

Blockchain et finance

RLDA 6526

Blockchain, cryptomonnaies, finance et droit : état des lieux

Tous les grands cabinets de consultants ont publié ces derniers mois des rapports sur les impacts de la blockchain dans les activités financières d'où il ressort que c'est l'une des industries qui devraient être le plus affectées par cette technologie. Au-delà du métier lui-même de la banque, les secteurs qui devraient le plus rapidement voir les effets de la blockchain sont les services de paiement, les activités de marchés, le financement du commerce international, l'identification des clients, les mesures de contrôle sur l'origine des fonds et la lutte contre le blanchiment.



Hubert de
VAUPLANE
Avocat Associé,
Kramer Levin
Naftalis & Frankel
LLP

Il ne s'agit pas ici de formuler ce que de nombreux rapports et livres ont déjà pu détailler sur le fonctionnement de la technologie blockchain mais juste d'effectuer quelques rappels.

Les blockchains (car il existe autant de blockchains qu'il existe de protocoles sous-jacents) peuvent être considérées comme des cas particuliers de registres distribués, et que pour cette raison un amalgame est souvent fait entre ce qu'on peut appeler la technologie blockchain et la technologie des registres distribués (*Distributed Ledger Technology – DLT*). Les registres distribués (*distributed ledgers*) permettent aux utilisateurs d'un réseau électronique d'enregistrer et de gérer les données relatives au fonctionnement du réseau. Les informations gérées par ce registre partagé peuvent varier suivant le *design* du système mais porteront typiquement sur différentes données transactionnelles : prix d'échange de titres ou d'actifs physiques, identifiants virtuels de ces derniers, etc. Ces informations sont réparties entre les utilisateurs, qui peuvent ensuite les utiliser pour régler leurs transferts sans avoir à se reposer, dans un modèle de fonctionnement distribué, sur un système central de validation de confiance.

Le fonctionnement d'un registre distribué tel qu'une blockchain implique les éléments suivants⁽¹⁾ :

- un réseau pair-à-pair (*peer to peer*) soit public, soit totalement ou partiellement privé ;
- une base de données distribuée servant de « grand livre » où sont inscrites toutes les transactions et autres informations utiles pour les membres du réseau ;
- un ensemble d'outils et de méthodes cryptographiques assurant la sécurité du réseau – en particulier contre toute attaque ou tentative de corruption du registre distribué – et l'intégrité des échanges entre ses membres ;
- un algorithme de consensus réglant la mise à jour et l'évolution du registre et permettant d'automatiser par un ensemble de règles le processus de validation des transactions entre membres du réseau ; et
- un mécanisme d'incitations inscrit dans le protocole de fonctionnement du ré-

(1) Pour plus de détails, v. Paris Europlace, Les impacts des réseaux distribués et de la technologie blockchain dans les activités de marché, oct. 2017.

seau, nécessaire pour rémunérer les membres actifs du réseau, à savoir ceux qui se chargent d'assurer la bonne marche et la sécurité du réseau, en particulier et surtout si ce dernier est complètement ouvert.

À cette organisation en réseau distribué, il convient d'ajouter une autre spécificité de la technologie blockchain⁽²⁾ : le recours à la cryptographie. La sécurité des blockchains est principalement fondée sur de la cryptographie, et cela à différents niveaux. Le premier concept essentiel est celui de fonction de « hachage » (*hash function*). La caractéristique déterminante d'une fonction de hachage est que, s'il est facile de calculer la sortie correspondante $y = H(x)$ (l'output) pour une entrée x donnée (l'input), il est cependant quasiment impossible pour un y donné de trouver x tel que $H(x) = y$. Tout comme ouvrir un coffre sans en connaître le code d'accès nécessite d'essayer une à une toutes les combinaisons possibles, inverser une fonction de hachage, *i.e.* trouver un x produisant un y donné, forcera celui qui veut résoudre ce problème à tester aléatoirement une série d'entrées jusqu'à trouver une solution.

I. – Et la finance là-dedans ?

À côté des activités bancaires classiques, c'est surtout au regard des activités des banques centrales que la technologie blockchain peut avoir des conséquences importantes.

Depuis quelques mois, de plus en plus de banques centrales explorent le potentiel de la technologie de la chaîne de blocs et du grand livre distribué. Comme l'ont montré les expériences des banques, les réseaux à chaîne de blocs peuvent conduire à des systèmes de paiement et de valeurs mobilières plus sûrs et de meilleure qualité.

