Université de Bordeaux ;

- **Pierre-Henri Faure**, Maître de conférences, spécialiste de modélisation économique et de théorie des jeux, membre du Larefi de l'Université de Bordeaux ;

- **Fabienne Pinos**, Doctorante travaillant sur l'inclusion financière des populations précarisées, membre du Larefi de l'Université de Bordeaux ;

• *Science juridique :*

- **Valérie Malabat**, Professeur, spécialiste de droit pénal, membre de l'ISCJ de l'Université de Bordeaux, **directrice du PEPS** ;

- **Charlotte Claverie-Rousset**, Professeur, spécialiste de droit pénal, membre de l'ISCJ de l'Université de Bordeaux ;

- **Matthias Lehmann**, Professeur, spécialiste de droit de droit international privé et de droit des affaires, directeur de l'Institut pour le droit international privé et le droit comparé de l'Université de Bonn.

- **Ronan Raffray**, Professeur, spécialiste de droit des affaires et du patrimoine, membre de l'IRDAP de l'Université de Bordeaux ;

- **Suzie Bradburn**, Maître de conférences, spécialiste des systèmes d'échange locaux, membre de l'IRDAP de l'Université de Bordeaux ;

- **Thibaud Guillebon**, Doctorant travaillant sur les monnaies virtuelles, membre de l'IRDAP de l'Université de Bordeaux ;

- **Olivier Dubos**, Professeur, spécialiste de droit européen et de droit transnational, membre du CRDEI de l'Université de Bordeaux ; **Jean-Pierre Laborde**, Professeur, spécialiste de droit international privé et de droit social, membre du CRDEI de l'Université de Bordeaux ;

- **Jean-Pierre Laborde**, Professeur, spécialiste de droit international privé et de droit social, membre du CRDEI de l'Université de Bordeaux ;

- **Sandrine Sana-Chaillé de Néré**, Professeur, spécialiste de droit international privé, membre du CRDEI de l'Université de Bordeaux ;

- **François-Vivien Guiot**, Docteur en droit, spécialiste de droit européen, membre du CRDEI de l'Université de Bordeaux, et assistant de recherche du projet.

Méthode de travail

Le groupe ainsi constitué s'est réuni à deux reprises dans le cadre de journée de travail, faisant suite à des investigations menées de manière individuelle. La première rencontre, en date du 21 janvier 2016, a été l'occasion d'aplanir les difficultés techniques qui s'opposaient à une bonne compréhension du concept de monnaie virtuelle, mais aussi de construire un langage commun susceptible d'éviter les ambiguïtés qui naissent lors de la juxtaposition de discours relevant de sciences distinctes. Pour ne prendre qu'un exemple, le terme de « monnaie légal » s'est avéré recevoir un sens différent pour les économistes et pour les juristes. En outre, cette première rencontre a permis l'adoption d'une notion de monnaie virtuelle commune de nature à délimiter le périmètre de recherche. Les membres présents ont ensuite fait part des problèmes et interrogations que l'utilisation ou l'existence des monnaies virtuelles pouvait à première vue induire dans les différents champs scientifiques représentés : théorie de la monnaie, politique monétaire, finance internationale, droit bancaire et droit des affaires, droit de la consommation, droit international privé, droit social, droit public et européen...

Un second workshop a eu lieu le 29 avril 2016, pour revenir sur les analyses discipline par discipline et présenter les résultats d'une réflexion plus approfondie menée par les membres du groupe de recherche. Cette réunion a permis également de faire le point sur la riche actualité des monnaies virtuelles et d'intégrer ainsi les dernières évolutions au processus d'analyse.

Les membres du groupe ont pu, pour ce faire, s'appuyer sur un travail documentaire fourni afin d'assurer non seulement le dépouillement de la littérature scientifique, en langue française comme en anglais, mais également une veille de la presse écrite et numérique. Par ailleurs, cette enquête bibliographique a été prolongée par des prises de contact auprès du monde économique. Celles-ci ont été réalisées, d'une part, grâce à la rencontre avec Eric Culnaert – chef de projets « numérique / commerce connecté » chez Aquitaine Développement Innovation – et, d'autre part, à la participation aux conférences et ateliers du salon Payforum 2016 – qui regroupe l'ensemble des acteurs français du secteur des paiements et de la monétique.

1.c Résultats

Les séances de travail collectif ont permis de mettre à jour l'intérêt d'une journée de conférences pluridisciplinaires et ouverte à la société civile. Prévue pour le 7 octobre 2016, elle sera l'occasion de poursuivre l'analyse mise en œuvre depuis le mois de novembre 2015 et de confronter le point de vue des universitaires avec celui des usagers potentiels ou effectifs. Le choix a donc été fait d'inviter des intervenants extérieurs afin d'ouvrir encore les perspectives de réflexion.

Le programme a été construit autour de deux axes : l'utilisation et la régulation.

INTRODUCTION

- *9 h : Le développement des monnaies virtuelles : Etat des lieux et enjeux essentiels*

par Jean-Marc Figuet et François Vivien Guiot

MATINEE : L'UTILISATION DES MONNAIES VIRTUELLES

Sous la présidence de Jean-Marc Figuet

• Les monnaies virtuelles : les procédés

- *9h30 : Un exemple : le fonctionnement du bitcoin*

Par Thibaud Guillebon

- 10h : « *Monnaies numériques : Algorithmes et protocoles »*

Par Emmanuel Fleury

• Les monnaies virtuelles : les usages

- *11h30 : Table ronde*

Animée par François Pellegrini, professeur à l'université de Bordeaux, *LaBRI, Vice-président de l'université en charge du numérique*.

Avec la participation (sous réserve) de Manuel Boutet, Maître de conférences en sociologie à l'université de Nice, *GREDEG*, (Groupe de recherche en droit, économie et gestion) ; Agnès Grange, Banque postale, spécialiste de l'innovation ; Alexis Roussel, co-fondateur de bity.com ; et Fabienne Pinos.

APRES-MIDI : LA REGULATION DES MONNAIES VIRTUELLES

Sous la présidence d'Olivier Dubos

• La chose : quelle qualification ?

- 14h30 : Le bitcoin peut-il être assimilé à une monnaie ? Un examen à partir des différentes grilles de lecture de la science économique

Par Pierre-Henri Faure

- 15h : La qualification juridique

Par Charlotte Claverie-Rousset

• Les protagonistes : quel contrôle ?

- 15h30 : L'utilisateur honnête

Par Pauline Pailler, professeur à l'université de Reims

- 16h : L'utilisateur mal intentionné

Par Valérie Malabat

- 17h : L'intermédiaire

Par Matthias Lehmann

CONCLUSION

- 17h30 : La norme : le Code ou la loi ?

Par Suzie Bradburn

Au regard de la singularité de la démarche poursuivie, il a semblé justifié de conclure les travaux par une publication scientifique des résultats du groupe de travail. L'ouvrage sera destiné à reprendre les développements de cette journée de conférence, mais offrira également un espace d'expression pour d'autres réflexions qui viendront ainsi enrichir la perspective pluridisciplinaire (on pense en particulier à la question de la légitimité de l'abstention de l'Etat régulateur face à une innovation se revendiquant d'aspirations libertariennes). Le présent livrable n'a donc pas pour objectif d'anticiper sur la publication à venir, qui permettra d'identifier plus précisément les questions technologiques et les enjeux

économiques induits par le développement des monnaies virtuelles, ainsi que les risques juridiques et les solutions envisageables. Il s'agit avant tout de présenter comment s'est construit ce regard croisé sur un objet complexe : ce n'est qu'après avoir appréhendé sa dimension novatrice, voire disruptive, que le débat a été porté sur le besoin de régulation.

2 ANALYSE ECONOMIQUE

Au regard des données quantitatives[115], la nécessité de réglementer les monnaies virtuelles pourrait paraître contestable – du moins au-delà de la question de la prévention des activités illicites. Toutefois, les études disponibles laissent à penser que l'utilisation de monnaie virtuelle pourrait être un facteur de croissance[116]. Ainsi, en 2011, le Groupe de travail mandaté par le ministre canadien des Finances a estimé « *qu'un système de paiement pleinement moderne entraînerait pour l'économie canadienne des gains de productivité équivalant à 2% du PIB, soit des économies annuelles de l'ordre de 32 milliards de dollars* »[117]. Si l'idée d'un système de paiement moderne ne se limite pas au développement

[115] Voir *infra*, §2.b.

[116] Maître Raphaël Rault souligne l'existence d'avantages financiers et commerciaux pour les entreprises : « *Les intérêts financiers sont non négligeables pour l'entreprise. Inciter les clients à réaliser leurs transactions dans la monnaie virtuelle « home made » permet de limiter le volume de transactions bancaires et notamment les micro-transactions [...] Lors d'un achat, les unités sont utilisées directement, la banque n'intervient pas dans la transaction et n'opère pas de prélèvement sur les comptes bancaires à chaque fois. [...] L'entreprise réduit ainsi sa dépendance aux établissements bancaires (banques mais aussi émetteurs de cartes bancaires)* » (« Monnaie virtuelle et monnaie électronique : distinction et encadrement contractuel des porte-monnaie virtuels affectés », disponible en ligne : http://www.tendancedroit.fr/monnaie-virtuelle-et-monnaie-electronique-distinction-et-encadrement-contractuel-des-porte-monnaie-virtuels-affectes/).

[117] Groupe de travail sur l'examen du système de paiement, *Le Canada à l'ère numérique*, 2012 (http://paymentsystemreview.ca/index.php/rapports/le-canada-a-lere-numerique/indexe68f.html?lang=fr).

des monnaies virtuelles, il est certain que ces dernières y participent – comme le montre aujourd'hui les travaux dont fait l'objet la technologie Blockchain qui en est le support[118].

2.a Approche quantitative

Les données recensées dans la littérature scientifique par Jean-Marc Figuet sont unanimes. Le « phénomène » reste d'une ampleur contenue si on l'appréhende en termes de volume de transaction : « *Selon les statistiques du Federal Reserve System (2015), le volume quotidien des transactions totales en bitcoin, depuis sa création, serait inférieur à 80 millions alors que les transactions en dollar scriptural seraient supérieures à 122,4 milliards en 2012. Holden (2015) estime qu'il y aurait 1,3 millions d'utilisateurs du bitcoin en 2014, et potentiellement, 4,7 millions en 2019. Et l'augmentation du volume des transactions en bitcoin ne serait pas tant le fait d'un panel plus large d'adoptants qu'une intensification des transactions entre utilisateurs habituels. Yermak (2013) recense 70 000 transactions journalières en bitcoin dont 80% seraient purement spéculatives. Segendorf (2014) estime que les transactions en bitcoin représentent 0.01% des transactions quotidiennes par cartes bancaires. La vitesse de circulation est faible. Seuls 4% des bitcoins en circulation seraient hebdomadairement utilisés, 24% dans les 3 mois et 50% dans les 6 mois. Plus du tiers serait conservé par leurs détenteurs au-delà de l'année. Au total, le bitcoin serait peu utilisé pour des transactions sur biens et services* »[119].

Il en va de même sous l'angle de la masse monétaire et de capital. Les plus de 15 millions de bitcoins en circulation représentent une masse de quelques milliards de dollars (près de 14 milliards en 2014, mais au mois d'août 2016 la valeur unitaire varie entre 500 et 600 dollars et le marché représente aujourd'hui autour de 9 milliards de dollars seulement). Ether, la seconde monnaie virtuelle actuellement, tend vers le milliard de dollars ; tandis qu'avec le numéro trois, Ripple, on tombe à quelques 200 millions[120]. En comparaison, il y existe plus de 1 200 milliard de dollars rien qu'en monnaie fiduciaire. Même en considérant le bitcoin

---

Si l'Agence bancaire européenne ne quantifie pas aussi précisément les bénéfices possibles en termes de PIB, elle souligne également dans son rapport de 2014 l'opportunité qu'elles pourraient représenter pour la croissance économique (EBA, *Opinion on 'virtual currencies'*, p. 18, https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf).

[118] Marc Lacoursière observe en ce sens que la Monnaie royale canadienne, inspirée par l'exemple du Bitcoin, avait l'intention de développer une monnaie numérique ayant cours légal – le *MintChip* (*op. cit.*, p. 22).

[119] J.-M. Figuet, *op. cit.*, p. 4.

[120] Selon les informations disponibles sur coinmarketcap.com, la capitalisation de l'ensemble des monnaies virtuelles est au 20 août 2016 de 11 478 781 423 dollars.

uniquement comme un moyen de paiement, la capitalisation boursière de Visa est de 55 milliards de dollars tandis que celle de MasterCard atteint 39 milliards de dollars.

La même relativisation se retrouve dans les divers rapports officiels. A titre d'illustration, on peut rappeler la position du Conseil économique, social, et environnemental présentée dans son rapport de 2015 sur les nouvelles monnaies : « *Si l'on se penche sur l'activité liée aux bitcoins, 80 000 transactions seraient effectuées chaque jour au niveau mondial pour un montant de 30 millions d'euros. A titre de comparaison, au sein de l'Union européenne, 250 millions de transactions sont effectuées* »[121].

Les perspectives d'évolution, que ce soit en termes de masse monétaire ou de flux de transactions, sont par ailleurs limitées dans la mesure où les principales monnaies virtuelles ont adopté des règles de monnayage prédéfinies et limitatives. Réaction aux politiques monétaires des banques centrales favorisant l'inflation, les monnaies virtuelles adoptant une limite maximum d'émission (comme bitcoin et Ether) sont donc par nature déflationnistes. Cet aspect sera développé ci-dessous, mais on peut noter dès à présent que ce choix est de nature à ralentir à terme la circulation de la monnaie virtuelle[122] : en laissant « dormir » son argent, on peut espérer qu'il prenne automatiquement de la valeur. Une telle propriété n'est donc pas nécessairement un avantage pour l'économie réelle, ni pour le développement des monnaies virtuelles en tant qu'instrument d'échange.

Le sentiment qu'il s'agit en définitive d'une activité relativement marginale se retrouve enfin dans l'examen de la diffusion géographique de ces monnaies *a priori* déterritorialisées : « *[leur] usage serait relativement concentré aux Etats Unis et en Chine. Les chinois utiliseraient le bitcoin pour acheter des biens à l'étranger et envoyer des fonds aux expatriés (Collomb, 2015). La communauté des utilisateurs traditionnels serait donc actuellement réduite et géographiquement concentrée* »[123].

Trois ans plus tard, même après les développements qu'elles ont connus, la conclusion d'Hendrix Vachon à propos des crypto-monnaies paraît donc toujours aussi solide : « *les monnaies nationales ne sont pas près d'être délogées* »[124].

---

[121] P. A. Gailly, « Nouvelles monnaies : les enjeux macro-économiques, financiers et sociétaux », *Avis du CESE, Section de l'économie et des finances*, 2015, p. 21.

[122] Voir en ce sens, H. Vachon, *op. cit.*, p. 4.

[123] J.-M. Figuet, *op. cit.*, p. 4.

[124] H. Vachon, « Les limites des monnaies du type *bitcoin* », *Point de vue économique*, novembre 2013, p. 5 (https://desjardins.com/ressources/pdf/pv131121-f.pdf?resVer=1385162817000).

2.b Approche qualitative

Sur le plan qualitatif, les obstacles à l'identification des monnaies virtuelles comme des monnaies sont nombreux et très largement reconnus. Sauf en Allemagne, où le bitcoin a été reconnue comme une « monnaie privée » dès le 16 août 2013, les monnaies virtuelles ont tout d'abord pour tare principale de ne pas avoir la qualité de monnaie au sens légale – et plus largement de revêtir un statut juridique incertain. En conséquence, sauf accord entre les parties, un paiement en bitcoin n'a pas de nature libératoire. Il ne peut donc être imposé à un créancier. Et d'ailleurs peu de marchands acceptent d'être payer en monnaie virtuelle[125].

Au-delà de cette problématique légale, le problème de la valeur des unités de monnaies virtuelles est régulièrement soulevé[126]. A l'inverse de la monnaie métallique, celles-ci n'ont pas de valeur intrinsèque et ne sont pas garanties comme les monnaies fiduciaires par le pouvoir public. Il est pourtant possible de lire qu'« *au contraire de la création monétaire usuelle [*i.e. monnaie-fiat ou monnaie fiduciaire*], le monde des unités numériques (*bits*) quasi métalliques (*coins*) serait garant d'une authenticité, car ancré dans l'effort nécessaire à leur extraction* »[127] – la tentation d'assimiler les bitcoins à une monnaie-marchandise est induite par le mécanisme de monnayage qui organise sa rareté[128]. En ce sens, on peut noter que le taux initial de conversion des bitcoins en dollars avait effectivement été établi à partir du coût énergétique de la production informatique d'une unité de monnaie virtuelle. Toutefois,

---

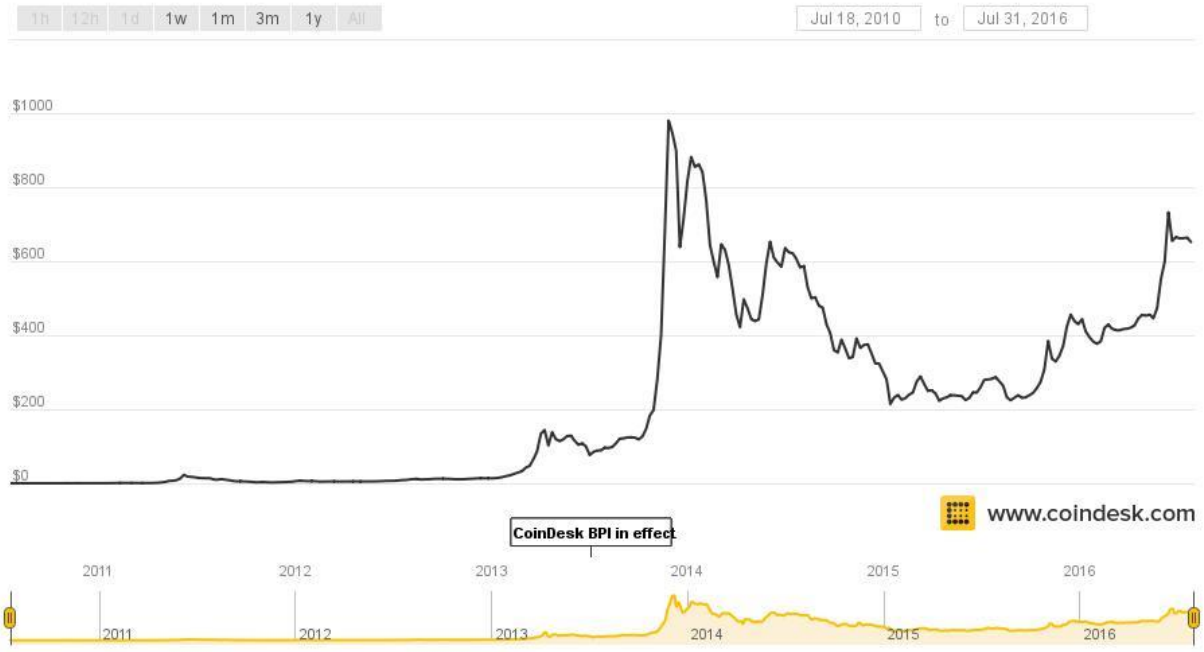
[125] On trouve des annuaires des commerçants acceptant les Bitcoins aux adresses suivantes : pour la France voir https://bitcoin.fr/depenser-ses-bitcoins/ (l'un des plus connus y figurant est showroomprive.com. Alors que Monoprix avait fait des annonces en ce sens, le Bitcoin n'a jamais été intégré comme moyen de paiement par cet enseigne), et au niveau mondial voir https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/.

[126] D. Yermack, « Is Bitcoin a Real Currency ? An economic Appraisal », NYU Stern School of Business, 2014, p. 10 et s. (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2361599) : en raison notamment du problème de volatilité, l'auteur considère que la qualification de monnaie ne peut être retenue pour le Bitcoin qu'il faudrait davantage considérer comme un investissement spéculatif. Dans le même sens, voir N. Gandal et H. Halaburday, « Competition in the Cryptocurrency Market », 30 janvier 2015, p. 4 (disponible en ligne : www.law.northwestern.edu/research-faculty/searlecenter/events/internet/documents/Halaburda_cryptocurrency. pdf).

[127] L. Desmedt, *op. cit.*, p. 10. C'est effectivement l'idée originelle de Satoshi Nakamoto, qui entendait recompense les mineurs par l'obtention de Bitcoins : « *The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended* » (*Bitcoin : A Peer-to-Peer Electronic Cash System*, 2008, §6).

[128] H. Vachon, *op. cit.*, p. 2 : « *À certains égards, les crypto-monnaies s'apparentent aux monnaies-marchandises. Conceptuellement, le mécanisme de création monétaire simule mathématiquement l'extraction d'un métal précieux, et surtout rare. [...] Sommes-nous en présence d'une forme de monnaie-marchandise version améliorée 2.0 ? La réponse à cette question est non, car une caractéristique fondamentale des monnaies-marchandises est leur valeur intrinsèque non nulle. [...] Les bitcoins et les autres crypto-monnaies n'ont aucune valeur intrinsèque et cette caractéristique fondamentale les classe plutôt parmi les monnaies fiduciaires* ».

ce rapport est loin d'être constant, et depuis lors la valeur des bitcoins semble en réalité totalement indépendante de l'idée de rétribution d'une *proof of work*[129].