Les banques centrales jouent un rôle crucial en tant que régulateurs et devraient atténuer les risques tout en encourageant l'innovation. Cela signifie pour la blockchain, créer des règles et des normes claires ainsi que des informations pour les consommateurs sur les risques potentiels d'investir dans des sociétés basées sur une chaîne de blocs et des lignes directrices pour les banques et les sociétés de technologie lorsqu'elles développent des applications pour le secteur des services financiers. En l'absence de clarté sur ce qu'il est possible de faire ou de ne pas faire, l'innovation liée à la technologie blockchain sera plus ou moins bridée.

À ce stade, et compte tenu du caractère encore innovant et récent de cette technologie, les banques centrales devraient élaborer une réglementation technologiquement neutre, afin de ne pas favoriser un fournisseur par rapport

(2) Pour plus de détails, v. Paris Europlace, Les impacts des réseaux distribués et de la technologie blockchain dans les activités de marché, octobre 2017, dont les lignes qui suivent sont issues.

à un autre, une technologie plutôt qu'une autre et de réduire la concurrence sur le marché.

Quels que soient les cas d'utilisation possibles pour une banque centrale, l'une des premières questions à se poser est de savoir quel(le) architecture / protocole il convient de choisir : blockchain publique ou DLT ? Ce point est crucial en ce qu'il déterminera le degré de confiance des acteurs dans le choix technologique retenu et le degré de confidentialité retenu. À cet égard, il est intéressant de constater que parmi les premières expérimentations auprès des banques centrales, la plupart d'entre elles recourent plutôt à une DLT qu'à une blockchain publique.

S'agissant des avantages potentiels de la blockchain pour les banques centrales, il est bien sûr difficile d'avancer des certitudes en ce domaine, et les réponses dépendent aussi des contextes culturels et économiques locaux. Ce qui pourra passer pour un avantage pour une banque centrale pourra, pour une autre, constituer un défi ou une menace. C'est donc localement, au niveau de chaque banque centrale, qu'il convient d'apprécier les avantages / défis de la technologie blockchain.

II. – Avantages de la blockchain pour une banque centrale

De manière non exhaustive, voici quelques avantages potentiels que pourrait représenter la blockchain pour les banques centrales⁽³⁾.

Traçabilité des transactions

La propriété inhérente d'immutabilité et de transparence associée à la chaîne de bloc permet aux banques centrales de retracer plus facilement la monnaie en circulation. Cela leur permettrait de suivre chaque euro, livre, dollar ou renminbi à chaque étape du système financier en temps réel.

Construction d'un enregistrement partagé unique

Les banques centrales peuvent voir un intérêt à cette technologie comme moyen d'établir un registre partagé de toutes les transactions entre plusieurs institutions. Les banques centrales espèrent pouvoir utiliser la méthode décentralisée de tenue des registres pour effectuer et enregistrer les transactions dans l'économie de manière plus efficace, rapide et transparente. La création d'une méthode normalisée d'enregistrement des transactions permettrait à tous les acteurs du système de communiquer plus facilement. Cela pourrait laisser beaucoup

(3) Les lignes qui suivent sont tirées pour l'essentiel de l'article de C. R. W. De Meijer, Blockchain and Central banks : a Tour de Table Part 1 : <https://www.finextra.com/blogposting/13507/blockchain-and-central-banks-a-tour-de-table-part-1>.

moins d'argent inactif pendant que les banques réconcilient leurs différents grands livres, comme c'est le cas aujourd'hui.

Modernisation des systèmes de paiement

L'une des applications les plus évidentes de la blockchain est celle des systèmes de paiement cash. Plusieurs banques centrales mènent déjà des recherches dans ce domaine, notamment la Banque du Canada, la Banque du Japon, la Banque de Suède, la Banque de Singapour, et la Banque centrale européenne. D'autres fonctions internes peuvent également bénéficier d'une chaîne de blocage, comme la gestion des réserves, la vérification, la conformité et la gestion des dossiers.

Simplification du processus de règlement / livraison de titres financiers

La blockchain, et plus largement les DLT, ont le potentiel de simplifier la chaîne de règlement / livraison autour des opérations sur titres, en particulier sur des bons du Trésor et des titres d'État. Les réductions de coûts qui en résultent, la rapidité du règlement (quasi-instantanéité) et l'amélioration de la transparence peuvent contribuer à rendre les paiements et les marchés financiers plus efficaces et plus sûrs. Un projet pilote d'émission des bons du trésor du Kenya a été lancé sous l'égide de la Banque Mondiale⁽⁴⁾.

Un rapport publié en mars 2018 par la Banque centrale européenne et la Banque du Japon⁽⁵⁾ indique que la technologie du grand livre distribué (DLT) pourrait être utilisée pour créer de nouveaux mécanismes de règlement de titres, y compris des « swaps atomiques inter-chaînes » entre les grands livres non connectés. Les résultats sont le fruit de l'initiative conjointe de recherche DLT des banques centrales, baptisée Projet Stella, qui a été lancée en décembre 2016.