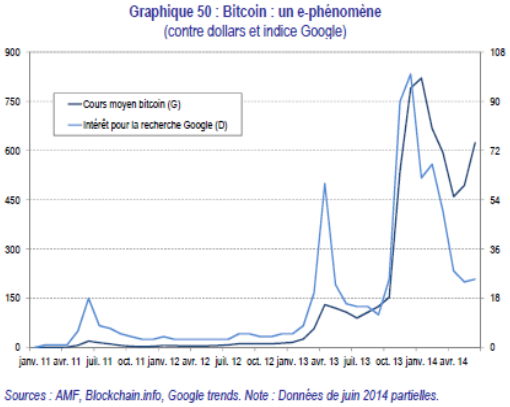
Si sa valeur n'est pas sensible à son coût de production, elle dépend en réalité de deux séries de variables. La première série est constituée par des données connues : la rareté, programmée par l'algorithme grâce à une difficulté croissante et périodique du minage ainsi qu'à une limitation prédéterminée du montant d'unité (le chiffre maximum, fixé à 21 millions de bitcoins, devrait être atteint en 2140), est destinée à favoriser une croissante régulière du taux. La deuxièmes série de variables se composent à l'inverse d'éléments conjoncturels et plus ou moins imprévisibles[130] : ainsi, la découverte de chacune des affaires mettant en cause le bitcoin conduit invariablement à un effondrement du cours[131], alors qu'à l'inverse les crises

[129] Comme le confirme Fabienne Pinos, les données économiques qu'il est possible d'établir « *mettent en évidence que l'activité de "minage" n'a pas un modèle économique fondé sur l'utilisation de ressources à destination d'une création de valeur réelle.* A contrario, *des ressources physiques (matériel, énergie) sont mises au service d'une activité qui ne deviendra rentable qu'en fonction du cours futur du Bitcoin. A défaut de couvrir leurs frais à court terme, les "mineurs" actuels accumulent les bitcoins minés dans la perspective d'une plus-value à la revente, soit une activité spéculative fondée sur une dépense énergétique. Dans un contexte de crise énergétique et écologique, ce dispositif interroge sur les externalités sociétales induites* » (*op. cit.*, p. 8).

[130] Voir le tableau chronologie reproduit en annexe 1.

[131] L'annonce en janvier 2016 de la banqueroute de la plateforme Crypsty (en raison de son incapacité à maintenir sur le long terme une réserve financière suffisante après la perte de plus de 10 millions d'euros lors du vol en 2014 de Bitcoins et Litecoins sur les portefeuilles qu'elles fournissaient aux utilisateurs de monnaie virtuelles) fut immédiatement suivie d'une chute du cours de change du Bitcoin (voir à ce sujet : http://www.tomshardware.fr/articles/bitcoin-mike-hearn-cryptsy-litecoin,1-58293.html). Tout récemment encore, le 3 août 2016, la société Bitfinex a annoncé le vol de 120 000 Bitcoins – soit près de 65 millions de dollars – ce qui en quelques heures a fait perdre à cette monnaie virtuelle 20 % de sa valeur (http://www.lesechos.fr/finance-marches/marches-financiers/0211179950165-le-bitcoin-chute-de-8-apres-le-hacking-de-bitfinex-2018534.php).

économiques et financières que connaissent certains pays sont de nature à multiplier la demande en bitcoin[132]. On a même pu établir une corrélation entre le cours de ce dernier et le nombre de requêtes effectuées à son sujet sur les moteurs de recherche[133]. Toutefois, certains observateurs considèrent qu'il est inapproprié de parler de bulles spéculatives, car après chaque « bouffées de volatilité » le cours du bitcoin se stabilise au-delà de son niveau antérieur (*voir les exemples ci-dessous*).



Aujourd'hui ce sont les débats sur l'évolution technologique qui semblent être les principaux facteurs principaux d'inquiétude et de variation du cours.

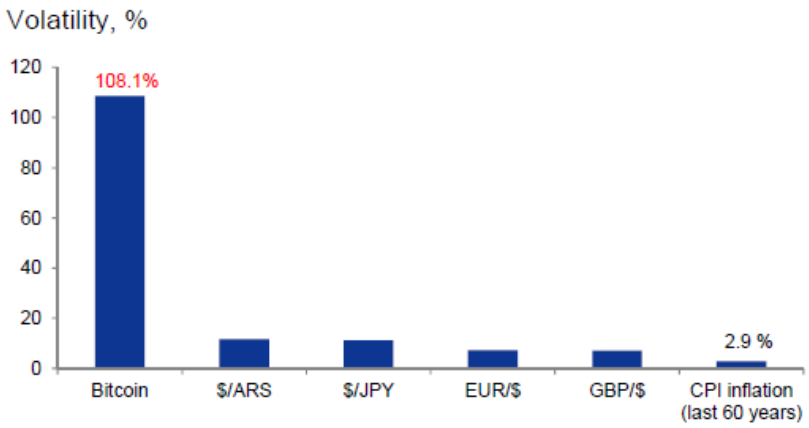
Par ailleurs, l'étendue des fluctuations observées est sans commune mesure par rapport à celles que l'on rencontre généralement avec les autres actifs. On peut même parler en ce sens d'une hyper-volatilité du bitcoin, qui est passé de moins de 1 dollars à 1000 dollars fin 2013[134], pour s'équilibrer entre 300 et 400 dollars[135].

---

[132] M. Chevalier et B. Vignolles, « Le bitcoin : défi à la souveraineté monétaire des Etats et ressource pour le blanchiment d'argent », *Regards croisés sur l'économie*, 2014, n° 14, p. 123 : « *Ainsi, à l'occasion de crises économiques ponctuelles, comme la restructuration de la dette grecque en 2011 ou celle de Chypre en 2013, il a vu rapidement son cours doubler, pour frôler les 200 dollars, avant de retomber rapidement à ses valeurs d'avant crise* ». On notera de manière plus anecdotique que le Brexit a suscité également des réflexions sur l'emploi du Bitcoin pour une Ecosse désireuse d'indépendance : C. Dalzell, « Scottish currency options post-Brexit. A discussion paper », *Common Weal Policy*, juin 2016, p. 15 (disponible en ligne : http://allofusfirst.org/tasks/render/file/?fileID=5DE9EBD7-0CBD-6002-A680D9035064FED1).

[133] Autorité des Marchés Financiers (AMF), « Emergences des monnaies virtuelles : risques et opportunités ? », *Risques et tendances*, juillet 2014, n° 15, p. 60 (http://www.amf-france.org/Publications/Lettres-et-cahiers/Risques-et-tendances/Archives.html?docId=workspace%3A%2F%2FSpacesStore%2Fb87033f5-ecbf-41f1-8236-ee44c91df3c7).

[134] Sur les méfaits d'une telle inflation, Paul Krugman écrivait en 2011 : « *Bear in mind that dollar prices have been relatively stable over the past few years – yes, some deflation in 2008-2009, then some inflation as commodity prices rebounded, but overall consumer prices are only slightly higher than they were three years*



Source: Coindesk.com, Goldman Sachs Global Investment Research.

S'il ne s'agit pas d'une spécificité des monnaies virtuelles, il est indiscutable qu'à leur égard « *l'arrimage au monde "réel" demeure problématique* »[136] et qu'il y a là un facteur d'incertitude et de risque important pour les utilisateurs comme pour les investisseurs[137]. Pour Odile Lakomski-Laguerre et Ludovic Desmedt « *[a]vec la valorisation phénoménale dont il a fait l'objet depuis sa création, et la volatilité de son cours relativement aux devises officielles, force est de constater qu'aujourd'hui, le bitcoin apparaît bien plus comme un actif spéculatif que comme un instrument au service d'une économie d'échanges et de paiements* »[138].

Les règles qui entourent le monnayage, et qui sont indépendantes de la demande et de l'offre, sont d'ailleurs de nature à favoriser les fluctuations du cours : « *Il peut y avoir trop de bitcoins en circulation quand le cours chute et pas assez quand le cours monte. [...] Par*

---

ago. What that means is that if you measure prices in Bitcoins, they have plunged; the Bitcoin economy has in effect experienced massive deflation. And bcause of that, there has been an incentive to hoard the virtual currency rather than spending it » (« Golden Cyberfetters », *The Opinion Pages – NY Times*, 7 septembre 2011, http://krugman.blogs.nytimes.com/2011/09/07/golden-cyberfetters/?_r=0).

[135] P. A. Gailly, « Nouvelles monnaies : les enjeux macro-économiques, financiers et sociétaux », *Avis du CESE, Section de l'économie et des finances*, 2015, p. 21 : « *entre les mois de mai 2012 et 2014, la volatilité mensuelle et quotidienne du bitcoin a atteint respectivement 265 % et 200 %, à comparer avec la parité euro-dollar qui est 40 fois moins volatile. Depuis sa création, sa valorisation a évolué entre 1 et 1163 dollars au plus haut. En ce sens, par sa volatilité, le bitcoin peut s'apparenter à un placement spéculatif* ».

[136] L. Desmedt, *op. cit.*, p. 11.

[137] Pauline Pailler observe à juste titre que le Bitcoin est un investissement à haut risque car si la monnaie virtuelle « *peut constituer ne réserve de valeur théorique, sa grande volatilité fragilise cette possibilité* » (*op. cit.*, p. 41).

[138] O. Lakomski-Laguerre et L. Desmedt, « L'alternative monétaire Bitcoin : une perspective institutionnaliste », *Revue de la régulation*, 2015, n° 18, §16 (http://regulation.revues.org/11489). Ludovic Desmedt réitère par ailleurs ce jugement en s'appuyant sur l'argument de la faible substituabilité des Bitcoins : « *les crypto-monnaies sont des actifs régis par un logique de choix de portefeuille, et non des monnaies au sens plein du terme* » (« Le bitcoin et les crypto-monnaies : nouveaux modèles, questions persistantes », *RISF*, 2014, n°4, p. 11).

définition, l'offre de bitcoins ne peut être manipulée, mais le taux de croissance de l'offre n'est peut pas être économiquement optimal au sens de Friedman »[139].

En définitive, il semble que la monnaie virtuelle « *ne permet l'évaluation de biens et de services que par référence, le plus souvent, à une monnaie légale : la valeur de la monnaie virtuelle dépend de sa convertibilité en monnaie scripturale, qui peut être extrêmement aléatoire* »[140]. Elle n'aurait donc pas la qualité d'une unité de compte. Certes, des initiatives ont vu le jour qui pourraient à long terme modifier cet état de fait. Tel est par exemple le cas du projet de la société *Bitwage*[141] qui propose de verser des salaires transfrontières en utilisant les bitcoins : percevoir ainsi son revenu est susceptible d'encrer cette monnaie dans le réel, dans le travail fourni, même si elle reste pour le moment un simple facilitateur de circulation. En dehors d'une petite communauté d'activistes, les utilisateurs prêts à prendre le risque induit par l'instabilité du cours sont encore peu nombreux. Ainsi, même chez les marchands qui acceptent le paiement en bitcoin, les prix sont affichés dans l'unité ayant cours légal avant d'être convertis au moment du paiement[142].

Le système bitcoin connait une seconde limite en raison du mécanisme d'émission programmée et de ses répercussions sur la structure du marché : « *[e]n limitant à terme l'offre de monnaie, cette règle organise la rareté du bitcoin et en fait davantage un instrument de réserve de valeur, voire un actif spéculatif, ces deux usages venant contrarier très fortement son statut de monnaie. Les détenteurs sont ainsi logiquement incités à stocker les bitcoins plutôt qu'à les dépenser. C'est ce qu'ont montré notamment Ron et Shamir en analysant la répartition des bitcoins (Ron et Shamir, 2012). Ils ont remarqué que 59,7 % des unités bitcoins étaient "dormantes". La même étude a permis d'établir que si 97 % des comptes possèdent moins de 10 bitcoins, à l'inverse à peine 78 comptes dans le monde concentrent plus de 10 000 bitcoins chacun. D'après Bitcoinica, 1 % seulement des acteurs possèdent 50 % des bitcoins. D'autres chercheurs ont identifié les premières transactions importantes et ont découvert qu'elles provenaient toutes d'une transaction initiale, tandis qu'un seul compte (celui de Satoshi Nakamoto en l'occurrence) avait accaparé à peu près 980 000 bitcoins* »[143].

---

[139] J.-M. Figuet, *op. cit.*, p. 10-11.

[140] P. Pailler, *op. cit.*, p. 41

[141] http://www.usine-digitale.fr/editorial/bitwage-la-fintech-qui-gere-des-salaires-avec-la-blockchain-du-bitcoin.N375227

[142] J.-M. Figuet, *op. cit.*, p. 9.

[143] O. Lakomski-Laguerre et L. Desmedt, *op. cit.*, §39 (citant, D. Ron et A. Shamir, « Quantitative analysis of the full Bitcoin transaction graph », 2012, https://eprint.iacr.org/2012/584.pdf).

Sous l'angle de la théorie institutionnelle de la monnaie, ces données semblent de nature à nuire à la reconnaissance des bitcoins comme nouvel ordre monétaire. Dans cette approche, la qualité d'une monnaie dépend de sa légitimité, de son acceptation inconditionnelle et non de sa valeur. Elle reposerait sur plus spécifiquement sur trois formes de confiance : méthodique, hiérarchique et éthique. Si la transparence du système est supposée permettre d'assurer la confiance méthodique et d'évincer la confiance hiérarchique relevant normalement de l'Etat ; non seulement, les vols observés ainsi que les problèmes techniques minent la confiance méthodique, mais surtout la structure du marché interroge la sincérité du fonctionnement décentralisé. Par ailleurs, les conditions du monnayage peuvent faire naître des doutes sur le plan éthique : le système de *proof of work* favorisant la concentration des mineurs, il est de nature à renforcer la structure oligopolistique du marché. En définitive, « *le Bitcoin reproduirait les caractéristiques d'une monnaie "capitaliste": accumulation, inégalités et concentration des richesses. Au-delà des formes politiques d'idéologie, la communauté ayant adopté le Bitcoin semble être traversée par deux systèmes de valeurs finalement antagonistes* »[144]. Face aux utilisateurs investis dans le projet initial et ayant tout intérêt au maintien d'une bonne réputation nécessaire à la généralisation progressive des monnaies numériques, ceux qui voient dans le bitcoin une simple opportunité d'investissement pourraient être attentifs uniquement à l'existence d'une forte demande – quitte à ce que celle-ci se nourrisse d'activités illicites[145].

Enfin, on ne saurait négliger le fait que les monnaies virtuelles n'apparaissent pas aujourd'hui comme un dispositif « grand public ». D'une part, « *[leur] disponibilité est faible par rapport aux moyens de paiement traditionnels assis sur la monnaie scripturale* »[146] ou par rapport à la monnaie fiduciaire – dont l'usage est en outre réellement anonyme. D'autre part, les transactions de faibles montants ne sont pas encouragées – du moins dans le réseau bitcoin, ce qui explique le développement de *side-chains*. Malgré ce que pourrait laisser penser la création du Satoshi (0.00000001 BTC), la plupart des mineurs n'acceptent effectivement qu'un

---

[144] O. Lakomski-Laguerre et L. Desmedt, *op. cit.*, §40.

[145] On notera toutefois que lors des auditions menées par la Commission des finances du Sénat, les professionnels impliqués dans les monnaies virtuelles ont au contraire appelé à une certaine régulation : « *L'audition du 15 janvier 2014 au Sénat a montré que certains acteurs privés présents sur le marché du* bitcoin *étaient en attente d'une régulation, ce dont il faut se féliciter. De nombreux acteurs français, regroupés au sein de l'*Association Bitcoin France*, ont ainsi appelé le 9 juillet 2014 à l'établissement d'un cadre réglementaire stable* » (régulation P. Marini et F. Marc, « Rapport d'information fait au nom de la Commission des finances sur les enjeux liés au développement du Bitcoin et des autres monnaies virtuelles », 23 juillet 2014, p. 11 (http://www.senat.fr/rap/r13-767/r13-7671.pdf).

[146] J.-M. Figuet, *op. cit.*, p. 6.

nombre limité de transactions de moins de 0,001 BTC (soit environ 0,5 dollar) par minute[147]. Et il faut encore ajouter que leur reconnaissance, en tant que moyen d'échange répandu, est toujours gênée par la mauvaise réputation qu'elles ont acquise en étant très régulièrement associées dans la presse[148] aux activités illicites du *Darknet*, au financement du terrorisme, et aux actes de piratages.

2.c Approche institutionnelle

Les approches quantitatives et qualitatives le montrent, la dimension disruptive des monnaies virtuelles ne repose pas sur sa capacité à supplanter les monnaies légales. C'est davantage sur le principe de désintermédiation que repose leur originalité et leur caractère précurseur. En ce sens, l'invention de Satoshi Nakamoto pourrait bien constituer une opportunité : « *la cryptographie et les réseaux informatiques permettraient à leurs utilisateurs de construire des espaces marchands sans banque et basés sur des relations interindividuelles. [...] En termes de pouvoir monétaire et financier, les crypto-monnaies constitueraient un moyen de "démocratiser la finance" au sein d'espaces alternatifs (transnationaux)* »[149].

Mais cette invention pourrait aussi être un risque, encouru par les acteurs institutionnels du système bancaire traditionnel. C'est en tout cas ainsi qu'aux Etats-Unis les choses ont pu être présentées : « *In February 2014, Federal Reserve Chair Janet Yellen told the Senate Banking Committee that "Bitcoin is a payment innovation that's taking place outside the banking industry. To the best of my knowledge there's no intersection at all, in any way, between Bitcoin and banks that the Federal Reserve has the ability to supervise and regulate"*[150]*. Nonetheless, the Federal Reserve Board, in its May 9, 2014, joint meeting with its Federal Advisory Council, considered Bitcoin's potential as "a threat to the banking system,*

[147] J. Bonneau, *op. cit.*, p. 6 : « *default nodes refuse to relay more than a few thousand transactions below B0.001 per minute as a penny-flooding defense* ».

[148] Même la production des institutions publiques participe à dépréciation des monnaies virtuelles. Voir, par exemple, B. Berton, European Union Institute for Security Studies, « The dark side of the web: ISIL's one-stop shop? », *Isssue Alert*, juin 2015, n° 30 (http://www.iss.europa.eu/uploads/media/Alert_30_The_Dark_Web.pdf).

[149] L. Desmedt, *op. cit.*, p. 9.

[150] Senate Committee on Banking, Housing, and Urban Affairs, *Semiannual Monetary Policy Report to the Congress*, 27 février 2014 (disponible en vidéo : http://www.banking.senate.gov/public/index.cfm?FuseAction=Newsroom).

economic activity, or financial stability"[151] *and appears to have adopted a policy that may be characterized as watchful waiting* »[152].

Plus prosaïquement, le *Federal Advisory Council* considère que les monnaies virtuelles ne sont pas à court terme une menace pour le système bancaire, mais qu'à long terme leur développement peut impliquer l'adaptation de ce dernier[153]. Cette opinion semble partagée aussi bien par les institutions de supervision que par les groupes bancaires[154].

De nombreuses initiatives privées ont ainsi vu le jour pour comprendre et superviser le phénomène des monnaies virtuelles[155]. Cependant, il semble que les acteurs institutionnels s'intéressent désormais moins au risque qu'elles représenteraient pour le système bancaire traditionnel qu'aux opportunités technologiques qu'elles ouvrent[156]. C'est en effet davantage sur la Blockchain que les initiatives concrètes ont été prises[157]. L'utilisation d'un registre d'opérations, que la cryptographie permet d'identifier et de rendre irréversibles, est de nature à permettre de simplifier grandement les transferts internationaux d'argent et à réduire les

---

[151] Federal Advisory Council and Board of Governors of the Federal Reserve System, *Record of Meeting*, 9 mai 2014 (http://www.federalreserve.gov/aboutthefed/fac.htm/).

[152] Congressional Research Service, « Bitcoin : Questions, Answers, and Analysis of Legal Issues », 13 octobre 2015, p. 13 (https://www.fas.org/sgp/crs/misc/R43339.pdf).

[153] Federal Advisory Council and Board of Governors of the Federal Reserve System, *Record of Meeting*, 9 mai 2014, p. 10 : les objectifs identifies sont les suivants : baisse des coûts, travail sur l'inclusion bancaire dans les pays en voie de développement, meilleure convertibilité entre les monnaies.

[154] Voir par exemple pour la Bank for International Settlements (société anonyme qui regroupe les banques centrales), Committee on Payments and Market Infrastructures, *Report on Digital Currencies*, novembre 2015, p. 13-14 (https://www.bis.org/cpmi/publ/d137.pdf).

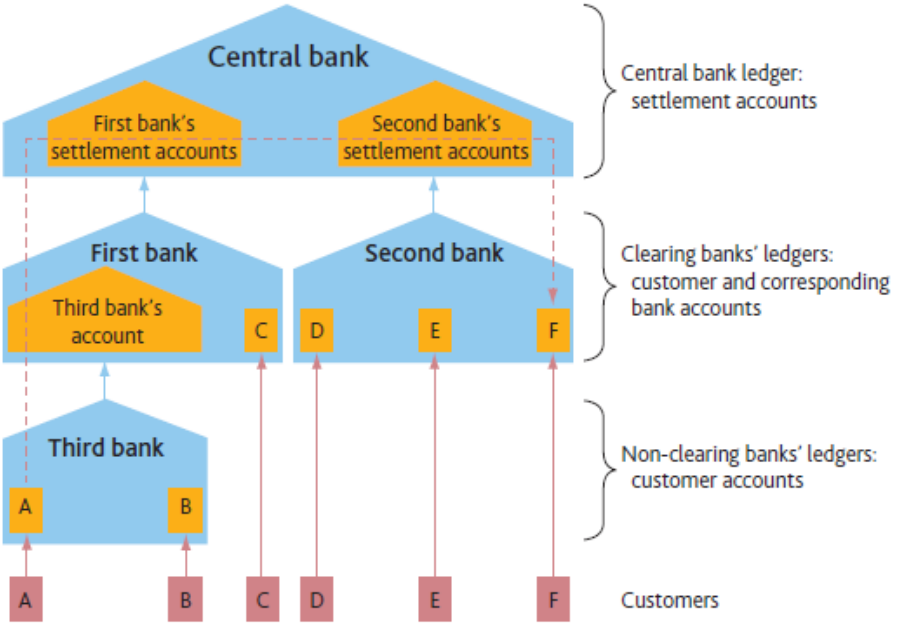
[155] Voir par exemple, pour la BNP, J. Palychata, « Bitcoin and blockchain. What you didn't know but always want to ask », *Quintessence. Smart thinking in finance* (http://securities.bnpparibas.com/quintessence/hot-topics/beyond/bitcoin-and-blockchain-what-you.html).