Réduction des coûts de transmission

Cette technologie peut également réduire considérablement les coûts et le temps de transmission associés aux transferts transfrontaliers, en permettant des transferts quasi-instantanés entre succursales ou différentes entités, tant à l'intérieur qu'à l'extérieur du pays.

(4) World Bank, Financial Sector Support Project : <https://www.blockchaintechnology-news.com/2017/05/02/world-bank-supporting-kenyan-blockchain-bonds-trial/>.

(5) ECB and Bank of Japan, Securities Settlement Systems : delivery versus payment in a DLT environment, March 2018. http://www.boj.or.jp/en/announcements/release_2018/data-re-1180327a1.pdf.

Réduction des coûts d'exploitation

L'utilisation d'une monnaie numérique ou digitale basée sur une chaîne de blocs pourrait réduire la quantité de billets et de pièces en circulation. Cela réduira les coûts d'exploitation associés à l'impression et à la distribution des billets de banque centrale, mais aussi facilitera le passage à une économie digitale.

Amélioration de la lutte contre le blanchiment d'argent

Le déploiement de monnaies digitales émises par les banques centrales aidera également les banques centrales (et les gouvernements) à lutter contre le blanchiment d'argent tout en éliminant le problème de la contrefaçon.

Autres avantages

La technologie de la chaîne de blocs fournit un outil pour mesurer l'effet de levier dans le système et le risque de contrepartie, et peut surveiller la conformité en temps réel. Il peut également répondre à des questions sur la propriété des garanties. Les monnaies digitales pourraient également profiter aux pays en développement. Parce qu'elles sont peu coûteuses et faciles à utiliser sur les appareils électroniques, les monnaies digitales peuvent permettre un meilleur accès aux services financiers pour les personnes non bancarisées dans le monde.

III. – La définition juridique de la monnaie

Ces cryptomonnaies sont-elles de la monnaie ? Répondent-elles à la définition économique de la monnaie ? On sait que depuis Aristote on attribue trois fonctions à la monnaie : unité de compte, réserve de valeur et intermédiaire des échanges. Vu sous cet angle, les « monnaies virtuelles » répondent à ces trois fonctions. Et l'on pourrait ici retrouver le débat qui secoue les économistes depuis le développement de cette discipline, à savoir celui de savoir qui de la monnaie ou de l'échange est apparu en premier dans l'histoire de l'humanité⁽⁶⁾. En ce sens que le support de la valeur monétaire de l'échange s'est longtemps confondu avec son support physique : coquillage, métaux précieux comme l'or ou l'argent, bien sûr, mais aussi pièces ou billets⁽⁷⁾. Mais beaucoup d'économistes refusent de voir dans ces cryptomonnaies des « véritables » monnaies. Et de se justifier par le caractère régalien propre à la monnaie : celle-ci est et ne peut être émise que par un pouvoir centralisé, hier le roi ou l'empereur, aujourd'hui la

(6) J. M. Servet, Le troc primitif, un mythe fondateur d'une approche économiste de la monnaie, in : Revue numismatique, 6^e série – T. 157, 2001, p. 15-32. La critique de la fable du troc est reprise dans D. Graeber, Dette : 5000 ans d'histoire, Éd. Les Liens qui libèrent, 2013.

(7) M. Amato, L'énigme de la monnaie, Paris, Éd. du Cerf, 2015.

banque centrale. Fondamentalement, la monnaie constitue un attribut de souveraineté, un pouvoir régalién. Or, justement les cryptomonnaies s'inscrivent dans une démarche totalement opposée, celle du refus d'un monde centralisé, d'un pouvoir hiérarchique, d'une organisation verticale de la société. C'est d'ailleurs ce qui a fait que ces « monnaies » ont longtemps été défendues par des mouvements libertariens ou alternatifs. Ce qui caractérise fondamentalement ces cryptomonnaies, c'est l'absence d'organisation centrale puisqu'elles s'inscrivent dans une logique d'architecture ouverte et libre.

Dans la mesure où la technologie blockchain reste encore associée aux cryptomonnaies, il est nécessaire et important de poser les bases juridiques permettant de cerner et qualifier ces cryptomonnaies afin de bien savoir de quoi l'on parle.