[156] Voir pour une illustration, les rapports Deloitte : *Banking reimagined. How disruptive forces will radically transform the industry in the decade ahead*, 2016, p. 8-11 (http://www.felabancelaes.com/downloads/us-fsi-banking-industry-outlook-2016_Deloitte.pdf) ; *Blockchain. Enigma. Paradox. Opportunity*, 2016, p. 8 et s. (http://www2.deloitte.com/uk/en/pages/innovation/articles/blockchain.html). On signalera toutefois l'étude réalisée par l'Independant Community Bankers of America, qui s'intéresse à la possibilité d'appliquer aux monnaies virtuelles les réglementations existantes : ICBA, « Virtual Currency : Risk and Regulation », 23 juin 2014, p. 12-24 (disponible en ligne : https://www.theclearinghouse.org/~/media/files/research/20140623%20tch%20%20icba%20virtual%20currency%20white%20paper%20june%20%202014%20revised.pdf).

[157] Cinquante acteurs majeurs du secteur financier, dont neuf grandes banques d'investissement (Goldman Sachs, Barclays, BBVA, Commonwealth Bank of Australia, Credit Suisse, JPMorgan, State Street, Royal Bank of Scotland et UBS), se sont ainsi alliés à une start-up new-yorkaise R3. Cette société, à l'image de nombreuses autres, telles que Ethereum ou Ripple, travaille sur les débouchés commerciaux des registres distribuées (voir, pour une analyse des opportunités offertes par la Blockchain d'Ethereum – à laquelle onze partenaires du consortium recourent depuis janvier 2016 pour partager un registre commun : http://r3cev.com/blog/2016/6/2/ethereum-platform-review).

frais de transaction en évitant d'avoir à solliciter des banques intermédiaires[158], mais c'est toute l'architecture bancaire – coiffée par les banques centrales – qui pourrait être simplifiée.

Figure 1 A tiered payment system



Note: A payment from **A's** account to **F's** account passes through a number of intermediaries, which verify each step of the process. Participants only have sight of their own assets and liabilities. The solid lines indicate deposits and the dashed line payments.

159

Par ailleurs, le développement des monnaies virtuelles est également souligné comme une opportunité « à côté » du système bancaire traditionnel[160]. En favorisant les transactions à faible coût, elles permettraient à des populations qui en sont aujourd'hui exclues – parce qu'elles sont considérées par les banques comme une clientèle à risque – de se doter d'un moyen de paiement adéquat. A l'image de la monnaie électronique et des paiements mobiles,

---

[158] Santander InnoVentures, « The Fintech 2.0 Paper : rebooting financial services », juin 2015, p. 14 (https://www.finextra.com/finextra-downloads/newsdocs/the%20fintech%202%200%20paper.pdf). Selon les estimations de Goldman Sachs, le recours aux monnaies virtuelles pourrait induire 43 milliards de dollars d'économie pour les consommateurs (R. Leal, « Is Bitcoin the Future of Payments ? », *TOP OF MIND (Goldman Sachs Global Investment Research Paper)*, mars 2014, n° 21, p. 18 (disponible en ligne : http://www.paymentlawadvisor.com/files/2014/01/GoldmanSachs-Bit-Coin.pdf).

[159] Bank of England, « Innovations in Payment Technologies and the Emergence of Digital Currencies », *Quaterly Bulletin*, 2014, Q3, p. 2.

[160] EBA, *Opinion on 'Virtual Currencies'*, p. 18 : « *The potential benefit is therefore more likely to advantage non-EU countries, especially in the case of money remittances, as VCs offer a less expensive alternative to conventional remittances that cost, on average, 8.36% of the amount sent. Less developed countries may also benefit, for example by linking VC services to mobile payment services, allowing users to exchange their currency into Bitcoins via mobile phone* ».

les monnaies virtuelles en tant que dernière technologie favoriseraient ainsi le commerce dans les pays en voie de développement[161].

Enfin, l'irruption des monnaies virtuelles est l'occasion de voir apparaître de nouveaux acteurs dans le domaine des services de paiement. Si la question de l'encadrement juridique se pose dès lors que leur assimilation à des prestataires de service de paiement n'est pas acquise de manière systématique[162], cela ne semble pas oblitérer le dynamisme de ce secteur en plein essor : « *[d]e plus en plus de sites tels que iCBIT ou bitcoin-otc voient le jour depuis 2014, proposant des plateformes de* trading *en bitcoin et des produits dérivés de gré-à-gré. En janvier 2015,* Coinbase *a annoncé l'ouverture de la première plateforme de change, respectant la réglementation financière aux États-Unis[163], signe de la vitalité de la monnaie. Toutes ces entreprises ont émergé en un temps record. Loin de tarir, les* start-ups *dédiées à Bitcoin continuent de lever des montants astronomiques auprès d'investisseurs. Ainsi, la* start-up 21 Inc.*, dont le business model est gardé secret, a récolté récemment 105 M$* »[164].

Ces nouveaux arrivants sont, d'une part, une source de vitalité pour le secteur des paiements grâce aux innovations qu'ils y apportent et, d'autre part, vecteur d'investissements dans l'économie des crypto-monnaies. Ils ont encore l'avantage d'en démocratiser l'usage en proposant des portefeuilles électroniques ou permettant d'effectuer des opérations de change. De telles plates-formes sont toutefois aussi une source de fragilité : elles concentrent les

---

[161] Le conflit opposant Bitcoin et M-pesa au Kenya montre toutefois que l'insertion des monnaies virtuelles dans les services de paiement ne se fera pas nécessairement aisément. En l'occurrence, la société Bitpesa reproche à l'opérateur Safaricom d'avoir fait obstacle à la conversion en Bitcoin de la monnaie électronique M-pesa déployée sur son réseau mobile (voir sur ce litige : http://www.ibtimes.co.uk/bitcoin-versus-m-pesa-digital-payments-rumble-jungle-1531208 ; http://www.coindesk.com/kenyan-court-upholds-bid-keep-bitpesa-off-mobile-money-platform/).

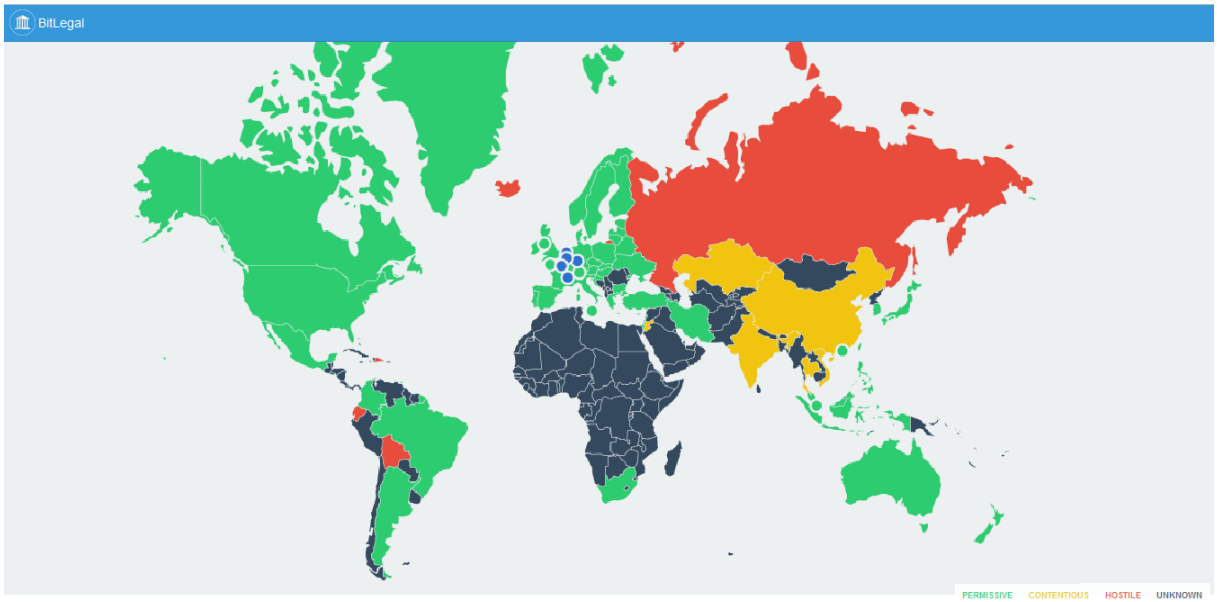
[162] Les prises de position des régulateurs en faveur de l'assimilation se multiplient. En France, la position 2014-P-01 de l'Autorité de contrôle prudentiel et de résolution (ACPR), adoptée le 29 janvier 2014, précise que « *l'activité d'intermédiation consistant à recevoir des fonds de l'acheteur de Bitcoins pour les transférer au vendeur de Bitcoins relève de la fourniture de services de paiement. Exercer cette activité à titre habituel en France implique de disposer d'un agrément de prestataire de services de paiement (établissement de crédit, établissement de paiement ou établissement de monnaie électronique) délivré par l'ACPR* ». Cela implique pour un tel opérateur de respecter toutes les règles applicables aux activités de PSP, notamment en matière prudentielle. Selon l'ACPR, la réglementation sur les services de paiement ne s'applique toutefois à cet intermédiaire (en pratique une plateforme de négociation) que sur la « jambe » de la transaction relative à la monnaie ayant cours légal et pas sur celle relative à la monnaie virtuelle. Paymium, qui est propriétaire de la plate-forme Bitcoin-central, a ainsi simplement conclu un accord avec l'établissement de paiement agréé Aqoba pour héberger les comptes en euro de sa société. La même exigence se retrouve, par exemple, au Luxembourg où la plate-forme Bitstamp a obtenu l'agrément d'institution de paiement auprès de la Commission de surveillance du secteur financier (CSSF). A la différence des règles applicables aux Etats-Unis qui imposent un agrément Etat par Etat, en vertu du droit de l'Union ce passeport lui ouvre désormais l'accès à l'ensemble du marché européen.

[163] Coinbase, numéro 1 sur le marché américain, n'aurait toutefois pas obtenu d'agrément dans une quinzaine d'Etats fédérés (http://www.agefi.fr/banque-assurance/actualites/quotidien/20160426/bitstamp-amene-trading-bitcoin-dans-nouvelle-ere-180383).

[164] N. Clausset et A. Sellem, *op. cit.*, p. 4.

risques de piratage et de vol. Elles ont donc fait l'objet d'une attention particulière de la part des autorités nationale de régulation, qui cherchent en particulier à leur imposer le respect d'obligations prudentielles.

3. ANALYSE JURIDIQUE



Alors que pour une partie importante des économistes, la « *nature monétaire du bitcoin n'est donc pas avérée économiquement* »[165], ce résultat ne saurait s'imposer nécessairement en droit. La règle juridique, et la qualification qu'elle emporte, possède en effet une dimension instrumentale qui pourrait justifier d'appréhender les monnaies virtuelles comme des monnaies légales au sens légale du terme. Cependant, au débat soulevé par l'approche économique, répondent les incertitudes quant à la qualification en droit de cet « *OVNI juridique et fiscal* »[166]. Les deux univers scientifiques partagent donc une même interrogation, sans que les réponses qu'ils apportent soient nécessairement pleinement interdépendantes. Ainsi, certaines décisions de justice rendues à propos des monnaies virtuelles n'hésitent pas à *assimiler* le bitcoin à une monnaie au sens juridique du terme.

Incitée en ce sens par la *Securities and Exchange Commission* (*SEC*), dans une affaire où l'agence accusait des opérateurs d'avoir mis en place une pyramide de Ponzi, une cour fédérale de district au Texas[167] a considéré que les bitcoin sont utilisés comme de la monnaie

[165] L. Desmedt, *op. cit.*, p. 11
[166] H. de Vauplane et S. Cazaillet, *op. cit.*, p. 1
[167] Voir *infra*.

pour acheter des biens ou des services et peuvent être échangés contre des monnaies conventionnelles. En conséquence, la juridiction a accepté de voir dans les contrats passés avec les sociétés en cause des contrats d'investissement au sens de la législation américaine[168]. La même fiction ou analogie a été retenue par la Cour de justice de l'Union européenne dans le cadre d'un litige relatif aux opérations de change et à la possibilité d'exempter de la TVA la rémunération acquise lors des opérations de conversion[169].

Comme ces exemples le montrent, l'absence de régulation propre aux monnaies virtuelles ne les fait pas entrer dans une sphère de non droit. En pratique, les différentes autorités publiques se sont évertuées, après avoir identifiés les risques encourus, à rappeler qu'un certain nombre d'obligations « générales » pouvaient, en l'état du droit, être considérées comme applicables aux opérations impliquant des monnaies virtuelles. Si les positions adoptées dans le monde par les autorités publiques peuvent être rapprochées et s'il est possible d'identifier des traits communs, il n'en demeure pas moins – comme le montre le planisphère reproduit ci-dessus – qu'une très grande diversité règne sur le traitement juridique des monnaies numériques. On peut se demander dans quelle mesure cette situation est satisfaisante face à une technologie déterritorialisée s'appuyant sur un réseau global. Il semble à cet égard qu'une régulation adéquate gagnerait à s'appuyer sur une coopération ou du moins sur un large consensus entre les Etats.

3.a Prises de position des autorités publiques

Le bitcoin soulève un risque financier, c'est évident au regard des données économiques développées précédemment : « *Aucune institution n'apporte sa garantie au bitcoin, aussi bien pour les "dépôts" des utilisateurs que pour la stabilité de son cours. [...] Sa forte volatilité expose donc les utilisateurs au risque de pertes importantes. Par ailleurs, en l'absence d'un animateur de marché, alors que le nombre d'utilisateurs semble encore réduit, le risque de liquidité est fortement présent. Le marché pourrait en effet s'assécher rapidement en cas d'une brusque perte de confiance, empêchant les utilisateurs de se séparer de leurs bitcoins* »[170].

[168] L'*ICBA* précise que si les Bitcoins peuvent constituer le support de contrats d'investissement, entrant dans le champ de compétence du *SEC*, la qualification d'instrument financier ne serait pas pertinente (« Virtual Currency : Risk and Regulation », *op. cit.*, p. 16 et s.).

[169] CJUE, 22 octobre 2015, *Skatteverket c. David Hedqvis*, Aff. C-264/14.

[170] N. Clausset et A. Sellem, *op. cit.*, p. 2.

Ces éléments sont aggravés par un risque technique ou opérationnel, lié à un système informatique dont la vulnérabilité est attestée par les faillites de plates-formes comme MtGOx qui ont fait suite aux vols de bitcoins par piratage[171]. On peut s'interroger, encore, sur l'existence d'une tendance à la cartellisation du minage, qui viendrait obérer le bon fonctionnement du mécanisme de consensus et des règles de monnayage au détriment des usagers. La rémunération des mineurs en vertu du système de *proof of work* ayant effectivement entrainé une course à l'équipement informatique (*hashrate war*), la possibilité de procéder au minage de façon isolée est devenue illusoire. L'augmentation constante du coût de l'opération de résolutions des algorithmes a rendu impérative l'augmentation parallèle des chances d'obtenir la récompense attribuée pour la création d'un nouveau *block*. Pour ce faire, les mineurs se sont donc regroupés en « coopératives » (*mining pools*), ce qui a conduit à une concentration des acteurs difficilement compatible avec la logique initiale d'un fonctionnement décentralisé du bitcoin.

La coopérative Ghash.io a ainsi réussi le 12 juin 2014 à posséder plus de 51% de la puissance de minage[172], entrainant une chute du cours en dollars des bitcoins. Si la société a rapidement annoncé s'engager à ne plus atteindre ce seuil[173], et a divisé le pool en plusieurs groupes distincts depuis, cet évènement montre la faisabilité d'une attaque *goldfinger* sur les monnaies virtuelles[174].

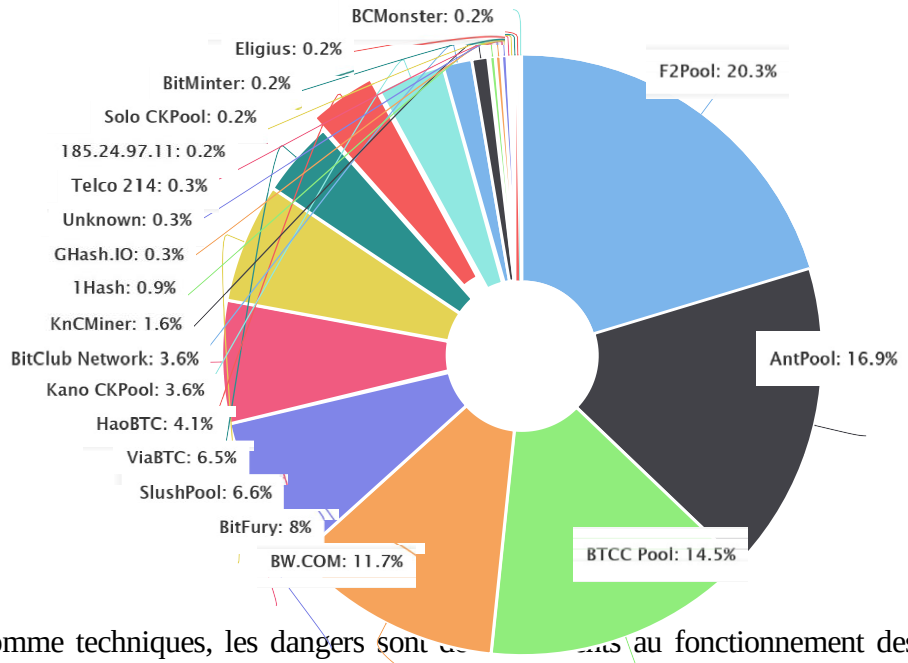
---

[171] N. Godlove, *op. cit.*, p. 18-20 : l'auteur souligne que le « vol » d'un million de dollar subi par la place d'échange BIPS en 2013 n'a pas pu être qualifié juridiquement de vol par la police danoise à défaut de soustraction matérielle. On rencontre la même difficulté en droit français, ce qui sera abordé lors de la journée de conférence, mais aussi en Allemagne. A l'inverse, il semble que la jurisprudence néerlandaise ait adopté une définition du vol qui ne se limite pas à la soustraction d'objet physique : « *the Supreme Court classified virtual goods as property and sentenced a teenager for stealing virtual money and virtual goods in the online fantasy role playing game Runescape* ». Les juridictions américaines ont rendu des décisions allant en ce sens à propos des noms de domaine, mais la situation des monnaies virtuelles restent incertaines (F. Boehm et P. Pesch, « Bitcoin: A First Legal Analysis - with reference to German and US-American law », in Financial Cryptography and Data Security, *Springer*, 2014, p. 49).

[172] Pour une présentation vidéo des risques qu'entrainent cette situation, voir : https://www.youtube.com/watch?v=6luEMwSAS0I&feature=youtu.be

[173] https://ghash.io/ghashio_press_release.pdf

[174] Le coût d'une attaque 51 %, ou *Goldfinger*, a été évalué par Jean-Paul Delahaye à 300 millions d'euros : « L'attaque Goldfinger d'une Blockchain », janvier 2015 (http://www.scilogs.fr/complexites/lattaque-goldfinder-dune-blockchain/).



Financiers comme techniques, les dangers sont de[illegible]its au fonctionnement des monnaies virtuelles. Ce n'est cependant qu'à partir de 2013, au moment où la valeur du bitcoin est montée en flèche, que les autorités nationales ont réellement compris la nécessité de s'intéresser aux risques induits par les monnaies virtuelles. Elles ont dès lors cherché à en dresser un tableau exhaustif.

L'identification des principaux risques

Les risques identifiés par les autorités nationales sont tout aussi nombreux que les études qui y sont désormais consacrées. Comme le constate Hubert de Vauplane, « *[l]es régulateurs publient de plus en plus des documents d'études sur les "monnaies virtuelles", soulignant, le plus souvent, les dangers de leur utilisation. Ainsi, en 2014, en France, la Banque de France (2013), puis l'Autorité de contrôle prudentiel et de résolution (ACPR, 2014) et l'Autorité des marchés financiers (AMF, 2014) ont chacune de leur côté mis en garde sur leur utilisation. En Europe, le régulateur bancaire européen, l'Autorité bancaire européenne (ABE, 2014), mais aussi la Banque centrale européenne (BCE, 2012) se sont penchés sur les risques associés à celles-ci (70 risques ont ainsi été identifiés !)* »[175]. On renverra au tableau réalisé par l'Autorité Bancaire Européenne, reproduit en annexe 3, pour une énumération exhaustive. Pour donner un exemple des problèmes généralement identifiés, la Banque de France dans la publication du 5 décembre 2013 a dressé la liste suivante : l'absence de garantie de remboursement pour les consommateurs, la nature hautement spéculative, le vide juridique autour des plates-formes et plus particulièrement en ce qui concerne les obligations de

[175] H. de Vauplane, « L'analyse juridique du Bitcoin », *op. cit.*, p. 352.

liquidité, l'absence de cours légal, la compatibilité avec la législation sur le blanchiment et le financement du terrorisme[176].

Les trois thématiques les plus régulièrement mises en avant sont le blanchiment d'argent, l'utilisation des monnaies virtuelles pour des activités illégales et terroristes, et la protection des utilisateurs. Les deux premiers points sont liés à l'anonymat des transactions (dont le caractère est plus ou moins relatif selon les crypto-monnaies[177]) et à l'absence d'attaches territoriales. Les autorités regrettent ainsi qu'il soit possible avec un simple accès internet d'ouvrir un portefeuille sans révéler son identité (seule l'adresse IP sera effectivement connue), afin de procéder rapidement et sans intermédiaires à des paiements irrévocables à travers le monde. De même, les monnaies numériques pâtissent des liens existants entre *bitcoin* et le *darknet* – liens que la fermeture par le FBI du site de vente illégal *Silk Road* a mis en lumière[178], ou de son utilisation par les pirates informatiques lors de leur demande de rançon[179]. Au lendemain des attentas de Paris, la France a ainsi fait part lors du Conseil européen extraordinaire du 20 novembre 2015 de son souhait de voir les monnaies virtuelles mieux encadrées afin de limiter les possibilités de financement souterrain du terrorisme[180].

Le dernier point met en cause pour sa part les qualités économiques des monnaies virtuelles et en particulier le risque dû à la volatilité des taux de change. Bien qu'il s'agisse deux types différents d'usage, les autorités nationales considèrent qu'elles sont dangereuses aussi bien pour les consommateurs que pour les investisseurs[181] qui pourraient être victimes de « pyramide de Ponzi ».

---

[176] Banque de France, « Les dangers liés au développement des monnaies virtuelles : l'exemple du bitcoin », *Focus*, 5 décembre 2013, n° 10.

[177] Des éléments extérieurs doivent être recoupés avec les données de la Blockchain pour identifier les propriétaires. Des logiciels, tel que Blockchain Inspector, sont développés afin de faciliter ces investigations (pour une présentation de ce dernier, voir http://www.charentelibre.fr/2016/04/19/les-bitcoins-suivis-a-la-trace-en-charente,3029369.php).

[178] N. Godlove, *op. cit.*, p. 15-16. *Silk Road* permettait d'acheter drogues et marchandises prohibées en utilisant des Bitcoins. La plate-forme de vente a été fermée en octobre 2013.

[179] Voir, pour une présentation de ces attaques appelées *Ransomware*, L. Constantin, « Le ransomware CBT-Locker stocke les clefs de chiffrement sur la blockchain », 16 avril 2016, le Monde informatique (http://www.lemondeinformatique.fr/actualites/lire-le-ransomware-ctb-locker-stocke-les-cles-de-dechiffrement-sur-blockchain-le-monde-informatique-64548.html).

[180] « Après les attentats, les monnaies virtuelles sous haute surveillance », *La Tribune*, 19 novembre 2015 (http://www.latribune.fr/technos-medias/internet/apres-les-attentats-les-monnaies-virtuelles-sous-haute-surveillance-523749.html). Les propositions française présentées lors de ce conseil « JAI » sont accessibles à l'adresse suivante : https://www.dropbox.com/s/t40eyae1200ea1q/eu-jha-council-french-proposals.pdf?dl=0).

[181] L'enquête ouverte par le NYSDFS le 11 août 2014, auprès de 22 sociétés ayant des activités liées au Bitcoin, s'appuyait sur le risque de méconnaissance des dispositions relatives aussi bien au blanchiment d'argent, qu'à la protection des consommateurs et des investissements. On retrouve cette double préoccupation dans le *Regulatory Framework* du 24 juin 2015 (Sect. 200.19) à l'origine de la *Bitlicence* (voir *infra*)

Au lendemain du scandale provoqué par Mt Gox, le besoin de protection des consommateurs est une évidence pour l'ensemble des régulateurs. Outre le problème de compréhension lié à la fluctuation du cours de change des monnaies virtuelles, il est apparu à plusieurs reprises que la sécurité des portefeuilles électroniques offerts par les opérateurs n'est pas toujours suffisante[182]. Les avertissements sur les dangers encourus par les consommateurs se sont multipliés. Ainsi, le *Government Accountability Office* américain (GAO), après avoir publié un rapport remarqué sur le sujet[183], a-t-il pressé le nouveau *Consumer Financial Protection Bureau* (CFPB) de s'emparer du sujet – ce qu'il a fait en publiant un avertissement très didactique à l'intention des utilisateurs en août 2014[184]. On peut penser cependant que la protection des consommateurs ne doit pas seulement être appréhendée sous l'angle financier. Il faut ainsi s'interroger sur les conditions dans lesquelles ceux-ci peuvent bénéficier du droit de rétractation lors des achats effectués en *bitcoin* (dont les transactions sont supposées être irréversibles), ou encore sur la législation applicable et la juridiction compétente en cas de litige[185].

Le risque encouru par les investisseurs a lui été mis en exergue dans une affaire judiciaire texane[186] : District Court de Sherman (Texas), 18 septembre 2014, *Securities and Exchange Commission (SEC) v. Trendon T. Shavers and Bitcoin Savings and Trust* (Civil Action N°4: 13-CV-416). La méfiance des autorités américaines a conduit à la condamnation d'une entité et de ses dirigeants pour violation de la réglementation applicable au marché de titres financiers. La vigilance de la *SEC* à l'égard de ce risque d'escroquerie se matérialise par des

---

[182] Ainsi, entre les scandales de MtGox et de Cryptsy, c'est la plateforme Flexcoin qui a dû fermer suite à la déclaration du vol des Bitcoins qu'elle conservait pour ses clients et qui sont désormais perdus pour eux (http://www.lemonde.fr/argent/article/2014/03/06/apres-mtgox-la-plateforme-flexcoin-ferme-victime-d-un-vol_4378348_1657007.html).

[183] Le *GAO* est un organe qui relève du Congrès américain et qui contrôle l'utilisation du budget par l'administration fédérale. Le rapport rendu en mai 2014 est disponible à l'adresse suivante : http://gao.gov/assets/670/663678.pdf

[184] http://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf

[185] Il est même possible de s'interroger sur la possibilité de former réellement un contrat de vente, alors que la formation de tel contrat dépend généralement du transfert d'un certain montant de monnaie légale (F. Boehm et P. Pesch, *op. cit.*, p. 50).

[186] N. Godlove, *op. cit.*, p. 27 : « *A Southlake oil and gas company ran afoul of Texas securities regulators after raising capital through the bitcoin. The Texas State Securities Board ordered Balanced Energy to stop selling securities on the grounds that it had failed to disclose to its investors the risk of financing operations through a virtual currency subject to large fluctuations in value* »

enquêtes fréquentes[187] et par la publication durant l'année 2015 d'un document d'information à l'intention des investisseurs[188].

Les réactions juridiques

S'agissant des réactions juridiques qui ont suivi l'énonciation des risques induits par les monnaies virtuelles, une opposition peut être faite entre les agissements des autorités administratives exerçant des fonctions de régulation, et les interventions législatives[189]. Cette présentation, certes schématique, a vocation à distinguer d'un côté les actions entreprises ou possible sans modification du corpus législatif et de l'autre celles qui supposent une intervention parlementaire.

Les régulateurs

Le premier réflexe des autorités administratives de régulation consiste généralement à justifier leur action, en démontrant que les risques induits par les monnaies virtuelles entrent dans leur champ de compétence. L'attitude des agences de l'Union européenne en est une illustration parfaite. Ainsi, en 2012, la Banque centrale européenne (*BCE*) motivait sa décision de se saisir de la problématique en ces termes : « *Consequently, it seems appropriate to consider the extent to which they might affect a central bank's tasks in the areas of payment systems, regulation, financial stability, monetary policy and price stability* »[190]. De même, l'Autorité bancaire européenne (*EBA*) a affirmé, en raison de sa mission de contrôle des activités financières, sa vocation à superviser le fonctionnement des monnaies virtuelles dès 2013[191]. Il en résulta la production d'un rapport complet en 2014 qui, à partir de l'analyse des risques et bénéfices[192], proposait les principes d'une réglementation jugée nécessaire et particulièrement exigeante[193]. Une fois leur compétence justifiée, les administrations

---

[187] Voir par exemple, l'ouverture d'une enquête à l'encontre d'une société de minage : http://www.sec.gov/news/pressrelease/2015-271.html.

[188] https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf

[189] Pour un rappel des principales réactions juridiques, actualisé jusqu'au mois de mars 2016, voir : https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html#EU ainsi que le tableau de l'AMF reproduit en annexe 4 ; et plus particulièrement pour l'actualité juridique des monnaies numériques aux Etats-Unis : https://www.virtualcurrencyreport.com/

[190] BCE, *Virtual currency schemes*, Francfort, 2012, p. 34 et s.

[191] Dans un communiqué de presse du 13 décembre 2013, l'agence prévenait les consommateurs des risques encourus, notamment du fait de l'absence de réglementation en cas de défaut ou de cessation d'activité des plateformes, et affirmait mener des investigations plus poussées sur le sujet (https://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies).

[192] Sur les méthodes de travail de l'EBA, voir D. Haubrich, « The monitoring and Regulation of Financial Innovation : The Case of Virtual Currencies and the European Banking Authority », *RISF*, 2014, n° 4, p. 28-38.

[193] EBA, *Opinion on 'virtual currencies'*, 2014, p. 38 et s. : l'agence fait notamment de l'identification du créateur d'une monnaie virtuelle l'une des premières nécessités, car il voit le moyen de clarifier le système de gouvernance des

nationales développent généralement une politique graduelle et progressive. Comme cela vient d'être rappelé, les régulateurs ont mis en place des processus d'information et de monitoring des activités liées aux monnaies numériques avant d'expliciter leur position à l'égard de ce phénomène nouveau[194]. Ainsi, durant une phase initiale, « *les autorités américaines en charge de surveiller le secteur financier se sont ponctuellement contenter d'indiquer les conditions dans lesquelles pourraient être appréhendées, le cas échéant, celles des activités, qui impliquant des monnaies virtuelles, seraient susceptibles de tomber dans leur champs de compétence* »[195]. Dans le même temps, elles ont proposé des analyses techniques du fonctionnement des monnaies virtuelles et tout particulièrement du bitcoin[196].

Ce travail d'analyse permis alors aux régulateurs d'émettre des mises en garde[197], mais surtout de justifier l'application de telle ou telle législation qu'ils ont la charge d'appliquer. Ainsi, à titre d'illustration, le bureau du Département du Trésor nord-américain qui lutte contre le blanchiment (*FinCEN*) a très rapidement averti qu'il considérait les opérations de conversion entre monnaies virtuelles, ou entre l'une d'elles et une monnaie fiat, comme entrant dans le champ du *Bank Secrecy Act* de 1970[198]. Les plateformes de conversion

---

monnaies virtuelles et d'en responsabiliser les acteurs. Elle considère également, afin de protéger les investisseurs, qu'une réglementation analogue à celle qui assure la sincérité des marchés financiers devrait être transposée.

[194] Voir en dernier, la position adoptée par le *Home Office* britannique à la suite d'un appel à information : HM Treasury, *Digital Currencies : Response to the Call for Information*, Mars 2015, 28 p. (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf).

[195] V. Jamet, *op. cit.*, p. 12.

[196] Voir par exemple, A. Badev et M. Chen, Federal Reserve Board, « Bitcoin: Technical Background and Data Analysis », *Finance and Economics Discussion Series*, 2014, n° 104, 34 p. (http://www.federalreserve.gov/econresdata/feds/2014/files/2014104pap.pdf).

[197] Ce fut notamment l'attitude des autorités chinoises dès 2013 : « *The People's Bank of China, among five Chinese agencies released a notice that they would not use virtual currency that citizens of the country would still be allowed to buy and sell, but it warned that participants "assume the risks themselves." This lack of protection is likely a calculated disincentive for the use of virtual currency in China, ensuring that Chinese banks retain tight control of the Yuan* » (N. Godlove, *op. cit.*, p. 20). De même, le 12 décembre 2013, *l'EBA* publiait également un avertissement sur l'absence de régulation spécifique et en conséquence de protection pour ceux qui souhaiteraient acheter, détenir ou vendre des bitcoins (https://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies). Au final, au regard des observations présentées dans le rapport de la *BCE* de 2015, il semble que la volonté d'avertir des risques est très largement partagées par les institutions publiques compétentes : « *Several central banks and supervisory authorities warned about risks associated with Bitcoin and/or virtual currency schemes in general. For example, the German Federal Financial Supervisory Authority (BaFin), the Banque de France and the Dutch and Belgian central bank and supervisor have published warnings about the possible use of Bitcoin in money laundering and financing terrorism, the lack of supervision, price fluctuations and security risks. The Deutsche Bundesbank has given such warnings in interviews. Outside Europe, the People's Bank of China, the Reserve Bank of India, the Monetary Authority of Singapore and Bank Indonesia are among those warning of the risks of Bitcoin* » (*Virtual currency schemes*, 2015, *op. cit.*, p. 30).

[198] FinCEN, « Guidance on the Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies », 18 mars 2013 (FIN-20013-G001). Cette position résultait déjà de la définition des services de transfert de fond adoptée par le bureau depuis juillet 2011, laquelle incluait la réception de toute valeur ayant vocation à se substituer à la monnaie.

seraient donc dans l'obligation de coopérer avec les agences américaines, de leur signaler les mouvements journaliers d'un montant de plus de 10 000 dollars, et de conserver les informations des transactions effectuées d'un montant de plus de 3 000 dollars. De même, dès 2014, la *SEC* a adopté des sanctions administratives contre des opérateurs ayant omis d'accompagner l'offre au public d'actions libellées en bitcoin de prospectus d'émission requis par la législation financière[199].

On peut toutefois s'interroger sur la pertinence de cette approche à droit constant, car elle ne remplit pas les exigences de sécurité juridique que l'on attend de toute régulation. La difficulté vient premièrement de la force contraignante parfois incertaine de ces diverses recommandations, prises de positions, ou « *interventions "doctrinales"* »[200] des autorités de régulations. Ceci tient, notamment, à leur faible portée hiérarchique qui induit leur fragilité en cas de contestation juridictionnelle[201]. Pour une sécurité juridique accrue, il semblerait donc souhaitable que la validité de ces analyses soient *a minima* confirmées, soit par une autorité juridictionnelle, soit par une autorité législative. Deuxièmement, si les prises de position se multiplient, elles restent parcellaires – de nombreux régulateurs n'ont pas encore explicité leur attitude vis-à-vis des monnaies virtuelles (ce problème est particulièrement significatif aux Etats-Unis en raison de la multiplicité des agences fédérales concernées par les activités impliquant les monnaies virtuelles)[202] – et sont potentiellement contradictoires. Un exemple permettra d'en donner illustration. Dans le cadre de sa décision, la Cour de justice de l'Union était amenée à examiner des activités d'échange de devises. Elle a considéré qu'au sens du droit de l'Union celles-ci ne constituent pas des activités de service de paiement. En conséquence, la plate-forme en cause ne semble pas devoir être qualifiée de prestataire de service de paiement. La compatibilité entre cette jurisprudence et la position défendue par la

---

Des décisions individuelles adoptées en 2014 sont venues préciser la position du bureau, qui a ainsi pu confirmer que si les opérations de change impliquant les monnaies virtuelles sont visées par le *BSA*, tel n'est pas le cas pour les opérations de minage, la création et la distribution de logiciel permettant l'achat et la vente de monnaies virtuelles, mais aussi – de manière plus étonnante – pour les opérations en monnaie virtuelle réalisées pour compte propre (c'est-à-dire l'achat et la vente de monnaie virtuelle liés à une activité de placement).

[199] Voir SEC, « SEC Charges Bitcoin Entrepreneur With Offering Unregistred Securities », *Communiqué de presse n° 2014-111* (www.sec.gov/litigation/admin//014/33-9592.pdf).

[200] V. Jamet, « La "Bitlicense" – Perspective nord-américaine d'un cadre juridique pour une "bitgénération" encore en devenir », *RISF*, 2014, n°4, p. 16.

[201] En ce sens, H. de Vauplane, « L'analyse juridique du Bitcoin », *op. cit.*, p. 355.

[202] Voir pour les Etats-Unis, V. Jamet, *op. cit.*, p. 16 : « *Au total, il apparaît donc qu'à l'échelon fédéral le phénomène des monnaies virtuelles reste appréhendé de manière ponctuelle et fragmentée par les différentes agences chargées de superviser le secteur financier. Faute d'une adaptation du* corpus *législatif, ces dernières ne peuvent en effet intervenir que dans la stricte limite de leurs attributions et pour autant que les opérations en cause soient susceptibles d'intégrer une qualification juridique préexistante* ».

Banque de France[203] comme par l'ACPR[204], lesquelles qualifient d'établissements de paiement soumis à l'obligation de détenir un agrément les organismes effectuant des opérations de change impliquant des euros, n'est donc pas certaine...

Cette méthode initiale, qui se propose à droit constat de faire entrer par défaut les monnaies virtuelles dans des régimes existants et de multiplier les avertissements quant aux risques encourus par les utilisateurs[205], a toutefois été complétée par certaines autorités administratives par une réflexion en amont sur la nécessité d'une législation spécifique[206]. Ainsi, dès 2013, « *en l'absence de réforme adoptée au niveau fédéral, certains Etats fédérés envisagent [...] d'amender leur corpus législatif et/ou réglementaire* »[207]. C'est dans cette logique que, le 17 juillet 2014, le *New York State Department of Financial Services* a créé la *Bitlicense*[208].

Cet outil apparaît comme une réglementation juridique spécifique, susceptible d'être transposée dans d'autres systèmes juridiques[209]. Le *regulatory framework* adopté par l'agence américaine

---

[203] Banque de France, *op. cit.*, p. 5-6. La position de la Banque de France se fonde sur la distinction entre les activités d'émission et de conversion des monnaies virtuelles : « *S'il n'est pas possible de réguler l'émission des monnaies virtuelles (conçue pour échapper à tout contrôle de la sphère publique et ne répondant à aucune qualification au regard de la réglementation bancaire et financière actuellement en vigueur), en revanche, l'activité de change/conversion de ces monnaies virtuelles en devises ayant cours légal entre bien dans le champ de la réglementation. Il s'agit en premier lieu de la lutte contre le blanchiment et le financement du terrorisme qui appelle une surveillance des services de conversion contre monnaie ayant cours légal. [...] Or cette activité de conversion contre monnaie ayant cours légal offerte par les plates-formes internet, comme bitcoin-central, doit s'analyser – dans la mesure où il y a réception, virement et tenue de comptes de fonds concernant une monnaie ayant cours légal – comme un service de paiement nécessitant un agrément de prestataire de service de paiement* ».

[204] Pour une analyse de cette position, voir notamment H. de Vauplanne, « L'analyse juridique du Bitcoin », *op. cit.*, p. 355-356.

[205] Pour ce qui est des autorités françaises : *ACPR*, « Position relative aux opérations sur bitcoins en France », *Position 2014-P-01*, 29 janvier 2014 (https://acpr.banque-france.fr/fileadmin/user_upload/acp/publications/registre-officiel/201401-Position-2014-P-01-de-l-ACPR.pdf) ; AMF, « Emergences des monnaies virtuelles : risques et opportunités ? », *Risques et tendances*, juillet 2014, n° 15, p. 59-68 ; Banque de France, « Les dangers liés au développement des monnaies virtuelles : l'exemple du bitcoin », *Focus*, 5 décembre 2013, n° 10, 6 p. ; Tracfin, *L'encadrement des monnaies virtuelles. Recommandations visant à prévenir leur usage à des fins frauduleuses ou de blanchiment*, juin 2014, 10 p.

[206] Sur les résultats de cette réflexion, voir E. L. Greebel, K. Moriarty, C. Callaway , G. Xethalis , « Recent key Bitcoin and virtual currency regulatory and law enforcement developments », *Journal of Investment Compliance*, 2015, Vol. 16, n° 1, p.13-18.

[207] V. Jamet, « La "Bitlicense" – Perspective nord-américaine d'un cadre juridique pour une "bitgénération" encore en devenir », *RISF*, 2014, n°4, p. 12.

[208] http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf

[209] La *CSBS* appelle ainsi de ses vœux l'adoption à l'échelle fédérale d'un système de licence, spécialement conçue pour les crypto-monnaies et obligatoire pour tout opérateur intervenant dans la transmission, l'échange ou le stockage d'unités (https://www.csbs.org/regulatory/ep/Documents/CSBS-Model-Regulatory-framework%28September%2015%202015%29.pdf). Cette solution paraîtrait plus rationnelle que la démarche actuelle reposant sur l'adoption de licence par les Etats fédérés (voir en ce sens, K. L. Penrose « Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws », *North Carolina Banking Institue Journal*, 2014, Vol. 18, p. 251 (https://www.law.unc.edu/journals/ncbank/volumes/volume18/citation-18-nc-banking-inst-2014/banking-on-bitcoin-applying-antimoney-laundering-and-money-transmitter-laws/ ; et pour un présentation des régimes adoptés par l'Etat

ne se contente pas de clarifier les obligations qui s'imposent en vertu du droit commun aux opérateurs de change, comme l'a fait l'ACPR en France[210], mais conduit à une double extension du cadre juridique contraignant pour l'utilisation des monnaies virtuelles.

Tout d'abord, il étend le champ des personnes et activités concernées puisque la *Bitlicense* vise toute « *Virtual Currency Business Activity* »[211] et que seuls les établissements bénéficiant d'un agrément bancaire en sont exemptés[212]. Il faut noter toutefois que des achats ou des opérations spéculatives peuvent être effectués par des particuliers comme par des professionnels ne détenant pas de licence[213].

Ensuite, ce sont les obligations qui s'imposent aux opérateurs qui sont très largement étendues par le *Regulatory Framework*. Si celui-ci rappelle et détaille les règles qui s'imposent dans le cadre de la lutte contre le blanchiment[214], il y ajoute surtout deux nouvelles séries d'obligations. Premièrement, la protection des usagers est assurée par la garantie de leurs actifs qui repose sur la détention par l'opérateur d'un compte en dollars jugé suffisant par le *NYSDFS*. Ceci devrait être de nature à éviter l'absence de recours pour les usagers qui sont victimes d'un piratage informatique du site hébergeant leur portefeuille virtuel. Les « *licensees* » sont par ailleurs tenus par des obligations prudentielles importantes destinées à protéger les consommateurs[215]. Deuxièmement, les plates-formes doivent faire la preuve de la solidité de leur système informatique et établir des protocoles destinés à contrer

---

de New York et le Connecticut, Congressional Research Service, « Bitcoin : Questions, Answers, and Analysis of Legal Issues », *op. cit.*, p. 14-16).

[210] La Banque de France semble elle aussi considérer comme suffisante la soumission des plates-formes aux obligations d'agrément, dès lors qu'elles emportent application de la législation sur le blanchiment et sur la lutte contre le financement du terrorisme et que la conversion en monnaie légale reste une quasi-nécessité pour l'utilisateur de monnaie virtuelle – à la condition toutefois précisait-elle que les forces de l'ordre s'investissent dans la poursuite des transactions illicites effectuées directement en Bitcoins (*op. cit.*, p. 6).