On sait qu'il existe plusieurs types de monnaies :

- la monnaie divisionnaire, composée de pièces dont la valeur n'est pas déterminée par la quantité de métal qui les constitue ;
- la monnaie fiduciaire qui regroupe les billets et les pièces métalliques, dont la valeur ne repose que sur un consensus social et non sur la valeur intrinsèque de l'*instrumentum* ;
- la monnaie scripturale qui prend la forme d'une écriture en compte. Le chèque et la carte de crédit permettent l'utilisation de la monnaie scripturale mais ne sont pas des monnaies en soi ;
- la monnaie électronique, qui constitue une forme de monnaie circulant en marge du secteur bancaire mais reposant tout de même, contrairement aux cryptomonnaies, sur la monnaie émise par la banque centrale ; « *C'est une valeur monétaire, 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 acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique* » (Journal officiel de l'Union européenne).

Le concept moderne de « monnaie » renvoie à la banque centrale, comme unique dépositaire de la prérogative de « battre monnaie », même s'il n'en fut pas toujours ainsi.

En effet, si l'existence de la monnaie est – presque – aussi vieille que celle de l'État, il n'en est pas de même avec les banques centrales, institutions relativement récentes puisque le premier établissement à pouvoir être dénommé comme tel est la Banque de Suède en 1668. Ce n'est qu'au XIX^e siècle que la prérogative d'émettre la monnaie a été confiée à une institution séparée de l'État. Et encore, jusqu'au XX^e siècle, ces institutions n'étaient pas toutes des émanations de l'État, même si elles étaient dotées de privilèges. La Banque de France était aux mains d'actionnaires privés jusqu'en 1945 et la *Federal Reserve Bank* de New York, était détenue par les principales banques com-

merciales des États-Unis. Ce n'est donc pas le fait que la monnaie soit émise par une banque centrale qui fonde – tout au moins historiquement – la distinction entre la notion traditionnelle de monnaie et celle de cryptomonnaie.

En revanche, le caractère juridiquement libérateur de la monnaie telle que reconnu par le droit d'un État serait un fondement plus pertinent pour distinguer les monnaies de banques centrales des cryptomonnaies. En effet, tous les pays disposent de leur propre monnaie. Celle-ci est généralement légalement définie dans le corpus juridique national comme la seule monnaie légale utilisable, c'est-à-dire ayant cours légal. Cette dernière notion signifie qu'un créancier ne peut pas refuser le règlement d'une dette par la monnaie ayant cours légal dans le territoire où l'opération est effectuée. L'atteinte au cours légal des monnaies est parfois sanctionnée pénalement. Dans d'autres cas, la sanction relève du seul droit des contrats : la personne qui refuse des monnaies (espèces) ayant cours légal s'expose à ce que sa dette ne soit pas honorée.

En Europe, dans les pays qui disposent de l'euro, la monnaie n'est définie que par son nom⁽⁸⁾. Il n'y a pas de référence à un étalon qui servirait à établir une valeur d'échange de la monnaie. L'euro comme monnaie existe par la seule déclaration de l'État qui décide qu'il s'agit de sa monnaie légale⁽⁹⁾. La monnaie désignée par la loi monétaire se définit aussi par différence avec les autres monnaies nationales, qui sont des devises.

Les cryptomonnaies ne bénéficient bien sûr pas de cette notion de cours légal puisqu'il ne s'agit pas de monnaie légale. Elles ne sont que des conventions monétaires entre des parties à une opération. Ces conventions ne sont pas opposables aux tiers et l'exécution de ces conventions dépend totalement de la bonne foi de chacune des parties.

Bien qu'il ne s'agisse pas juridiquement de monnaie, il n'en demeure pas moins que les cryptomonnaies servent aujourd'hui de valeur d'échange.

Par ailleurs, les banques centrales, comme la Banque de France, n'hésitent pas à rappeler que les cryptomonnaies ne permettent pas, ou de façon limitée, de remplir les trois fonctions essentielles d'une monnaie au sens traditionnel qui sont :

- constituer une unité de compte : leur valeur fluctue très fortement, ce qui ne permet pas d'en faire des uni-

(8) Au sein de la zone euro, l'article 106 TFUE indique : « 1^o La BCE est seule habilitée à autoriser l'émission de billets de banque dans la Communauté. La BCE et les banques centrales nationales peuvent émettre de tels billets. Les billets de banque émis par la BCE et les banques centrales nationales sont les seuls à avoir cours légal dans la Communauté ». Pour préciser cette notion, la Commission européenne a adopté le 22 mars 2010 une recommandation sur l'étendue et les effets du cours légal des billets et des pièces en euros.