[211] « Virtual Currency Business Activity *means the conduct of any one of the following types of activities involving New York or a New York Resident : (1) receiving Virtual Currency for Transmission or Transmitting Virtual Currency, except where the transaction is undertaken for non-financial purposes and does not involve the transfer of more than a nominal amount of Virtual Currency; (2) storing, holding, or maintaining custody or control of Virtual Currency on behalf of others; (3) buying and selling Virtual Currency as a customer business; (4) performing Exchange Services as a customer business; or (5) controlling, administering, or issuing a Virtual Currency*. » (*Regulatory Framework* du 24 juin 2015, Sect. 200.2, q)).

[212] *Regulatory Framework* du 24 juin 2015, Sect. 200.3, c), 1).

[213] *Regulatory Framework* du 24 juin 2015, Sect. 200.3, c), 2).

[214] *Regulatory Framework* du 24 juin 2015, Sect. 200.15 : conservation d'informations, vérification de l'identité des parties impliquées dans les transactions, vérification des circonstances de l'opération, obligation de déclaration, etc. (voir V. Jamet, « La "Bitlicense" – Perspective nord-américaine d'un cadre juridique pour une "bitgénération" encore en devenir », *RISF*, 2014, n°4, p. 18-19).

[215] *Regulatory Framework*, Section 200.19 : la réglementation impose en particulier que soient adressées aux utilisateurs des informations sur les monnaies virtuelles et leur absence de statut légal, des informations générales sur les conséquences et les conditions de leur utilisation, ainsi que des informations sur les modalités de transactions.

les tentatives de piratage[216]. L'existence d'un programme de cyber-sécurité, établi sous la responsabilité d'une personne qualifiée désignée par la société (*Licensee's Chief Information Security Officer*) doit permettre d'identifier les risques internes et externes de fragilité ainsi que les données sensibles, d'instaurer une infrastructure défensive, une politique et une procédure en cas d'attaque, de permettre la détection de toutes formes d'intrusions et de rétablir enfin rapidement le système en cas d'incident. Les opérateurs doivent en outre adresser à l'administration un rapport annuel établi par les *CISO*, afin que soient vérifiés l'intégrité et le bon fonctionnement de leur système informatique.

Au final, le corpus constitué par la *Bitlicense* paraît offrir des garanties sérieuses aux usagers des services offerts par des entreprises agréées. Toutefois, au regard de la déterritorialisation des monnaies virtuelles, le risque de *forum shopping* des utilisateurs était un obstacle sérieux à l'effectivité du *Regulatory Framework* adopté par le *NYSDFS*. Il suffisait aux opérateurs soucieux d'éviter les contraintes d'agrément, de sécurité et de robustesse de domicilier leur société en dehors de l'Etat de New York. C'est pourquoi, lors de la révision du cadre réglementaire en 2015, l'obligation de détenir une licence a été étendue à tout opérateur qui commerce avec un utilisateur résidant ou se situant dans l'Etat de New-York[217].

A défaut d'avoir la compétence pour adopter elles-mêmes les outils juridiques nécessaires à la réglementation des monnaies virtuelles, les administrations concernées sont réduites à faire des propositions et à attirer l'attention des autorités compétentes. En France, après avoir identifié les principaux risques, *Tracfin* présente dans son rapport de 2014 trois volets d'action à mettre en œuvre : encadrement de l'utilisation, régulation et coopération, connaissance et investigation. Le groupe de travail vise plus particulièrement la nécessité de lever l'anonymat des utilisateurs, au minimum lorsqu'ils recourent au service de plateformes d'échange, la consécration explicite des obligations qui s'imposent à ces dernières en matière de lutte contre le blanchiment, et la nécessité d'établir une coopération internationale destinée à éviter le contournement des règles françaises[218]. La même démarche s'observe au niveau européen : après avoir affirmé que les monnaies virtuelles n'entrent pas dans son champ de

[216] *Regulatory Framework,* Section 200.16.

[217] M. Santori et J. Jacobi, « New York Revises "BitLicense" Regulations for Virtual Currency Businesses », *Pillsbury Client Alert*, février 2015 (disponible en ligne : http://www.pillsburylaw.com/publications/new-york-revises-bitlicense-regulations).

[218] Tracfin, *L'encadrement des monnaies virtuelles. Recommandation visant à prévenir leurs usages à des fins frauduleuses ou de blanchiment*, juin 2014, p. 8-9.

compétence, la *BCE* appelle dans son rapport de 2015 à une clarification de leur statut[219] ; tandis que *l'EBA* invite le législateur à encadrer très strictement la gouvernance des crypto-monnaies en imposant l'identification d'une identité qui en soit responsable[220].

Ces initiatives restent encore faiblement suivies d'effet dans la mesure où, comme cela sera développer ci-dessous, les Etats sont peu nombreux à avoir adopté une législation spécifique et adaptée au développement des monnaies virtuelles.

Il faut ajouter, pour conclure sur l'action des autorités administratives, quelques mots sur la problématique de l'imposition des monnaies virtuelles. Les administrations nationales ont unanimement pris position sur la question fiscale en faveur de leur soumission à l'impôt**.** Ainsi, le *CESE* précise-t-il que dans le cas français « *il n'est pas interdit de détenir des bitcoins et il est même demandé de mentionner le nombre de bitcoins détenus dans sa déclaration d'impôts dès 2015* »[221].

Si les plus-values et les pertes, liées notamment à la conversion de monnaie virtuelle en monnaie légale, semblent donc devoir faire l'objet d'une imposition, la nature de cette imposition varie selon les Etats. La décision prise en Allemagne de considérer les monnaies virtuelles comme des monnaies privées fait figure d'exception[222]. Elle soumet les soumets en vertu des § 22 et 23 du *Einkommenssteuergesetz* à une imposition à hauteur de 25 % des bénéfices. En Chine, c'est sous l'angle des gains de jeux que les monnaies virtuelles sont appréhendées. En Russie, bien que leur usage en principe soit prohibé, l'administration sollicitée sur ce point à préciser qu'elle considérerait fiscale les bitcoins comme des monnaies étrangères[223] dans la mesure où leur utilisation pourrait être autorisées à l'étranger[224]. Au Canada, l'Agence du revenu considère depuis 2013 que l'imposition est due au « *titre de*

---

[219] BCE, *Virtual Currency Schemes*, 2015, p. 25 : « *It is, however, desirable that legal clarity is established by the relevant authorities, explaining how the current legal framework applies to virtual currency and related aspects* ».

[220] EBA, *Opinion on 'virtual currencies'*, p. 39-40 : l'EBA propose que soit imposée la création d'une entité responsable du bon fonctionnement du système pour toute monnaie virtuelle.

[221] P. A. Gailly, « Nouvelles monnaies : les enjeux macro-économiques, financiers et sociétaux », *Avis du CESE, Section de l'économie et des finances*, 2015, p. 20.

[222] V. Herry et J. Pécastaing, « Les Bitcoins, nouvelle monnaie virtuelle : quels enjeux ? », *Revue Sorbonne OFIS*, octobre 2014, p. 3 (https://www.univ-paris1.fr/fileadmin/diplome_M2OFIS/_2_2014_Article_Revue_OFIS_-_Novembre_2014_-_Les_bitcoin.pdf) : « *La BaFin, l'autorité de supervision financière allemande, fait figure d'exception en qualifiant les monnaies virtuelles d' "unités de compte", qui entrent dans la catégorie des instruments financiers au même titre que les devises* ».

[223] La réponse du *Federal Tax Service* (datée du 14 juillet 2016) fait suite à une requête adressée par *Coindesk* (elle est disponible à l'adresse suivante : https://www.dropbox.com/s/u2sxfbiic95wvgx/320680091-RF-Federal-Tax-Service-Letter.pdf?dl=0).

[224] Au début du mois d'août, le ministre des finances russes a en effet proposé de restreindre l'interdiction faite aux citoyens russes au seul territoire nationale – sur lequel le Rouble constitue le seul moyen de paiement autorisé (http://bitlegal.io/2016/08/11/russia-to-allow-foreign-trading-of-virtual-currency/).

revenu ou de gain ou perte de capital »[225]. La monnaie numérique y est donc dans ce dernier cas assimilée à un bien meuble[226]. Si en conséquence, lorsqu'elle sert à l'achat de biens ou de service, ce sont les règles du troc qui s'appliquent, il n'en demeure pas moins que le vendeur reste également tenu de déclarer les bénéfices éventuels au titre des revenus.

En France, la qualification de bien meuble n'a pas été retenue[227]. Le fisc a précisé sa position en la matière par une instruction fiscale publiée au Bulletin officiel des finances publiques. Dans sa doctrine fiscale, l'administration va distinguer les plus-values réalisées à titre occasionnel (c'est-à-dire inférieures à 2000 euros par trimestre), qui relèvent de l'impôt sur le revenu au titre des bénéfices non commerciaux[228], et à titre habituel, qui relèvent alors de l'imposition des bénéfices industriels et commerciaux[229]. Le choix de ne pas considérer les monnaies virtuelles comme des monnaies au sens de la législation fiscal, mais comme des actifs mobiliers, n'est pas le plus avantageux pour le contribuable[230]. Il s'explique par la prise en compte de leur nature hautement spéculative par l'administration fiscale. La même approche retenue aux Etats-Unis[231] a été critiquée parce qu'elle renforcerait justement ce penchant spéculatif[232]. Par ailleurs, les unités détenues doivent également être prises en

---

[225] Agence du revenu du Canada, « Que devez-vous savoir à propos de la monnaie numérique ? », *Documents d'information*, 2013 (disponible en ligne : http://www.cra-arc.gc.ca/nwsrm/fctshts/2013/m11/fs131105-fra.html).

[226] Pour d'autres autorités administratives canadiennes, les Bitcoins semblent également pouvoir être assimilés à des valeurs mobilières.

[227] Le régime des biens meubles au sens de l'article 150 UA CGI aurait permis une exonération des plus-values lorsque le prix de cession reste inférieur à 5000 euros.

[228] Pour les revenus tirés de crypto-monnaies à titre occasionnel, BOI-BNC-CHAMP-10-10-20-40-20160203, n°1080, mis à jour le 3 février 2016 : « *leur acquisition en vue de leur revente procède d'une intention spéculative. Les produits tirés de cette activité, lorsqu'elle est exercée à titre occasionnel, sont des revenus relevant des prévisions de l'article 92 du CGI. Il est précisé que les gains sont imposables, quelle que soit la nature des biens ou valeurs contre lesquels les bitcoins sont échangés* ».

[229] Pour les revenus tirés de crypto-monnaies à titre habituel, BOI-BIC-CHAMP-60-50-20140711, n°730, en date du 11 juillet 2014 : « *Le bitcoin est une unité de compte virtuelle qui peut être valorisée et utilisée comme outil spéculatif. Par conséquent, conformément aux dispositions de l'article L. 110-1 du code de commerce qui répute acte de commerce toute acquisition de biens meubles aux fins de les revendre, l'achat-revente de bitcoins exercée à titre habituel et pour son propre compte constitue une activité commerciale par nature dont les revenus sont à déclarer dans la catégorie des bénéfices industriels et commerciaux (BIC) en application de l'article 34 du CGI* ». L'administration précise que l'activité de minage relève bien de cette catégorie, et *« la valeur d'acquisition retenue pour le calcul du résultat imposable est nulle lorsque les bitcoins ont été attribués gratuitement* ». Il n'est toutefois pas précisé dans quelle mesure le coût de l'équipement informatique peut être amorti.

[230] En ce sens, voir V. Herry et J. Pécastaing, *op. cit.*, p. 2.

[231] Notice 2014-21 de l'*Internal Revenu Service* (https://www.irs.gov/pub/irs-drop/n-14-21.pdf)

[232] L. Lee, *op. cit.*, p. 87-88 : « *the Internal Revenue Service ("IRS") classified Bitcoin and all other digital currencies as property for tax purposes, as opposed to as currency. This decision encourages investment in Bitcoin while discouraging users to trade in Bitcoin because they must calculate gain or loss and report it like they would for any other property for tax purposes. However, stocks and bonds are also classified as property for tax purposes and therefore if Bitcoins are more like a security and less like a currency then it makes sense to classify them as property. In the* Securities Act *of 1933, Congress defined a "security" as: any note, stock, treasury stock, security future, securitybased swap, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable*

compte dans la déclaration de capital pour le calcul de l'impôt de solidarité sur la fortune (ISF)[233] ou l'application des droits de succession[234]. Il n'est cependant pas préciser dans la doctrine fiscale comment et à quelle date doit être évaluée la valeur des unités détenues[235]. Enfin, si la question s'est posée, devant les difficultés qu'induirait le choix contraire, l'administration française a finalement opté pour l'application d'une exemption de TVA aux opérations de change impliquant des devises virtuelles (les opérations d'achat de bien ou de service en bitcoin restent évidemment redevables de la TVA) – pratique validée par la suite la Cour de justice et devant donc s'imposer à tous les Etats européens[236].

La position des administrations fiscales, qui cherchent à embrasser le plus largement possible les mouvements de monnaies virtuelles, rencontre toutefois une difficulté majeure dans les systèmes qui garantissent réellement l'anonymat des opérations. Même dans le cadre des monnaies virtuelles qui se veulent transparente, il est difficile d'envisager que les autorités nationales puissent réellement contrôler l'ensemble des transactions afin d'identifier les contribuables responsables de fraude[237]. On ajoutera que malgré la multiplication des

---

share, investment contract, voting-trust certificate, certificate of deposit for a security, factional undivided interest in oil, gas, or other mineral rights, and put, call, straddle, option, or privilege on any security, certificate of deposit, or group or index of securities (including any interest therein or based on the value thereof), or any put, call, straddle, option, or privilege entered into on a national securities exchange relating to foreign currency, or, in general, any interest or instrument commonly known as a "security", or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing.
First, cryptocurrencies — or any currencies for that matter — are not explicitly listed in the statute. Second, Bitcoin does not pass the investment contract test the U.S. Supreme Court developed in SEC v. W.J. Howey Co. *(the "Howey test"). For an investment to constitute a security under the Howey test, it must involve the investment of money — or any valuable consideration — in a common enterprise with a reasonable expectation of profits derived primarily from the efforts of a promoter or third party. The first issue is that there is no common enterprise. Unless attached to an investment trust, Bitcoins are not being pooled into groups. No one enterprise is in charge of Bitcoin, seeking to take people's money with the promise of profits. Bitcoin is purely autonomous and has no central authority. Secondly, "primarily from the efforts of another" prong is not satisfied in the case of Bitcoin because whether the value of Bitcoin rises or falls is not dependent on anyone's efforts* ».

[233] Pour l'imposition à l'ISF, BOI-PAT-ISF-30-20-10-20140711, n°80, en date du 11 juillet 2014.

[234] Pour les droits de donation ou de succession, BOI-ENR-DMTG-10-10-20-10-20140711, n°10, en date du 11 juillet 2014 : font partie du patrimoine du défunt « *les unités de compte virtuelles stockées sur un support électronique (notamment les "bitcoins")* ».

[235] A l'inverse, l'administration américaine a précisé que la valeur des unités détenues devait être évaluée à la date de leur réception, conformément aux conditions du marché qui pourront être raisonnablement prouvées.

[236] CJUE, 22 octobre 2015, *Skatteverket c. David Hedqvist*, Aff. C-264/14 (la Suède mise en cause dans ce litige, tout comme l'Allemagne ou la Pologne, avait pris position en faveur de la soumission à la TVA des opérations de change. A l'inverse, la Finlande, la Belgique, l'Espagne ou encore la Suisse avaient pris position en faveur de l'exemption).

[237] En ce sens, B. Rotschild, « Bitcoin : la Blockchain va-t-elle permettre de contourner l'impôt ? », *Contrepoints*, 10 juin 2016 (https://www.contrepoints.org/2016/06/10/256093-bitcoin-blockchain-remet-cause-lassiette-de-limpot).

avertissements sur leur caractère imposable, il est fort probable que nombre d'utilisateur ignorent complètement le statut fiscal des monnaies virtuelles[238].

Les législateurs

Le besoin de clarification des règles applicables à l'ensemble des activités impliquant des crypto-monnaies paraît difficilement contestable : ainsi, aux Etats-Unis, il résulte de l'approche des différentes autorités de régulation qu'elles sont à la fois des propriétés (*IRS*), des matières premières (*CFTC*[239]), et des monnaies (*SEC* et *FinCEn*) – et les difficultés sont loin de se réduire à la question de leur qualification[240].

Les prises de position adoptées par les régulateurs nationaux sont souvent l'occasion d'identifier un besoin législatif afin d'assurer l'encadrement juridique des monnaies virtuelles et de leur utilisation[241]. C'est par exemple après qu'une étude de l'administration canadienne a pointé l'incertitude entourant leur statut juridique, que le législateur est ainsi intervenu en 2014 pour affirmer que les « *entités qui se livrent au "commerce d'une monnaie virtuelle"* » doivent être considérées comme des « *entreprises de transfert de fonds ou de vente de titres négociables* »[242] soumises à la loi sur le recyclage des produits de la criminalité et le financement des activités terroristes.

Dans le même sens, une récente décision de la justice floridienne devrait pousser les autorités de l'Etat fédéré à adopter une législation spécifique. La juge Teresa Mary Pooler, membre du *Eleventh Judicial Circuit of Florida*, a en effet considéré que les charges de transmission illégale d'argent et de blanchiment ne pouvaient être retenues contre Michell Espinoza dans la mesure où le bitcoin ne pouvait être considéré comme une monnaie[243]. Ce dernier était poursuivi depuis 2013 pour avoir effectué des opérations de vente de bitcoins sans avoir

---

[238] Plus largement, lors de la création de la *Bitlicence*, le fondateur de *Bitcoin Foundation* avait adressée une lettre au *superintendent* Benjamin Lawsky pour l'alerter sur le fait que la majorité des membres de la communauté Bitcoin n'étaient pas familiers avec les régulations sectorielles en cause (disponible à l'adresse suivante : https://www.scribd.com/document/236042382/Bitcoin-Foundation-Letter-to-NYDFS).

[239] Depuis le 17 septembre 2015, la CFTC a pu faire application de la qualification de « *commodities* » à plusieurs reprises après avoir ordonné à Coinflip de suspendre ses offres de contrats dérivés du Bitcoin (http://www.cftc.gov/PressRoom/PressReleases/pr7231-15 ; et pour un cas récent, http://www.cftc.gov/PressRoom/PressReleases/pr7380-16).

[240] Le 20 juillet dernier, une requête a ainsi été adressée à la *CFTC* afin qu'elle clarifie les conditions dans lesquelles elle considérera qu'une société s'est conformée aux exigences légales applicables en matière de marchés financiers adossés aux monnaies virtuelles (http://www.coindesk.com/petition-cftc-clarify-blockchain-rules-delivery/).

[241] Pour les problèmes de qualification au Canada, voir M. Lacoursière, *op. cit.*, p. 25-26.

[242] *Ibid*., p. 25.

[243] Circuit Court of the Eleventh Judicial Circuit in and for Miami-Dade County, Florida, *Florida v. Espinoza*, 22 juillet 2016, F14-2923 (disponible à l'adresse suivante : http://www.miamiherald.com/latest-news/article91701087.ece/BINARY/Read%20the%20ruling%20%28.PDF%29).

l'agrément requis pour les prestataires de services financiers. Si le précédent constitué par cette décision est de faible portée, en raison notamment des possibilités d'appel et de la structure du système juridictionnel américain, la magistrate a motivé sa position de manière très directe et ses arguments ne semblent pas dépourvus de poids : « *This court is unwilling to punish a man for selling his property to another, when his actions fall under a statute so vaguely written that even legal professionals have difficulty finding a singular meaning. [...] The Florida Legislature may choose to adopt statutes regulating virtual currency in the future. At this time, however, attempting to fit the sale of bitcoin into a statutory scheme regulating money services businesses is like fitting square peg in a round hole. […] Nothing in our frame of reference allows us to accurately define or describe bitcoin* ». Même les tenants du bitcoin, qui contestent le bien-fondé du rejet de la qualification de monnaie, reconnaissent la nécessité d'une clarification législative[244] – à l'échelle fédérale, comme en témoigne l'opposition de jurisprudence avec la décision précitée *SEC v. Shavers* de la juridiction du district Sud de New-York. A l'échelle internationale, les divergences se multiplient encore[245].

Dans la perspective d'actions législatives, on a vu se multiplier les enquêtes et auditions diligentées par des commissions parlementaires. Aux Etats-Unis[246], en France[247], comme au sein de l'Union européenne[248] par exemple, les représentants ont en effet suivi le même

---

[244] Voir par exemple, S. D. Palley, « Why Florida's "Bitcoin Isn't Money" Ruling Could Have Limited Impact » (http://www.coindesk.com/florida-bitcoin-money-legal-system/)

[245] En ce sens, voir N. P. Mooney, « Virtual Currencies and the Risks They Bring to Community Banks and the Financial Industry », *Martindale-Hubbell Legal Library*, 30 décembre 2015 (http://www.martindale.com/banking-law/article_Spilman-Thomas-Battle-PLLC_2223256.htm) : « *The biggest problem associated with virtual currencies thus far is the inability of regulators to agree on how these currencies should be classified under existing financial regulations. Some commentators note that virtual currencies appear to function like "reloadable general-use prepaid cards" […] However, the Internal Revenue Service has advised that virtual currencies should be considered property for federal income tax purposes. On the other hand, the Securities and Exchange Commission already has taken steps to regulate entities that are based on Bitcoin, such as Bitcoin Savings & Trust, but has refused to pronounce whether it views virtual currencies as any type of security (such as an investment contract under the Securities Exchange Act of 1934). Still others note that virtual currencies might be properly classified as a commodity under the Commodity Exchange Act. The uncertainty on how to regulate virtual currencies is not limited to the United States. The Chinese central bank has prohibited merchants from accepting Bitcoin as payment. Canadian authorities have undertaken efforts to expand existing regulations to explicitly cover virtual currencies. In Finland, virtual currencies are treated the same as commodities. Sweden disagrees, classifying virtual currencies the same way it classifies fine art* ».

[246] L. Lee, *op. cit.*, p. 84 : « *On November 18, 2013, the Senate held a hearing during the aftermath of the Silk Road shut down* ».