(9) C. mon. fin., art. L. 111-1 : « La monnaie de la France est l'euro. Un euro est divisé en cent centimes ».

tés de compte. De fait, très peu de prix sont exprimés dans ces cryptoactifs ;

- être considérée comme intermédiaire des échanges : les cryptomonnaies sont moins efficaces que la monnaie qui a cours légal, dans la mesure où (i) la volatilité de leur cours rend de plus en plus difficile leur utilisation comme moyen de paiement ; (ii) ils induisent des frais de transactions qui sont démesurés pour de simples opérations de détail ; et (iii) ils n'offrent aucune garantie de remboursement en cas de fraude ;
- constituer une réserve de valeur : leur absence de valeur intrinsèque ne permet pas non plus d'en faire des réserves de valeur, inspirant confiance. Les cryptomonnaies ne s'appuient sur aucun sous-jacent réel. Ils sont souvent émis en fonction d'une puissance de calcul informatique, sans considération des besoins de l'économie et de ses échanges, ce qui ne permet pas de leur attacher une valeur intrinsèque⁽¹⁰⁾.

IV. – Essai de définition juridique d'une cryptomonnaie

À défaut de savoir ce que sont précisément les cryptomonnaies, il convient de commencer par dire ce qu'elles ne sont pas.

Comme évoqué *supra*, les cryptomonnaies ne sont pas une monnaie légale, à défaut de disposer du caractère libératoire.

Les cryptomonnaies ne sont pas non plus une monnaie électronique au sens où l'entend le droit européen. Cette dernière supposant une créance de son détenteur contre l'émetteur qui peut à tout moment demander à ce dernier de lui « rembourser » cette valeur contre une somme d'argent dans une devise ayant cours légal. Les cryptomonnaies, elles, ne sont pas émises contre la remise de fonds, au sens de la directive 2009/110/CE du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements.

Les cryptomonnaies ne sont pas des instruments financiers au sens du droit européen en ce qu'elles ne répondent à aucune des énumérations proposées par la directive marchés d'instruments financiers définissant les instruments financiers⁽¹¹⁾.

Enfin, les cryptomonnaies ne constituent pas un service de paiement au sens du droit européen, mais l'échange de devises contre une cryptomonnaie peut être qualifié de service

de paiement au sens de la directive européenne sur les services de paiement⁽¹²⁾. C'est le sens de la jurisprudence précitée de la cour d'appel de Paris, mais aussi la position de nombreux régulateurs en Europe, à commencer par le régulateur français⁽¹³⁾.

Ayant écarté ce qu'elles ne sont pas, reste à tenter un essai de définition des cryptomonnaies.

De façon pragmatique, on peut considérer que ces cryptomonnaies sont des unités de valeur, au sens qu'elles permettent d'échanger des biens et des services. Il ne s'agit pas simplement d'unité de compte, c'est-à-dire d'unité de mesure monétaire, mais bien d'unité de valeur, au sens qu'elles constituent par elles-mêmes une unité d'échange du fait de leur valeur propre. Mais, comme toute unité de valeur, il s'agit juridiquement d'une convention entre des parties. Autrement dit, ce n'est que parce que les parties à un contrat de vente ou d'échange (ou tout autre contrat) acceptent d'être payées en cryptomonnaies que ces unités de valeurs remplissent une fonction monétaire.

D'un point de vue juridique, l'on retrouve ici le débat classique sur la validité des clauses monétaires dans les contrats et la distinction entre monnaie de paiement et monnaie de compte, et plus généralement de la question de l'indexation. En effet, la loi ou la jurisprudence assimilent souvent la clause de valeur monnaie étrangère à une clause d'indexation, laquelle se caractérise par l'existence d'un aléa (qui doit être réciproque entre les parties).

La validité de ces clauses dépend de la législation propre à chaque État mais on peut estimer que la tendance générale est d'accepter la validité des clauses d'indexation dès lors que le contrat présente un caractère international, autrement dit qu'il n'est pas un contrat interne.

Dans certains cas, les États reconnaissent aux devises (c'est-à-dire aux monnaies étrangères) des droits assez proches de ceux de leur monnaie nationale ; la principale différence étant cependant que les devises n'ont pas de cours légal sur le territoire national. Encore faut-il pour autant qu'il s'agisse bien de monnaies étrangères, et non de marchandises. En effet, pour que des droits soient reconnus à ces devises, encore convient-il de considérer que celles-ci soient qualifiées dans leur ordre juridique interne comme des monnaies légales. À défaut, il ne s'agira que de marchandises. Tel est le bien le cas des cryptomonnaies : n'étant nulle part au monde une monnaie légale, elles ne peuvent pas bénéficier du statut de monnaies étrangères et doivent ainsi être traitées comme de simples marchandises.

(10) https://publications.banque-france.fr/sites/default/files/medias/documents/focus-16_2018_03_05_fr.pdf.

(11) Dir. 2014/65/UE, 15 mai 2014, concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE.

(12) Dir. 2015/2366/UE, 25 nov. 2015, concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant la directive 2007/64/CE.

(13) Position du 20 janvier 2014 de l'ACPR relative aux opérations sur bitcoins en France, Position 2014-P-01 et Banque de France, Les dangers liés au développement des monnaies virtuelles : l'exemple du bitcoin, Focus, n° 10, 5 déc. 2013.

Ainsi, un contrat qui prévoirait le calcul de la dette à payer en cryptomonnaies serait un contrat disposant d'une clause de « monnaie de paiement ». Le même contrat qui prévoirait le paiement de cette dette sous forme de cryptomonnaies serait un contrat stipulant une clause de monnaie de paiement, et plus précisément une clause de « monnaie étrangère » c'est-à-dire une clause dont la dette est indexée sur un indice ou un cours de change d'une devise ou d'un actif.

La question pratique qui se pose pour une banque centrale est de savoir si de telles clauses d'indexation seraient valides ou non dans son ordre juridique interne. La réponse dépend soit de ce que prévoit la législation nationale, soit de la jurisprudence nationale. Ainsi en France, la validité des clauses d'indexation est reconnue depuis des arrêts de la Cour de cassation de 1873⁽¹⁴⁾ et 1927⁽¹⁵⁾.

V. – Vers l'émission de cybermonnaies par les banques centrales ?

À première vue, et compte tenu de leur nature disruptive, les cybermonnaies ne devraient pas avoir la faveur des banques centrales, pas plus que des États. Et pourtant, après avoir critiqué ou, à tout le moins, s'être inquiétés de ce phénomène, de plus en plus d'États et de banques centrales réfléchissent sur les avantages que leur apporteraient les cryptomonnaies...s'ils en maîtrisent l'émission et la gestion ! Un document de la Banque des règlements internationaux (BRI) a fait à cet égard grand bruit en 2017. Bien qu'il ne s'agisse pas d'une position officielle de la Banque, mais d'une étude, ce document incite les banques centrales à s'interroger sur la possibilité d'émettre des cryptomonnaies⁽¹⁶⁾, ce que le document appelle des CBCC (Central Bank Crypto Currency). Contrairement à la monnaie échangée par les comptes des banques centrales de manière centralisée, une CBCC serait échangée directement entre le payeur et le bénéficiaire sans intermédiaire central en utilisant la technologie blockchain. La BRI a proposé un CBCC destiné aux consommateurs pour les transactions de détail et une monnaie symbolique de CBCC de gros pour le règlement numérique institutionnel des transactions. En fait, l'idée de voir des banques centrales émettre des cryptomonnaies fait l'objet d'études par certaines banques centrales et universités, comme le projet de FedCoin⁽¹⁷⁾. Mais, plus fondamentalement, cette perspective s'inscrit dans la logique de la disparition de

l'argent fiduciaire. En effet, une CBCC en aurait les mêmes caractéristiques, en particulier un certain anonymat. Car ce qui freine aujourd'hui le mouvement de suppression de l'argent fiduciaire, c'est l'anonymat que permettent les transactions en monnaie fiduciaire. Une CBCC permettrait de garder cette fonction d'anonymat (jusqu'à un certain point, car réduite aux relations bilatérales entre un débiteur et un créancier, mais interdite vis-à-vis des tiers) et ainsi faciliterait la suppression progressive des instruments physiques monétaires tout en gardant la main par la banque centrale sur la circulation de la masse monétaire et donc le pilotage de l'inflation, car elle seule aurait pouvoir d'en émettre. On notera au passage que la création d'une telle monnaie digitale éliminerait le rôle des banques commerciales comme « dépositaire » des fonds, puisque les détenteurs de CBCC auraient directement un compte auprès de leur banque centrale. En fait, une CBCC ne serait rien d'autre que du cash digitalisé.