[247] P. Marini et F. Marc, « Rapport d'information fait au nom de la Commission des finances sur les enjeux liés au développement du Bitcoin et des autres monnaies virtuelles », 23 juillet 2014, 143 p. (http://www.senat.fr/rap/r13-767/r13-7671.pdf).

[248] J. von Weizsäcker, *Rapport sur les monnaies virtuelles de la Commission des affaires économiques et monétaires du Parlement européen*, 3 mai 2016, 20 p. (http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-

processus que les régulateurs en cherchant à s'informer avant d'envisager les possibilités d'encadrement. Une fois ce bilan établi, les autorités nationales peuvent adopter schématiquement trois types de position.

Premièrement, les interventions législatives peuvent être considérées comme nécessaires pour clarifier le caractère légal de l'utilisation des monnaies virtuelles. Ainsi, dans l'Etat de Californie, une loi du 22 mai 2014 a été adopté pour amender le *Financial Code* : la Section 107, qui interdisait l'émission ou l'utilisation de tout autre moyen de paiement que la monnaie légale a simplement été supprimé[249]. Cette modification est présentée comme une évolution nécessaire au regard des usages qui se sont développés aux Etats-Unis avec l'utilisation croissantes des coupons, des monnaies privées ou alternatives (du type d'Amazon Coins et d'Equal Dollars), ainsi que des bitcoins. Cela ne fait pas des monnaies virtuelles une monnaie légale (*legal Tender*), mais évite à ceux qui s'en servent d'être poursuivie pour contrefaçon.

Deuxièmement, le législateur pourrait faire le choix inverse et chercher à limiter l'utilisation des monnaies virtuelles ou le minage. C'est cependant pour le moment seulement par leur inaction que les institutions parlementaires ont marqué leur défiance. *« Les positions les plus strictes viennent de la Russie, de la Chine et du Japon. La Chine et le Japon interdisent tout usage du bitcoin aux établissements financiers, et notamment l'échange contre des devises ; en Chine, les détenteurs de bitcoins sont toutefois autorisés à échanger cette "marchandise" entre eux[250]. Plus stricte encore, la Russie attache tout simplement à l'usage des monnaies virtuelles une présomption de "participation à des opérations illégales, notamment de blanchiment d'argent et de financement du terrorisme"* »[251]. Malgré les présentations faites dans les revues d'actualité, la position de la Russie résulte bien uniquement de l'application

---

//EP//NONSGML+REPORT+A8-2016-0168+0+DOC+PDF+V0//FR [les auditions de la Commission peuvent visionnées à l'adresse suivante : https://youtu.be/whN6XYJegO0]).

[249] https://bitcoin.fr/public/divers/docs/AB_129_-_Monnaies_ayant_cours_legal_en_Californie.pdf

[250] P. Marini et F. Marc, *op. cit.,* « *La circulaire du 5 décembre 2013 interdit aux institutions financières tout usage du bitcoin et notamment : l'échange de bitcoins contre des CNY ou des devises étrangères, les opérations de paiement en bitcoin, le développement de produits financiers en bitcoins, ou encore l'utilisation du bitcoin comme unité de compte. La circulaire justifie ces interdictions par les risques inhérents au bitcoin : spéculation et volatilité, utilisation à des fins de blanchiment, utilisation pour des transactions illégales, risque opérationnel des plateformes. L'utilisation de bitcoins reste toutefois autorisée dans le cadre de la loi sur les télécommunications et la circulaire précise que les détenteurs de bitcoins sont libres d'échanger cette "marchandise virtuelle" entre eux. Les plateformes d'échange de bitcoins doivent s'enregistrer auprès de l'autorité de contrôle des télécommunications. Ces plateformes ont également pour obligation de recueillir des pièces justifiant de l'identité des utilisateurs. Enfin, il leur est demandé de mettre en place un dispositif de détection des opérations suspectes et de coopérer avec le Bureau chargé de la lutte anti-blanchiment au sein de la PBoC* ».

[251] P. Marini et F. Marc, *op. cit.*, p. 15.

de la législation existante, dont les autorités n'ont fait que clarifier les conséquences[252]. Il arrive régulièrement que des pays qui n'ont en réalité procédé à aucune action législative soient perçus comme ayant interdit l'utilisation des monnaies virtuelles, du seul fait que les régulateurs nationaux ont émis des avertissements sur les dangers induits. C'est également le cas de la Thaïlande[253]. A l'observation, il s'avère donc que dans les Etats qui sont défiants à l'égard des crypto-monnaies, la réticence n'a pas eu besoin d'action législative pour se manifester. Le gouvernement japonais estime en ce sens que réguler, ce serait donner la possibilité de devenir important à un phénomène qu'il souhaite voir rester marginal.

Troisièmement, dans une approche plus complète mais aussi plus complexe, l'action législative peut avoir pour objet d'encadrer les activités liées aux crypto-monnaies. La France s'engage résolument dans cette voie, car cela lui semble être un d'attractivité pour les acteurs de cette économie émergente[254]. Le Premier ministre a fait une annonce en ce sens le 6 juillet dernier à propos des registres décentralisés : « *C'est en droit français que, pour la première fois en Europe, nous allons fixer les conditions juridiques et de sécurité dans lesquelles on pourra réaliser les transactions financières décentralisées sur Internet, ce qu'on appelle le* blockchain »[255]. L'affirmation de Manuel Valls fait suite à l'adoption de l'ordonnance du 28 avril 2016 sur les bons de caisse, qui « *introduit pour la première fois en droit français une définition de la blockchain et reconnaît la légalité de son utilisation pour un domaine très limité, mais porteur, que sont les minibons. Ces titres ont été créés par l'ordonnance pour accorder des prêts aux petites et moyennes entreprises par le biais de plateformes de financement participatif en utilisant la blockchain* »[256]. Ce texte a institué un régime de transfert de propriété permettant de dématérialiser les registres de mouvements de titres en recourant à la technologie issue du bitcoin. Laure de la Raudière[257] a, dans la continuité de cette première réforme, présenté des amendements destinés à étendre à l'ensemble des titres

[252] La position russe résulte d'une part d'une déclaration de la banque centrale du 27 janvier 2014 et d'une autre du Parquet général du 6 février 2104, qui se fondent sur l'article 27 de la loi fédérale sur la Banque Centrale de la Fédération de Russie (en vertu de laquelle l'émission de substituts monétaires est interdite sur le territoire de la Fédération de Russie). Comme cela a été évoqué précédemment, un amendement législatif proposé par le gouvernement et destiné à légaliser l'utilisation à l'étranger des monnaies virtuelles est actuellement à l'étude.

[253] https://bitcoin.co.th/trading-suspended-due-to-bank-of-thailand-advisement/ et Matt Clinch, « Bitcoin Banned in Thailand », *CNBC*, 30 juillet 2013 (http://www.cnbc.com/id/100923551). Pour une analyse exacte de la situation dans ce pays, voir P. Marini et F. Marc, *op. cit.*, p. 95 et s.

[254] Il faut également mentionner le Canada et le projet de loi C-31 modifiant les lois sur le recyclage des produits de la criminalité et sur le financement des activités terroristes (voir à ce sujet, R. Preda, *op. cit.*, p. 79).

[255] http://www.gouvernement.fr/partage/7673-discours-du-premier-ministre-aux-rencontres-financieres-paris-europlace

[256] M. Abraham, « La France veut être la première à réglementer la blockchain en Europe (1/3) », 4 août 2016 (https://bitcoin.fr/la-france-veut-etre-la-premiere-a-reglementer-la-blockchain-en-europe-par-michelle-abraham/).

[257] Députée LR, elle parraine également le *Forum parlementaire de la Blockchain*, qui aura lieu le 4 octobre 2016.

non cotés, au choix des émetteurs, le régime prévu par l'ordonnance 2016-520[258]. La député propose également de « *considérer que les opérations de règlement livraison d'instruments financiers ou de devises dénouées dans un système de règlement [au sens au sens de la directive 98/26/ CE du Parlement européen et du Conseil du 19 mai 1998, concernant le caractère définitif du règlement dans les systèmes de paiement et de règlement des opérations sur titres], et dont le fonctionnement utilise la technologie dite de la "blockchain", constituent des actes authentiques électroniques de la même manière que les actes passés devant notaires* ». Pourvus d'une date certaine et d'un contenu garanti, ces actes auraient dès lors force probante et force exécutoire. Ces évolutions juridiques sont présentées comme nécessaires au maintien de l'attractivité de la place financière de Paris.

En 1ère lecture, l'AN (14 juin) et le Sénat (8 juillet) n'ont pas mis en œuvre ces propositions, mais ont toutefois ajouté un article 34 *ter* habilitant le gouvernement, conformément à l'article 38 de la Constitution, à « 1° Adapter le droit applicable aux titres financiers et aux valeurs mobilières afin de permettre la représentation et la transmission au moyen d'un dispositif d'enregistrement électronique partagé des titres financiers qui ne sont pas admis aux opérations d'un dépositaire central ni livrés dans un système de règlement et de livraison d'instruments financiers ».

Sur le terrain des monnaies virtuelles, la proposition d'Albéric Montgolfier de faire figurer les activités d'intermédiations offertes par les plates-formes d'échange parmi la liste des activités considérées comme des services de paiement a été adoptée en première lecture par l'Assemblée nationale le 16 mars 2016[259]. Cet amendement avait pour objet de soumettre les opérateurs au statut de prestataire de service de paiement, et ainsi de les obliger à déclarer auprès de *Tracfin* leur soupçon de blanchiment et à mettre en place des mesures de vigilance en matière de financement du terrorisme. Il ne figure toutefois pas dans la version de la loi adopté et promulguée par le Président de la république le 3 juin dernier.

C'est donc en définitive certainement du côté du droit européen qu'il faudra attendre les évolutions législatives. Si l'Union européenne s'est largement saisie des questions soulevées par le numérique[260], elle est pourtant restée longtemps faiblement active sur la question des

[258] Amendement n° 229 au projet de loi relatif à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

[259] Amendement n°445 au projet de loi de lutte contre le crime organisé et le terrorisme, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.

[260] Voir en dernier lieu, la stratégie sur le marché unique numérique et la lutte contre la cybercriminalité (L. Idot, « Commerce en ligne, plates-formes numériques, *big data*... au cœur des préoccupations de la Commission et des

monnaies virtuelles (en dehors de l'activité de *reporting* de ces agences et institutions). Alors qu'au lendemain des attentats de Paris du 13 novembre 2015, les ministres réunis au sein du Conseil « Justice et Affaires intérieures » ont inscrit la lutte contre le financement du terrorisme par les monnaies virtuelles à l'agenda de l'Union[261], force est de constater que les actions concrètes se sont faites attendre. Le rapprochement explicite avec le régime juridique applicable aux prestataires de services de paiement, envisagé lors de l'adoption de la directive *DSP2*[262], n'a effectivement pas été mené à son terme. De même, lors de l'adoption de la 4ème directive anti-blanchiment (*AMLD*)[263], le législateur européen n'avait pas souhaité réglé la situation des plates-formes. La Commission a cependant publié le 2 février 2016 un plan d'action destiné à renforcer la lutte contre le financement du terrorisme[264]. Dans sa communication l'institution affirmait vouloir proposer des outils capables de « *gérer les risques liés à l'utilisation anonyme* » des « *outils financiers innovants* » au titre desquels elle mentionnait les monnaies virtuelles. Pour ce faire, elle proposait pour le 2nd semestre de 2016 de « *placer les opérations de change anonymes sous le contrôle des autorités compétentes, en étendant le champ d'application de la directive anti-blanchiment aux plateformes de change de monnaies virtuelles* » et d'assurer « *l'application, aux plateformes de change de monnaies virtuelles, [ainsi qu'aux fournisseurs de portefeuilles électroniques] des règles prévues en matière d'agrément et de surveillance par la directive sur les services de paiement (DSP)* ». Les modifications proposées ont pris la forme d'une proposition d'amendement de la 4ème directive anti-blanchiment qui reprend l'essentiel du contenu du plan d'action[265]. Une seule différence notable doit être signalée : si les Etats devront s'assurer que les opérateurs possèdent une licence (de prestataire de service de paiement *a priori*) ou simplement

---

autorités nationales », *Europe*, 2016, n° 6, p. 2 ; A. Desforges, « Les stratégies européennes dans le cyberespace », in A. Blandin-Obernesser (dir.), *Droits et souveraineté numérique en Europe*, Bruylant, 2016, p. 81-90 ; Y. Van Couter et E. Roegiers, « Les défis de la cybersécurité », *Journal de droit européen*, 2016, n° 230, p. 1).

[261] http://www.consilium.europa.eu/fr/press/press-releases/2015/11/20-jha-conclusions-counter-terrorism/

[262] Directive n°2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur.

[263] Directive (UE) 2015/849 du Parlement Européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme.

[264] Communication disponible à l'adresse suivante : http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52016DC0050&from=FR

[265] *Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC* (http://ec.europa.eu/justice/criminal/document/files/aml-directive_en.pdf). On peut lire dans la présentation du texte, daté du 5 juillet 2016, l'explication suivante : « *With regard to improving the detection of suspicious virtual currency transactions, six regulatory options were examined. The option retained consists of a combination of means, namely (i) bringing virtual currency exchange platforms and (ii) custodial wallet providers under the scope of the Directive, while (iii) allowing more time to consider options as regards a system of voluntary self-identification of virtual currency users* ».

enregistrés, il n'est plus question de les soumettre à la directive DSP2. Dès lors qu'en France, l'*ACPR* avait déjà pris position en faveur d'une solution identique, la future directive ne devrait pas radicalement changer la situation des plates-formes de conversion. Elle entraînera par contre une extension importante pour les sociétés qui ne proposaient jusqu'alors que des solutions de stockage électronique ou de gestion des transactions. La proposition de la Commission a également le mérite de proposer une définition des monnaies virtuelles (« *'virtual currencies' means a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically* »), des plates-formes (« *providers engaged primarily and professionally in exchange services between virtual currencies and fiat currencies* »), ainsi que des fournisseurs de portefeuille (« *wallet providers offering custodial services of credentials necessary to access virtual currencies* »). Enfin, dernière perspective intéressante, le prochain rapport sur l'application de l'*AMLD* pourra, si besoin, présenter de nouvelles propositions relatives à la création une base de données centrales regroupant l'identité des usagers et l'adresse de leurs comptes à destination des autorités de surveillance.

L'*EBA* a publié rapidement un avis dans lequel elle prend position sur les amendements proposés[266]. Il en ressort qu'elle les considère comme insuffisants face à une activité décentralisée et globalisée. Elle estime, notamment, que si les prestataires en cause doivent rester en dehors du cadre de la DSP2, il conviendrait d'établir des obligations particulières au regard du risque technologique propre aux monnaies virtuelles[267]. De même, elle juge la proposition insuffisante en absence de dispositions sur la protection des consommateurs et sur les obligations prudentielles. Enfin, elle regrette l'absence disposition relative à la coopération des autorités nationales, et se propose de contribuer à l'encadrement des activités relatives aux monnaies virtuelles par l'édiction de lignes directrices.

Si l'adoption de la proposition d'amendement par le Conseil et le Parlement européen devrait se faire sans trop de difficulté, il semble donc qu'elle ne viendra pas clore le débat sur la nécessité de réguler à l'échelle européenne l'usage des monnaies virtuelles. De manière générale, et bien qu'elle apparaisse pressante dans de plus en plus d'Etats, l'intervention

[266] *EBA, Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD)*, 11 août 2016, 9 p. (www.eba.europa.eu/documents/10180/1547217/EBA+Opinion+on+the+Commission's+proposal+to+bring+virtual+currency+entities+into+the+scope+of+4AMLD).

[267] Elle inclut dans ces risques l'hypothèse d'une attaque *Goldfinger*, ce qui pourrait faire entrer en jeu le droit de la concurrence et plus particulièrement les règles relatives aux concentrations.

législative reste toujours délicate face à cette technologie innovante et quelque part un peu fuyante ! L'actualité californienne en témoigne : alors qu'un projet avait été déposé le 8 août 2016 devant le législateur californien afin de créer une procédure d'autorisation, le Sénat a décidé de le retirer le 15 août dernier et de reporter son examen à la prochaine législative en raison des inquiétudes exprimées par la société civile et le *Committee on Banking and Financial Institutions*. Ces péripéties législatives témoignent du besoin de continuer les investigations scientifiques dans le domaine des monnaies virtuelles. La communauté scientifique a effectivement un rôle à jouer, aux côtés des professionnels du secteur, dans la démarche qui consiste à identifier les problèmes posés par leur utilisation et à trouver les solutions les plus conformes à l'intérêt public.

3.b Investigations des acteurs scientifiques

Avant de présenter quelques pistes de réflexion quant aux rôles des acteurs scientifiques, on fera deux observations préliminaires : d'une part, la doctrine américaine est bien davantage investie dans l'étude technique, économique et juridique des monnaies virtuelles ; d'autre part, il semble que ce mouvement se soit quelque peu tari depuis la fin de l'année 2014. Il y a donc un besoin à combler en la matière.

Sur le fond, il est possible de penser que trop d'analyse se focalisent sur la question de la classification, alors qu'aucune catégorie existante n'est réellement adaptée face aux caractéristiques originales des monnaies virtuelles. L'analyse gagnerait à être étendue et menée dans une perspective finaliste, afin de déterminer comment il convient d'appréhender les crypto-monnaies pour en assurer un encadrement juridique effectif et efficace. Une approche en termes d'utilisation apparaît en ce sens bien davantage prometteur.

La volonté de trouver des réponses concrètes à des problèmes pratiques ne doit pas laisser penser que la portée du questionnement soulevé par les crypto-monnaies se limite à cela. Il ne faut pas oublier qu'elles sont aussi un contre-projet : « *[d]ans l'imaginaire collectif, des moyens de paiements reprenant les principes des systèmes métalliques auraient l'avantage d'être soustraits à l'arbitraire d'un pouvoir politique très enclin à manipuler les cours (dévaluations ou réévaluations, etc.). Ainsi, les crypto-monnaies organisent des espaces sans souverain, sur lesquels transitent des monnaies a-bancaires* »[268]. A l'image des *SEL*, explique Pauline Paillet, « *le développement de ces monnaies alternative à la monnaie légale interroge*

[268] L. Desmedt, *op. cit.*, p. 9.

[...] la monnaie et, au-delà, la souveraineté étatique »[269]. Les monnaies virtuelles peuvent en ce sens être rapprochées des travaux de Freidrich Hayek, qui prônait en 1976 la « *dénationalisation de la monnaie* »[270]. Dans une certaine mesure, si l'on admet de les considérer comme des équivalents monétaires, elles participent de la remise en cause de l'idée selon laquelle battre la monnaie serait un privilège régalien[271]. Plus encore, elles contredisent à l'idée que la monnaie aurait une attache géographique pour en faire un instrument d'échange transfrontière. De même, et c'est particulièrement vrai pour le bitcoin qui repose sur un plafonnement à terme du nombre d'unités, il est possible de faire des liens avec la théorie monétaire de Milton Friedman[272]. Les implications théoriques sont donc fondamentales, et cette technologie disruptive doit être l'occasion de penser et de repenser les cadres intellectuels entourant usuellement la question monétaire. Mais la portée de cette innovation ne se limite pas à la compréhension de l'argent. Elle pose aussi de nouveaux défis dans la façon de concevoir et de recevoir les mécanismes de gouvernance qui régissent les interactions sociales. L'expérience de *TheDAO* témoigne du fait que la « révolution *Bit* » se conçoit comme une nouvelle façon de pensée la démocratie.

Au-delà des préoccupations pratiques qui appellent en droit des solutions concrètes et rapides, élaborées branche par branche, il semble en définitive que deux axes de réflexion théorique pourraient utilement être investis par la recherche scientifique : déterritorialisation et régulation[273], d'une part ; décentralisation et gouvernance, d'autre part.

---

[269] P. Pailler, *op. cit.*, p. 4.

[270] Il est à cet égard significatif que la troisième édition de l'ouvrage de F. A. Hayek (*Denationalisation of Money : The Argument Refined. An Analysis of the Theory and Practice of Concurrent Currencies*, The Institute of Economic Affairs, 1990, 146 p.) soit disponible sur le site du Satoshi Nakamoto Institute : http://nakamotoinstitute.org/static/docs/denationalisation.pdf
Pour une analyse de la théorie de F. A. Hayek, voir C. Tutin, « Monnaie et libéralisme : le cas Hayek », *Cahiers d'économie politique*, 1989, Vol. 16, n° 1, p. 153-178 (http://www.persee.fr/doc/cep_0154-8344_1989_num_16_1_1081).

[271] N. Godlove, *op. cit.*, p. 31 : « *The US Constitution109 and the Stamp Payments Act of 1862110 give the Federal Government the exclusive authority to create official coinage and currency of the United States* ».

[272] N. Clausset et A. Sellem, *op. cit.*, p. 1 : « *Cette gestion très rigide de la politique monétaire, qui exclut a priori toute utilisation des leviers monétaires à des fins "politiques", satisfait en partie aux aspirations monétaristes d'un Milton Friedman…* ».

[273] F. Boehm et P. Pesch, *op. cit.* p. 43 : « *since neither the criminal law, nor the civil law order is accustomed to dealing with virtual objects, fundamental questions relating to the enforcement of long-established legal rules arise* ».

3.c Identification des principes d'une régulation intelligente

Le présent rapport n'a pas vocation à se substituer aux travaux qui seront présentés lors de la conférence du 7 octobre 2016, et ils ne peuvent envisager question par question les possibilités en termes de régulation. Quelques pistes de réflexion et principes peuvent toutefois être présentées.

Quelle régulation ?