VI. – Distinction juridique entre un jeton (token) et une cryptomonnaie

Il y a une confusion souvent effectuée entre cryptomonnaies et « token ». Or, les deux ne se confondent pas et il est important pour une banque centrale de bien les distinguer dans la mesure où tous les *tokens* ne permettent pas toujours une fonction de paiement. Un jeton est avant tout un concept technologique. Il confère à son détenteur certains droits en fonction du contenu de la chaîne de blocs ou d'un contrat intelligent (*smart contract*). S'il s'agit d'un actif ou d'un droit sur une blockchain, un jeton peut fonctionner sans cadre juridique *ad hoc* sous-jacent. Les jetons peuvent également représenter des actifs hors chaîne de blocs mais nécessitent alors un cadre juridique spécifique. On peut aujourd'hui schématiquement distinguer quatre types de jetons. Tout d'abord, les « jetons intrinsèques ». Ce type de jeton représente des droits ou des actifs sur la blockchain, comme le Bitcoin ou l'Ethereum. Ensuite, les « jetons à support d'actifs ». Ce type de jeton est adossé à un ou plusieurs actifs hors de la blockchain, comme de l'or, des devises, des biens immobiliers, des droits de propriété intellectuelle. L'utilisation de ces jetons nécessite un cadre juridique particulier, notamment pour en reconnaître la propriété. Il y a aussi, les « jetons liés à des droits » qui, tout comme les jetons d'actifs, sont adossés à des éléments hors de la chaîne de blocs, mais alors que les jetons d'actifs sont adossés à des biens, ceux-ci sont adossés à des droits, comme des droits aux revenus, aux dividendes, à la gouvernance. Là encore, pour être pleinement utilisés, ces jetons nécessitent un cadre juridique *ad hoc*. Enfin, tous les jetons peuvent être utilisés dans une fonction d'échange monétaire.

Fondamentalement (ou sociologiquement), une cryptomonnaie n'est pas différente d'un jeton. Une fois que les jetons ont été créés par une société puis achetés et

(14) Cass. civ., Audience publique, 11 févr. 1873.

(15) Cass. civ., Audience publique, 17 mai 1927.

(16) M. Bech, R. Garratt, Central Bank cryptocurrencies, BIS, Quarterly Review, September 2017, p. 55.

(17) S. Gupta, P. Lauppe, S. Ravishankar, « FedCoin, a blockchain backed Central Bank cryptocurrency », Yale University, 2017 : https://law.yale.edu/system/files/area/center/global/document/411_final_paper_-_fedcoin.pdf.

acceptés au sein d'une communauté, ils deviennent des cryptomonnaies. Mais la réalité est plus complexe. Une cryptomonnaie est, comme son nom l'indique, un mode de paiement (au sens économique du terme) quand un jeton répond à des fonctionnalités beaucoup plus larges, pouvant aller jusqu'à conférer des droits sur des revenus, voire sur la gouvernance d'un projet. Une cryptomonnaie est un logiciel *peer to peer* ou un programme construit à partir d'un code source unique ou cloné à partir d'un autre code source, comme Litecoin, Peercoin, ou bien sûr Bitcoin ou Ethereum, alors que le jeton n'est pas lié à un seul protocole spécifique. En pratique, la ligne de partage entre une cryptomonnaie et un jeton n'est pas claire et nette. Les deux peuvent être utilisés dans une fonctionnalité de paiement. En réalité, la différence majeure entre une cryptomonnaie et un jeton tient à leur structure : les premières sont des modes d'échange liés à leur propre protocole blockchain, alors que les jetons ne sont pas liés à un protocole blockchain spécifique mais à chaque entreprise émettrice. En d'autres termes, une cryptomonnaie est « émise » dans le cadre d'une blockchain, généralement en rémunération d'un travail (le minage) alors que le jeton représente un actif sous-jacent, qu'il s'agisse d'un droit sur des biens sous-jacents, des revenus futurs ou d'échange contre services.

VII. – La blockchain et le droit

Dans quelle mesure la technologie blockchain ne vient-elle pas modifier les règles de droit existantes compte tenu de ses caractéristiques propres, notamment le caractère ineffaçable et inaltérable des informations y figurant, mais aussi les questions de preuve ou de propriété.

Existe-t-il des questions juridiques propres aux activités financières et différentes des questions de droit commun posées par la blockchain ? Il s'agit d'évaluer en quoi celle-ci bouleverse ou non les concepts juridiques traditionnels et, selon le cas, la nécessité ou non de réformer en profondeur certaines branches du droit afin de l'adapter à cette technologie. La question doit être examinée tant sur les domaines transversaux du droit comme la propriété intellectuelle, la protection des données, la signature électronique ou encore la cybersécurité, que dans le droit plus spécifique qui régit les activités de post-marché.

Notre conviction est qu'à ce stade de réflexion, la blockchain ne s'avère pas à ce point incompatible avec le cadre juridique existant qu'il serait nécessaire de créer une nouvelle branche du droit spécifique à cette technologie. Au contraire, le droit commun permet de traiter de manière convaincante la plupart des questions posées par cette technologie. Si des adaptations seront sans doute nécessaires à la marge, en particulier pour la prise en compte du régime de propriété des titres enregistrés dans une blockchain, il s'agit là plus de précision que de modifications substantielles.

C'est aussi l'opinion du groupe de travail Europlace⁽¹⁸⁾ et dans une moindre mesure du rapport de France Stratégie⁽¹⁹⁾.