Le besoin d'équilibre paraît en ce domaine impératif si l'on veut trouver la voie qui permettra aux monnaies virtuelles de se développer. Or, comme l'observe Hubert de Vauplane, en matière de régulation s'est bien souvent tout le problème : « [l]*a régulation consiste pour les uns à minimiser l'intervention régulatrice des pouvoirs publics qui ne doit pas nuire au libre jeu des forces du marché. Pour les autres, elle doit modifier le fonctionnement de certains marchés en fonction d'objectifs d'intérêt général en incitant les acteurs à modifier leurs comportements. Dans un cas comme dans l'autre, il s'agit de déterminer positivement ou négativement le rôle de l'État et celui du marché comme force de régulation* »[274]. Lorsqu'existe cette régulation, le droit qu'elle emporte se contente trop souvent d'un mode coercitif selon Anne Frison-Roche[275]. Il y aurait avec les monnaies virtuelles matière à trouver une méthodologie nouvelle, oubliant pour un temps l'entassement et la sanction, sans forcément retomber dans l'autorégulation[276].

Cela peut-il se faire par le jeu de la *soft law* et des codes de bonnes pratiques ? La règle du monde informatique – *code is law* – est-elle par elle-même suffisante ? Faut-il un cadre « *agnostique* »[277], à l'image de ce que prétend être la *Bitlicense* ? Ou au contraire, faut-il se prémunir de tout risque et procéder à l'interdiction pure et simple des monnaies virtuelles ? Cette solution, peu réaliste dans un monde numérique sans frontière et sans souveraineté

---

[274] H. de Vauplane, « Fondements et limites de la régulation financière », *Rapport Moral sur l'Argent dans le Monde*, 2014, p. 30.

[275] A. Frison-Roche, « La nature prométhéenne du droit en construction pour réguler la banque et la finance », *Rapport Moral sur l'Argent dans le Monde*, 2014, p. 37 et s.

[276] Bien que les SEL soient plus anciens, il semble que pendant longtemps les autorités publiques n'ont pas estimé nécessaire de réguler leur création ou leur utilisation (R. Libchaber, « Actualité du non-droit : les systèmes d'échanges locaux », *RTD Civ.*, 1998, p. 800). Il a fallu attendre, en France, la loi du 31 juillet 2014 relative à l'économie sociale et solidaire, qui vise les « titres de monnaie locale complémentaire » (JO du 1 août 2014, p. 12666). Faut-il suivre la même logique pour les monnaies virtuelles qui revêtent une nature transnationale et libertarienne ?

[277] V. Jamet, *op. cit.*, p. 13.

clairement établie, a pu être un temps envisagé en France[278] comme ailleurs. Cela a été souligné par plusieurs acteurs institutionnels, cette solution est par ailleurs peu souhaitable. Ainsi, pour l'ancien *Superintendent* du *NYSDFS*, « *virtual currency could ultimately have a number of benefits for our financial system. It could force the traditional payments community to up its game in terms of the speed, affordability, and reliability of financial transactions* »[279]. Au final, Jean-Baptiste Carpentier qui représentait *Tracfin* lors des auditions organisées par le Séant en janvier 2014, considère à juste titre que la situation des monnaies virtuelles n'est pas « *dans l'illégal mais dans l' "a-légal"* » et que, plutôt que d'interdire, il faut « *imposer des obligations lorsque monnaies virtuelles et monnaie légale se rencontrent* ». Comme le rappelle Pierre Storrer[280], ces « *lieux de rencontres* » se sont les plateformes d'échange, qui devraient dès lors concentrer l'essentiel de la réglementation à venir. Pour les raisons exposées ci-dessus[281], il semble toutefois souhaitable que soit substitué à l'application par extension des règles applicables aux prestataires de service de paiement un rappel explicite et spécifique des obligations qui s'imposeront à ces opérateurs en termes de protection des utilisateurs, de garantie des fonds, de cyber-sécurité et de lutte contre le blanchiment. Par ailleurs, il n'est pas certains que la réglementation des activités des plateformes d'échange soit suffisante. La prise en compte des services de *e-Wallets* par la Commission européenne va dans le bon sens. Mais la vente de marchandises en bitcoin peut aussi bien servir à blanchir de l'argent, être concernée par des activités terroristes, ou poser des problèmes de protection des consommateurs.

Si comme le prétend Lawrence Lessig, il est nécessaire de laisser dans un premier temps les innovations du monde de l'Internet se développer avant d'établir une régulation adéquate destinée à préserver les valeurs constitutionnelles, les monnaies virtuelles entrent aujourd'hui dans l'âge de la maturité. A l'image de ce qu'a connu l'Internet, l'encadrement juridique apparaît en effet comme un facteur de confiance requis à un stade de développement où les monnaies virtuelles prétendent ne plus rester d'usage confidentiel.

---

[278] Voir la question posée en ce sens par le député E. Straumann au ministre de l'Economie et des Finances : Question n° 51719, JO 11 mars 2014, p. 2243 (http://questions.assemblee-nationale.fr/q14/14-51719QE.htm).

[279] Cité par P. Storrer, « Crowdfunding, bitcoin *: quelle régulation ?* », *Dalloz*, 2014, n° 14, p. 833.

[280] P. Storrer, *op. cit*., p. 833.

[281] On rappellera simplement ici que la jurisprudence de la Cour d'appel de Paris du 26 septembre 2013 ne vise que l'hypothèse où une prestation de paiement est effectuée pour le compte de tiers, sans s'intéresser au cas où seule une opération de change est effectuée en absence de vendeur tiers par rapport à la plateforme (dans la position adoptée par l'ACPR le 29 janvier 2014, il ne semble également être fait cas que de l'hypothèse où la plateforme une activité d'intermédiation).

Quels principes ?

Il est possible d'essayer d'identifier quelques uns des principes qui devraient structurer la conception de cette régulation idéale des monnaies virtuelles.

1. Une législation qui parte des « *causal drivers* », des facteurs de risque clairement identifiés. Comme le note Dirk Haubrich « *a regulatory response will only be successful if the correct factor(s) are identified and a regulatory approach is developed that mitigates them* »[282]. L'auteur illustre son propos avec le problème de la compréhension insuffisante du fonctionnement des monnaies virtuelles par les utilisateurs potentiels : il ne suffit pas de ce constat pour élaborer la contre-mesure efficace ; encore faut-il déterminer si le manque d'accessibilité de l'information est dû à la technicité du domaine, ou à un manque de transparence et de diffusion de l'information. Sur ce point, il semble que ce soit par la conjugaison d'un « *programme d'éducation financière* »[283] et d'obligations de divulgation que le problème pourra être résolu.

Dans cette perspective, les travaux élaborés par les autorités de régulation constituent des éléments importants, mais peut-être encore insuffisants. La question de l'anonymat des utilisateurs, pour prendre un autre exemple, fait encore très souvent l'objet de contresens et d'affirmations contradictoires insuffisamment étayées sur le plan technique et informatique. Il faut donc vider de ses ambiguïtés le tableau des risques induits par les monnaies virtuelles. Pour ce faire, le travail des équipes pluridisciplinaires de chercheurs doit être valorisé et mis à la disposition du législateur – les auditions qui ont pu être organisées au niveau national comme au niveau européen vont donc dans le bon sens, même si le périmètre des disciplines concernées reste encore restreint.

2. Une législation qui soit globale est préférable face à un bien et à des utilisations déterritorrialisés[284]. Le constat est unanime, et pourtant les réactions juridiques que l'on a pu constater se font sans réelle concertation.

---

[282] D. Haubrich, *op. cit.*, p. 36-37 : *l'EBA* a identifié dix-huit facteurs dont les principaux sont l'anonymat des créateurs et la possibilité de modifier le protocole par quiconque atteint les 51% de la puissance de calcul, l'anonymat des parties lors des transactions, la déterritorialité des monnaies virtuelles qui ne relèvent pas d'une juridiction en particulier, l'absence de certificat de conformité pour les opérateurs, l'opacité sur la formation du taux de change, l'irréversibilité des transactions même en cas d'erreur commise, la cyber-sécurité, la garantie des fonds détenus sur les portefeuilles électroniques.

[283] D. Haubrich, *op. cit.*, p. 36.

[284] La commission du Sénat a pris position en ce sens, appelant à une régulation à l'échelle européenne et internationale.

3. Une législation qui ne se limite pas à réagir à la crainte d'activités illicites, mais qui soit de nature à instaurer la confiance nécessaire au développement de la monnaie virtuelle (en tout cas c'est ce que devrait souhaiter les utilisateurs, et c'est le choix logique à défaut de l'interdire afin d'atteindre les gains de productivité envisageables).

4. Une législation qui ne s'attaque pas uniquement à la responsabilité des plateformes. L'*EBA* a cartographié les différents acteurs liées aux monnaies virtuelles[285], et il semble raisonnable de penser que chaque catégorie de participant aux activités qui les entourent devrait voir les risques encourus identifiés, ainsi que les droits et obligations correspondants clarifiés : utilisateurs, marchands, plateformes, acteurs de la gouvernance, fournisseurs de services (portefeuille électronique, assistance technique, information), mineurs, inventeurs, pouvoirs publics... ne sont évidemment pas dans une situation identique bien que tous interagissent entre eux et avec les monnaies virtuelles[286]. En conséquence, on peut penser que pour plus de clarté et pour éviter la dispersion des règles pertinentes, la modification au cas par cas de législations sectorielles – relatives, par exemple, au blanchiment d'argent ou aux obligations des prestataires de service de paiement – n'est pas satisfaisante. Plutôt qu'une intégration des monnaies virtuelles dans le droit par un simple élargissement des définitions légales existantes, il semble en effet préférable de regrouper dans un acte unique l'ensemble des dispositions applicables aux activités liées aux monnaies virtuelles – c'est en pratique la logique adoptée par la *Bitlicense*, mais qu'il faudrait étendre au-delà des seules plateformes d'échange.

5. Une législation qui ne cherche pas à réintégrer les monnaies virtuelles dans le giron du système bancaire traditionnel. Or ce risque est grand, car c'est « *dans la délicate cohésion à construire entre procédures privées et publiques que réside depuis des siècles la difficulté à analyser "l'ambivalence de la monnaie"*[287]*. [...] L'interaction entre procédures étatiques et bancaires est aujourd'hui malmenée par l'essor des crypto-monnaies* »[288]. Alors que les efforts entrepris pour la numérisation de la monnaie, ou du moins des transferts monétaires depuis 1973 par le réseau international SWIFT (Society for Worldwide Interbank Financial Telecommunication), « *supposaient toujours un adossement au système bancaire, qui*

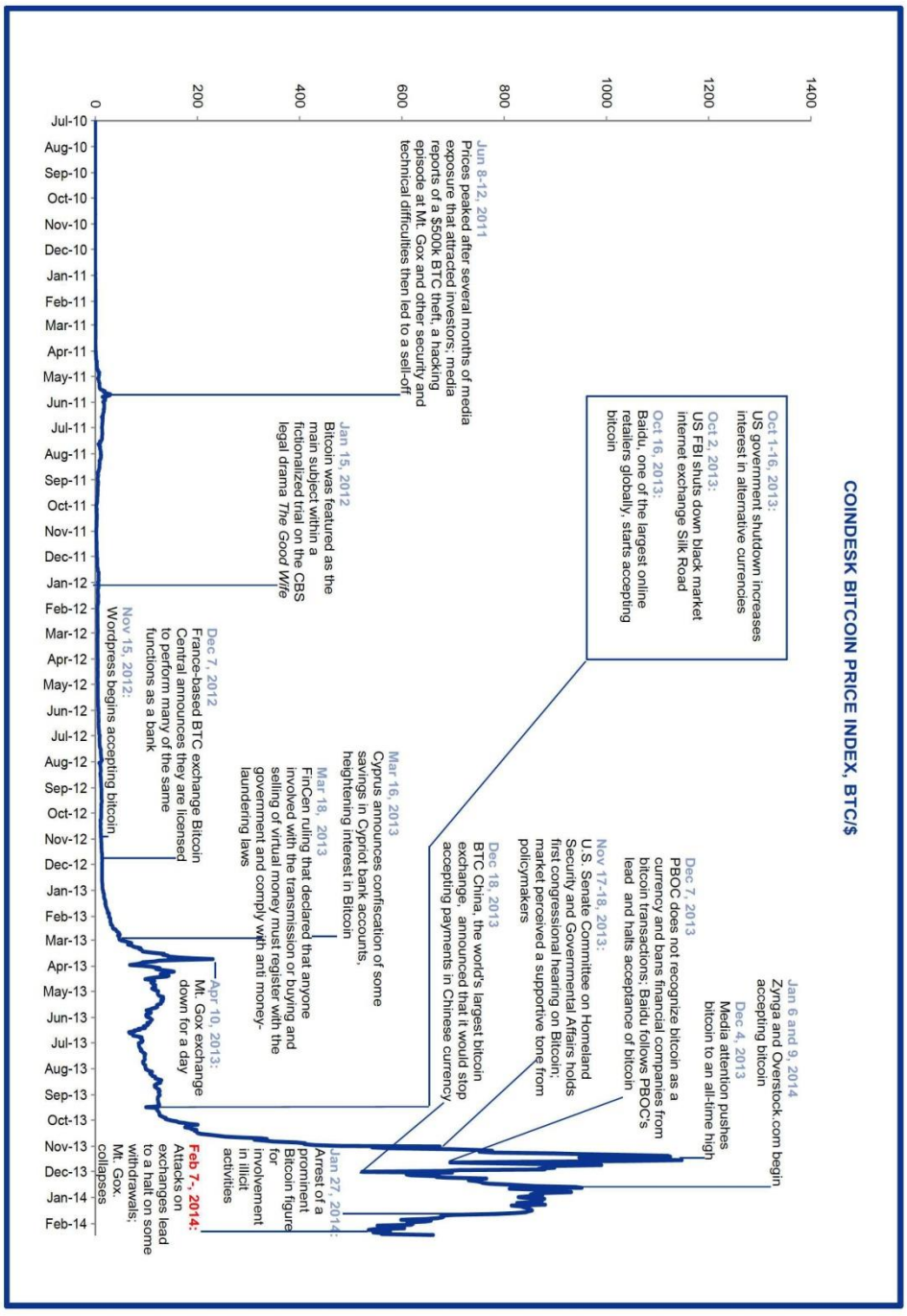
[285] *EBA, Opinion on 'virtual currencies'*, 2014, p. 13-15.
[286] D. Haubrich, *op. cit.*, p. 30-31.
[287] P. Ancel, « La monnaie électronique : régime juridique », in *Droit et monnaie – Etats et espace monétaire transnational*, Credimi, Litec, 1988, p. 305.
[288] L. Desmedt, *op. cit.* p. 7.

contrôlait le bon déroulement des opérations de compte à compte »[289], tout le projet de Satoshi Nakamoto repose sur une défiance à l'endroit des acteurs du système monétaire traditionnel. L'inventeur du bitcoin écrivait ainsi en 2009 : « *The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve* ». Le recours à la cryptographie va permettre à la monnaie virtuelle de rompre complètement avec le circuit institutionnel de l'argent, en substituant à une logique de coopération public/privé une logique de coopération complètement décentralisée[290] et supposément entre les mains des seuls utilisateurs. Si l'on ne parvient pas à inventer un encadrement viable en dehors du réseau bancaire traditionnel, c'est toute l'originalité du projet qui serait abandonné.

[289] *Ibid*., p. 8.

[290] Système qualifié de « panoptique » par L. Desmedt en référence aux travaux de Bentham et de Foucault (*ibid*., p. 9).

Annexe 1 – Evolution du taux de change et chronologie du bitcoin



Source: Coindesk.com, Goldman Sachs Global Investment Research.

Annexe 2 – Panorama des activités et investissements liés au concept de Blockchain

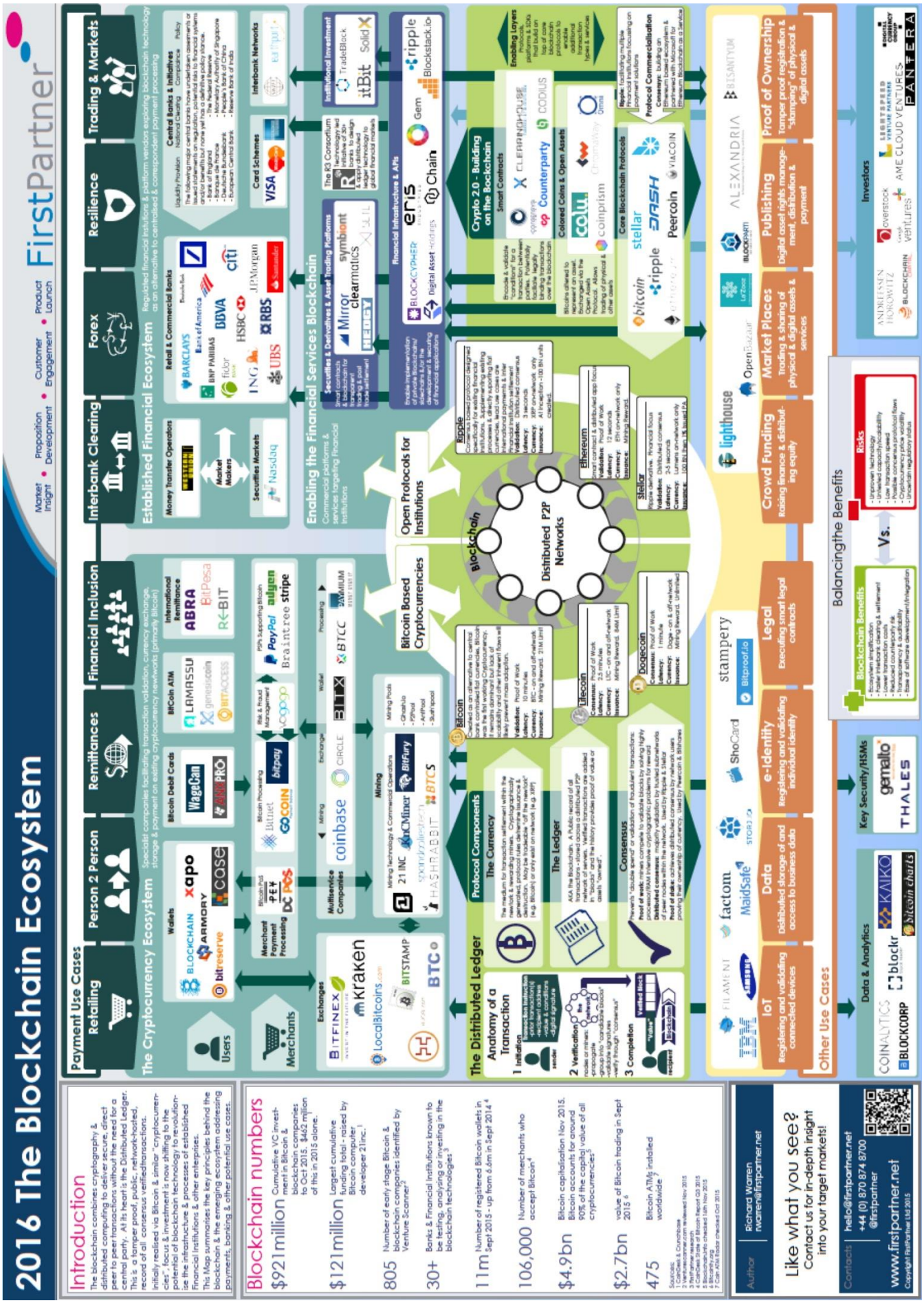


Figure 1: Overview of risks

		ID	Risk description	Rank
A) Risks to users	General risks, irrespective of purpose	A01	User suffers loss when an exchange is fraudulent	High
		A02	User suffers loss when an ostensible exchange is not a genuine exchange	High
		A03	User experiences drop in value of VCs due to (significant and unexpected) exchange rate fluctuation	High
		A04	User holding VCs may unexpectedly become liable to tax requirements	Med
		A05	User who is a member of a VC mining pool does not get fair share of mined VC units from a mining consortium	Low
		A06	User suffers loss when buying VCs that do not have the VC features that the user expects	Med
		A07	User's computing capacity is abused for the mining benefit of others	Low
		A08	User suffers loss due to changes made to the VC protocol and other core components	High
		A09	User is not in a position to identify and assess the risks arising from VCs	Low
		A10	User is in violation of applicable laws and regulations	Med
		A11	User loses VC units through e-wallet theft or hacking	High
		A12	User loses VC units when exchange gets hacked	High
		A13	User's identity may be stolen when providing identification credentials to access VCs	High
		A14	Market participants suffer losses due to unexpected application of law that renders contracts illegal/unenforceable	Med
		A15	Market participants suffer losses due to delays in the recovery of VC units or the freezing of positions	High
		A16	Market participants suffer losses due to counterparties/intermediaries failing to meet contractual settlement obligations	High
		A17	Market participants suffer losses of VC units held in custody by others	Med
		A18	Market participants suffer losses through information inequality regarding other actors	Med
	When used as a means of payment	A21	User suffers loss when counterparty fails to meet contractual payment or settlement obligations	High
		A22	User experiences fraud or loss of FC when using VC cash machines	Med
		A23	User has no guarantee that VCs are accepted by merchants as a means of payment on a permanent basis	High
		A24	User suffers loss when VC payment they have made to purchase a good is incorrectly debited from their e-wallet	High
		A25	User is not able to convert VCs into fiat currency, or not at a reasonable price	High
		A26	User is unable to access VCs after losing passwords/keys to their e-wallet	High
		A27	User is not able to access VCs on an exchange that is a 'going concern' (i.e. has the resources to operate)	High
		A28	User is not able to access VCs on an exchange that has gone out of business (i.e. does no longer have resources to operate)	High
	When used as an investment	A41	User suffers loss as a result of VC prices being manipulated	High
		A42	User investing in regulated financial instruments (e.g. derivatives, SPS, CIS) using unregulated VCs suffers unexpected loss	Med
		A43	User is misled by unreliable exchange rate data	Med
		A44	User suffers loss when investing in fraudulent VC investment schemes	Med
		A45	User is exposed to significant price volatility within very short time frames	Med
		A46	User cannot execute the VC exchange at the expected price	Med
		A47	User is exploited by a VC Ponzi scheme	Med
B) Risks to non-user market participants	Specific to exchanges	B11	Exchange is operationally unable to fulfil payment obligations denominated in VCs or FCs	Med
		B12	Exchange is not in control of its operation	Med
		B13	E-wallet provider faces loss should their refund policies be abused to hedge currency transactions	Med
	Specific to merchants	B21	After accepting VC for payment, merchant is not reimbursed	Med
		B22	Unlike a FC, the merchant cannot be certain that they can spend the VCs received	Med
		B23	The merchant cannot be certain of the FC purchasing power of the VCs they have received	Med
		B24	Merchant faces compensation claims from customers if transactions have been wrongly debited	Med
	Specific to some other market participants	B31	Wallet provider loses e-wallets provided for individuals	High
		B32	Scheme governance authority fails to meet payment and other obligations	High
		B33	Scheme governance authority is subject to unexpected civil/criminal liability that brings the VC scheme to a halt	Med
		B34	E-wallet provider faces compensation claims from customers if functionality of wallet is compromised or fails to provide expected functionality	Med

		ID	Risk description	Rank
C) Risks to financial integrity	Money laundering and terrorist financing	C01	Criminals are able to launder proceeds of crime because they can deposit/transfer VCs anonymously	High
		C02	Criminals are able to launder proceeds of crime because they can deposit/transfer VCs globally, rapidly and irrevocably	High
		C03	Criminals/terrorists use the VC remittance systems and accounts for financing purposes	High
		C04	Criminals/terrorists disguise the origins of criminal proceeds, undermining the ability of enforcement to obtain evidence and recover criminal assets	High
		C05	Market participants are controlled by criminals, terrorists or related organisations	High
	Financial crime risks	C11	Criminal uses VC exchanges to trade illegal commodities and abuse regulated financial sector at point of entry	High
		C12	Restorative justice of victims of crime is hindered by criminal using VCs to avoid seizure of assets, confiscation and financial sanctions	High
		C13	Criminal can use VCs for anonymous extortion	High
		C14	Criminal organisations can use VCs to settle internal or inter-organisational payments	Med
		C15	VCs make it more feasible for individuals to engage in criminal activity	High
		C16	Hacking of VC software, wallets or exchanges allows a criminal to implicate others in the criminal activities they commit	Me
		C17	Criminals, terrorist financiers and even entire jurisdictions are able to avoid seizure of assets, confiscation, embargos and financial sanctions (incl. those imposed by IGOs)	Med
		C18	Criminals are able to create a VC scheme	High
		C19	Tax evaders are able to obtain income in VCs, outside monitored FC payment systems	Med
D) Risks to payment systems in FCs		D01	Payment service providers (PSPs) that use FC and also provide VC services suffer losses due laws that render VC contracts illegal	Low
		D02	PSPs that use FC and also provide VC services fail due to liquidity exposures in their VC operations	Low
		D03	PSPs that offer VC payment services suffer loss of reputation when VC payments fail, because they gave the impression that VCs were regulated	Med
		D04	Businesses in the real economy suffer losses due to disruptions in financial markets that were caused by VC assets blocked, delayed, etc.	Low
E) Risks to regulatory authorities	Reputation risks	E01	Regulators decide to regulate VCs but the chosen regulatory approach fails	Med
		E02	Regulators do not regulate VCs but the viability of regulated financial institutions is compromised as a result of their interaction with VCs	Med
		E03	Regulation and supervision of conventional financial activities is circumvented by unregulated 'shadow' activities that incur the same risks	Med
	Legal	E11	Regulator is subject to litigation as a result of introducing regulation that renders pre-existing contracts illegal/unenforceable	Low
	Risks to competition objectives	E21	Should the regulator decide to regulate VCs more leniently than FCs, an unequal playing field in the market for payment services will emerge	Med
		E22	If an unequal playing field is retained, the intensity of competition in the market for FC payment services diminishes as providers exit FC markets	Med
		E23	Regulators prevent potential new entrants to payment services market if the regulatory approach to VCs is excessive	Med
	To authority issuing FC (out of scope of	E31	Should VCs gain widespread acceptance, central bank as issuer of FC can no longer steer the economy, as the impact of its monetary measures become difficult to predict	Low

Annexe 3 – Tableau exhaustif des risques induit par les monnaies virtuelles (EBA)

Annexe 4 – Tableau comparatif des réactions juridiques de l'AMF

Tableau 8 : Premières interprétations du statut des bitcoins et réglementations associées

Juridictions	Qualification juridique du bitcoin	Traitement proposé
Union européenne	Respect du 1er et du 3e critère de la directive sur les moyens de paiement électronique (*electronic storage, acceptance as a mean of payment*) mais pas du 2e (*issuance upon receipt of funds*).	Avertissement de l'EBA sur les dangers associés aux transactions (achat, détention ou trading de monnaies virtuelles), aucune protection des consommateurs et gains réalisés potentiellement taxables fiscalement. Les institutions de paiement n'ont pas le droit d'émettre de la monnaie électronique.
Allemagne	Unité de compte privé (*binding financial instrument, private mean of payment withing private trading exchanges*) (août 2013).	Communication de la BaFin : pas d'obligation de licence bancaire mais régulation du trading de bitcoins. Pas encore de position fiscale. Exigence d'une autorisation préalable en cas d'utilisation commerciale, d'activités de trading pour compte propre ou de *brokerage* ou de système plateforme multilatérale.
Chypre	-	Déclaration de la Banque Centrale sur les risques associés aux monnaies virtuelles (déc. 2013)
Danemark	Pas une monnaie mais un service électronique.	La FSA a déclaré qu'elle ne régulerait pas l'utilisation du bitcoin, car hors du champ de la régulation financière (déc. 2013). Les gains de ce service électronique seraient taxables mais pas encore de position officielle.
Espagne	Pas une monnaie ayant cours légal. Considéré comme des biens digitaux.0	En tant que « bien digital », le bitcoin est assujetti à la TVA.
Estonie	-	Transactions suivies par la Banque Centrale.
Finlande	Matière première	Pas de loi mais taxation des gains réalisés lors de la conversion de monnaies virtuelles en monnaies ayant cours légal et assujettissement du *mining* au titre de l'impôt sur le revenu.
France	Bien meuble incorporel (Trésor). Pas une monnaie. Pas un moyen de paiement.	Avertissement de la Banque de France sur les risques associés (déc. 2013). Position de l'ACPR (jan. 2014)[80] : Opération de conversion de monnaies virtuelles contre une monnaie ayant cours légal relève de la fourniture de services de paiement donc agrément obligatoire de prestataire de service de paiement délivré par l'ACPR[81].
Grèce	-	Pour autant, le bitcoin est accepté par certaine sociétés de paiement.
Irlande	-	Uniquement monitoring par l'administration fiscale.
Italie	-	-
Malte	-	*Hedge fund* maltais investi en bitcoin.
Pays-Bas	Pas une monnaie électronique. Pas un produit financier.	Question de la taxation des plus-values à régler. Décembre 2013 : alerte de la banque centrale sur les risques associés.
Pologne	-	-
Portugal	Bitcoin : modèle de paiement en monnaie virtuelle bidirectionnel. bitcoin : -	Communication de la banque centrale en novembre 2013 sur les risques du bitcoin, qui ne serait pas une monnaie sure.
Royaume-Uni	« *Single purpose voucher* » selon l'administration fiscale.	En tant que tel, assujetti à la TVA.
Slovénie	Pas un moyen de paiement. Pas un instrument financier.	Opinion du Ministère des Finances émis en décembre 2013, sans pour autant définir de statut. Question de la taxation à régler.
Chine	Interdiction des institutions financières (déc. 2013) et des sociétés de paiement (avr. 2014) de traiter des bitcoins. Autorisation du *trading* en ligne.	
États-Unis	Actif (*property*) et non devise.	Actif soumis à l'impôt : plus-values imposées comme les gains sur le capital et revenus tirés de l'activité de minage au-delà de 600 USD soumis à l'impôt sur le revenu (IRS, mar. 2014). La négociation/conversion d'une monnaie virtuelle contre une monnaie légale étant assimilable à un service de transmission de fonds, obligation d'agrément en tant que *Money Service Business (*FinCEN, mar. 2013).
Japon	Statut de marchandise ou de chose (mais pas une monnaie).	Soumis à l'impôt (mar. 2014)
Russie	Illégal.	
Singapour	Pas une valeur mobilière.	Régulation des intermédiaires en monnaie virtuels (mar. 2014) afin de limiter les risques (blanchiment, financement du terrorisme, etc.) : devoir de vérification de l'identité des contreparties des transactions et de signalisation toute transaction suspecte au *Suspicious Transaction Reporting Office*.
Taïwan	Illégal.	
Thaïlande	Illégal.	Interdiction des monnaies virtuelles

Source : AMF.

BIBLIOGRAPHIE INDICATIVE

Rapports officiels et prises de positions des autorités publiques

• ACPR, « Position relative aux opérations sur bitcoins en France », *Position 2014-P-01,* 29 janvier 2014 (https://acpr.banque-france.fr/fileadmin/user_upload/acp/publications/registre-officiel/ 201401-Position-2014-P-01-de-l-ACPR.pdf).

• AMF, « Emergences des monnaies virtuelles : risques et opportunités ? », *Risques et tendances*, juillet 2014, n° 15, p. 60 (http://www.amf-france.org/Publications/Lettres-et-cahiers/Risques-et-tendances/Archives.html?docId=workspace%3A%2F%2FSpacesStore%2Fb87033f5-ecbf-41f1-8236-ee44c91df3c7).

• A. Badev et M. Chen, Federal Reserve Board, « Bitcoin: Technical Background and Data Analysis », *Finance and Economics Discussion Series*, 2014, n° 104, 34 p. (http://www.federalreserve.gov/ econresdata/feds/2014/files/2014104pap.pdf).

• Banque de France, « Les dangers liés au développement des monnaies virtuelles : l'exemple du bitcoin », *Focus*, 5 décembre 2013, n°1°, 6 p.

• Bank for International Settlements (Committee on Payments and Market Infrastructures), *Report on Digital Currencies*, novembre 2015, 24 p. (disponible en ligne : https://www.bis.org/cpmi/publ/d137.pdf).

• Bank of England, « Innovations in Payment Technologies and the Emergence of Digital Currencies », *Quaterly Bulletin*, 2014, Q3, 14 p.

• BCE, *Virtual currency schemes*, Francfort, 2012, 55 p.

• BCE, *Virtual currency schemes – a further analyse*, Francfort, 2015, 37 p.

• B. Berton, European Union Institute for Security Studies, « The dark side of the web: ISIL's one-stop shop? », *Isssue Alert*, juin 2015, n° 30 (http://www.iss.europa.eu/uploads/media/Alert_30_The_Dark_Web.pdf).

• CA Paris, Ord., 26 août 2011, *SA Crédit Industriel et Commercial c. S.A.S. Maracaja*, n° 11/15269.

• CA Paris, 26 septembre 2013, *SA Crédit Industriel et Commercial c. S.A.S. Maracaja*, n° 12/00161.

• Circuit Court of the Eleventh Judicial Circuit in and for Miami-Dade County, Florida, *Florida v. Espinoza*, 22 juillet 2016, F14-2923.

• CJUE, 22 octobre 2015, *Skatteverket c. David Hedqvist*, Aff. C-264/14.

• Congressional Research Service, « Bitcoin : Questions, Answers, and Analysis of Legal Issues », 13 octobre 2015, 36 p. (https://www.fas.org/sgp/crs/misc/R43339.pdf).

• Conseil fédéral suisse, *Rapport du Conseil fédéral sur les monnaies virtuelles en réponse aux postulats Schwaab (13.3687) et Weibel (13.4070)*, 2014, 42 p.

• CSBS, « State Regulatory for Virtual Currency Activities. CSBS Model Regulatory Framework », 15 septembre 2015, 14 p. (https://www.csbs.org/regulatory/ep/Documents/CSBS-Model-Regulatory-Framework%28September%2015%202015%29.pdf).

• Federal Advisory Council and Board of Governors of the Federal Reserve System, *Record of Meeting*, 9 mai 2014 (http://www.federalreserve.gov/aboutthefed/fac.htm/).

• FMI, « Virtual Currencies and Beyond: Initial Considerations », *IMF Staff Discussion Note*, janvier 2016, 42 p.

• P. A. Gailly, « Nouvelles monnaies : les enjeux macro-économiques, financiers et sociétaux », *Avis du CESE, Section de l'économie et des finances*, 2015, 66 p. (disponible en ligne : http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/154000302.pdf).

• HM Treasury, *Digital Currencies : Response to the Call for Information*, Mars 2015, 28 p. (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf).

• P. Marini et F. Marc, « Rapport d'information fait au nom de la Commission des finances sur les enjeux liés au développement du Bitcoin et des autres monnaies virtuelles », 23 juillet 2014, p. 11 (http://www.senat.fr/rap/r13-767/r13-7671.pdf).

• SEC, « Investor Alert - Ponzi schemes Using virtual Currencies », *SEC Pub*., n°. 153 (7/13), 3 p.

• SEC, « SEC Charges Bitcoin Entrepreneur With Offering Unregistred Securities », *Communiqué de presse n° 2014-111* (www.sec.gov/litigation/admin//014/33-9592.pdf)

• Senate Committee on Banking, Housing, and Urban Affairs, *Semiannual Monetary Policy Report to the Congress*, 27 février 2014 (disponible en vidéo : http://www.banking.senate.gov/public/index.cfm?FuseAction= Newsroom).

• Tracfin, *L'encadrement des monnaies virtuelles. Recommandation visant à prévenir leurs usages à des fins frauduleuses ou de blanchiment*, juin 2014, p. 8-9.

• J. von Weizsäcker, *Rapport sur les monnaies virtuelles de la Commission des affaires économiques et monétaires du Parlement européen*, 3 mai 2016, 20 p. (http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2016-0168+0+DOC+PDF+V0//FR.

Monographies et ouvrages collectifs

• *Dictionnaire encyclopédique de l'Etat*, Paris, Berger-Levrault, 2014, 1008 p.

• P. Ancel, « La monnaie électronique : régime juridique », in *Droit et monnaie – Etats et espace monétaire transnational*, Credimi, Litec, 1988, p. 302-315.

• A. Desforges, « Les stratégies européennes dans le cyberespace », in A. Blandin-Obernesser (dir.), *Droits et souveraineté numérique en Europe*, Bruylant, 2016, p. 81-90.

• M-A. Frison-Roche (dir.), *Internet, espace d'interrégulation*, Dalloz, 2016, 208 p.

• F. A. Hayek, *Denationalisation of Money : The Argument Refined. An Analysis of the Theory and Practice of Concurrent Currencies*, The Institute of Economic Affairs, 1990, 146 p.

• R. Libchaber, *Recherches sur la monnaie en droit privé*, LGDJ, 1992, 440 p.

• R. Preda, « Les monnaies virtuelles, enjeux de régulation », in A. Blandin-Obernesser (dir.), *Droits et souveraineté numérique en Europe*, Bruylant, 2016, p. 73-79.

Articles de revues, conférences

• E. Ben Sasson e.a., « Zerocash : Decentralized Anonymous Payments from Bitcoin », 56 p. (disponible en ligne : http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf).

• F. Boehm et P. Pesch, « Bitcoin: A First Legal Analysis - with reference to German and US-American law », in *Financial Cryptography and Data Security*, *Springer*, 2014, p. 43-56.

• J. Bonneau e.a., « SoK : Research Perspectives and Challenges for Bitcoin and Cryptocurrencies », *2015 IEEE Symposium on Security and Privacy*, 2015 18 p. (http://www.ieee-security.org/TC/SP2015/papers-archived/6949a104.pdf).

• T. Bonneau, « Commentaire sous CA Paris, 26 septembre 2013, n° 12/00161, *SAS Macaraja c/ SA Crédit industriel et commercial* », *JCP E*, 2014, p. 1091.

• E. Castronova, « Virtual Worlds: A First-Hand Account of Market and Society on the Cyberian Frontier », *CESifo Working Paper Series No. 618*, 2001 (http://papers.ssrn.com/sol3/ papers.cfm?abstract_id=294828).

• M. Chevalier et B. Vignolles, « Le bitcoin : défi à la souveraineté monétaire des Etats et ressource pour le blanchiment d'argent », *Regards croisés sur l'économie*, 2014, n° 14, p. 122-125.

• N. Clausset et A. Sellem, « Le bitcoin, de l'engouement à l'indifférence : L'avenir d'une monnaie qui a dérangé », *La Gazette de la Société et des Techniques*, 2015, n° 82, p. 1-4.

• L. Desmedt, « Le bitcoin et les crypto-monnaies : nouveaux modèles, questions persistantes », *RISF*, 2014, n°4, p. 7-11.

• P. de Filippi, et D. Bourcier, « Réseaux et gouvernance. Le cas des architectures distribuées sur internet », *Pensée plurielle*, 2014/2, n° 36, p. 37-53.

• A. Frison-Roche, « La nature prométhéenne du droit en construction pour réguler la banque et la finance », *Rapport Moral sur l'Argent dans le Monde*, 2014, p. 37 et s.

• N. Gandal et H. Halaburday, « Competition in the Crypto currency Market », 30 janvier 2015, 32 p. (http://www.law.northwestern.edu/research-faculty/searlecenter/events/internet/documents/Halaburda_cryptocurrency.pdf.

• M. E. Gladden « Cryptocurrency with a Conscience: Using Artificial Intelligence to Develop Money that Advances Human Ethical Values », *Annales. Ethics in Economic* Life, 2015, Vol. 18, n° 4, p. 85-98.

• N. Godlove, « Regulatory Overview of Virtual Currency », *Oklahoma Journal of Law and Technology*, 2014, Vol. 10, 67 p.

• E. L. Greebel, K. Moriarty, C. Callaway , G. Xethalis , « Recent key Bitcoin and virtual currency regulatory and law enforcement developments », *Journal of Investment Compliance*, 2015, Vol. 16, n° 1, p.13-18.

• D. Haubrich, « The monitoring and Regulation of Financial Innovation : The Case of Virtual Currencies and the European Banking Authority », *RISF*, 2014, n° 4, p. 28-38.

• V. Herry et J. Pécastaing, « Les Bitcoins, nouvelle monnaie virtuelle : quels enjeux ? », *Revue Sorbonne OFIS*, octobre 2014, 4 p. (https://www.univ-paris1.fr/fileadmin/diplôme_M2OFIS/_2_2014_Article_Revue_ OFIS_-_Novembre_2014_-_Les_bitcoin.pdf).

• L. Idot, « Commerce en ligne, plates-formes numériques, *big data*... au cœur des préoccupations de la Commission et des autorités nationales », *Europe*, 2016, n° 6, p. 2.

• J. A. Kroll, e.a., « The Economics of Bitcoin Mining – or Bitcoin in Presence of Adversaries », *The Twelfth Workshop on the Economics of Information Security (WEIS 2013)*, Juin 2013, 21 p.

• M. Lacoursière, « L'encadrement juridique de la monnaie virtuelle au Canada », *RISF*, 2014, n° 4, p. 21-27.

• O. Lakomski-Laguerre et L. Desmedt, « L'alternative monétaire Bitcoin : une perspective institutionnaliste », *Revue de la régulation*, 2015, n° 18,

• L. Lee, (« New Kids on the Blockchain : How Bitcoin's Technology Could Reinvent the Stock Market », *Hastings Business Law Journal*, 2016, Vol. 12, n° 2, p. 81-132 (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2656501=).

• L. Lessig, « Code Is Law. On Liberty in Cyberspace », *Harvard Magazine*, 2000 (http://harvardmagazine.com/2000/01/code-is-law-html).

• R. Libchaber, « Actualité du non-droit : les systèmes d'échanges locaux », *RTD Civ.*, 1998, p. 800.

• S. Mignot, « Le Bitcoin : nature et fonctionnement », *Banque & Droit*, 2015, n° 159, p. 10-13.

• P. Pailler, « Quelles règles pour l'encadrement de la monnaie virtuelle en France ? », *RISF*, 2014, n° 4, p. 39-43.

• K. L. Penrose « Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws », *North Carolina Banking Institue Journal*, 2014, Vol. 18, p. 251 ((https://www.law.unc.edu/journals/ncbank/volumes/volume18/citation-18-nc-banking-inst-2014/banking-on-bitcoin-applying-antimoney-laundering-and-money-transmitter-laws).

• J. Poon et T. Dryja, « The Bitcoin Lightning Network : Scalable Off-Chain Instant Payments », 14 janvier 2016, 59 p. (https://lightning.network/lightning-network-paper.pdf).

• F. Reid et M. Harrigan, « An Analysis of Anonymity in the Bitcoin System », *Cornwell University Librairy*, p. 15-25 (http://arxiv.org/pdf/1107.4524.pdf).

• P. Storrer, « Crowdfunding, bitcoin *: quelle régulation ?* », *Dalloz*, 2014, n° 14, p. 832-834.

• P. Tasca, « Digital Currencies : Principles, Trends, Opportunities, and Risks », *Ecurex Research Working Paper*, Octobre 2015, 110 p. (http://papers.ssrn.com/sol3/ papers.cfm?abstract_id=2657598).

• C. Tutin, « Monnaie et libéralisme : le cas Hayek », *Cahiers d'économie politique*, 1989, Vol. 16, n° 1, p. 153-178.

• R. Vabres, « Le statut fiscal de la "monnaie virtuelle" en droit français », *RISF*, 2014, n° 4, p. 44-48.

• H. Vachon, « Les limites des monnaies du type *bitcoin* », *Point de vue économique*, novembre 2013, p. 5 (https://desjardins.com/ressources/pdf/pv131121-f.pdf?resVer=1385162817000).

• Y. Van Couter et E. Roegiers, « Les défis de la cybersécurité », *Journal de droit européen*, 2016, n° 230, p. 1.

• H. de Vauplane, « L'analyse juridique du Bitcoin », *Rapport Moral sur l'Argent dans le Monde*, 2014, p. 351-360.

• H. de Vauplane et S. Cazaillet, « Bitcoin : *money, money, money* », *La lettre juridique*, 17 avril 2014, n° 567, p. 1-13.

• D. Yermack, « Is Bitcoin a Real Currency ? An economic Appraisal », *NYU Stern School of Business*, 2014, 23 p. (http://papers.ssrn.com/sol3/papers.cfm?abstract_id =2361599)