Chaque législateur, banque centrale ou superviseur, doit procéder à une évaluation de son cadre juridique et réglementaire afin de vérifier si, en fonction de tel ou tel projet, il convient d'adapter cet environnement, voire même créer un nouveau régime particulier. Chaque État doit ainsi procéder à une évaluation de son cadre juridique pour mesurer les écarts existants entre celui-ci et les attentes liées à l'utilisation de cette technologie.

Prenons l'exemple d'un cadastre foncier dont les informations sont enregistrées dans la blockchain ou une DLT. Pour donner plein effet juridique à ces informations figurant dans les chaînes de blocs, il conviendra avant de vérifier les lois relatives aux registres fonciers et au régime des hypothèques.

C'est donc le plus souvent au cas par cas qu'un État décide de reconnaître les effets de la blockchain ; non pas pour toutes ses applications, mais pour des usages particuliers tels que la circulation d'instruments financiers, la signature électronique, la preuve électronique, les *smart contracts*...

Si les initiatives gouvernementales en la matière sont plutôt rares, on peut toutefois relever quelques cas intéressants.

Ainsi, aux États-Unis d'Amérique, plusieurs États ont adopté ou sont sur le point d'adopter des législations reconnaissant les effets de la blockchain : Hawaï (cryptomonnaies), Arizona et Californie (signature électronique), Nevada, Tennessee et New Hampshire (*smart contract*), Delaware (registre des titres des sociétés).

En Europe, la France fait figure de pionnier avec deux textes (2016 et 2017) venant donner légale reconnaissance à l'utilisation de la blockchain en matière d'émission et de circulation de titres de dette sous forme de bons de caisse, mais aussi de titres de sociétés non cotées⁽²⁰⁾.

Plusieurs branches du droit peuvent être affectées par la technologie blockchain et DLT. Signalons, de façon non exhaustive, les situations suivantes :

(18) Europlace, Livre Blanc sur la blockchain : Les Impacts des Réseaux distribués et de la Technologie blockchain dans les Activités de Marché, 2017 : <https://www.paris-europlace.com/fr/actualites/paris-europlace-publie-un-livre-blanc-sur-la-blockchain-les-impacts-des-reseaux>.

(19) France Stratégie : les enjeux de la blockchain, (2018) : <http://www.strategie.gouv.fr/publications/enjeux-blockchains>.

(20) Ord. n° 2016-520, 28 avr. 2016, relative aux bons de caisse, et Ord. n° 2017-1674, 8 déc. 2017, relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers.

Protection des données

La blockchain étant définie comme un registre d'opérations infalsifiable, distribué, vérifiable par tous et reposant sur un consensus, il en résulte que les opérations enregistrées dans une blockchain ont vocation à être inaltérables et donc ineffaçables. S'il est possible d'annuler une opération en passant une opération opposée, il n'est pas possible d'effacer une opération. Les identifiants utilisés par ces technologies sont pseudonymes et non nominatifs, mais permettent cependant l'identification indirecte d'un individu. Plusieurs États disposent de règles relatives à la protection des données personnelles et de la vie privée, et dont la définition de « données personnelles » peut recouvrir les données pseudonymes. Parfois même, ces législations mettent en place un véritable « droit à l'oubli », comme dans l'Union européenne. Lorsque ces législations ont été mises en place avant l'introduction de la technologie blockchain ou DLT, elles n'ont pas pu intégrer les spécificités de celles-ci. D'où parfois de véritables difficultés, comme au sein de l'UE avec le Règlement de protection de données personnelles⁽²¹⁾.

Signature électronique

Les caractéristiques de la blockchain et des DLT en font une technologie particulièrement adaptée pour les signatures électroniques permettant d'intégrer au sein de chaque document numérique une preuve d'intégrité et une preuve de l'identité de l'émetteur.

De nombreux pays ont légiféré depuis de nombreuses années pour introduire la signature électronique à côté de la signature olographe. Mais la reconnaissance de ces signatures passe généralement par la présence d'un tiers de confiance émettant un certificat d'authentification. Alors que les technologies de signature numérique traditionnelles tournent sur un serveur centralisé, ce que l'on appelle l'autorité de certification, en recourant à la blockchain, c'est la signature elle-même qui est insérée dans une chaîne de blocs : l'utilisateur crée une signature numérique, qui peut être utilisée (immédiatement) pour signer n'importe quel contrat. La signature et une référence unique au contrat (appelée « hash ») sont placées sur la chaîne de blocs, où elles peuvent être consultées par tout le monde, à tout moment.

Il convient donc d'évaluer les lois et règlement en vigueur afin de vérifier si la signature électronique via la blockchain peut être considérée comme une signature valide au sens de cette réglementation. En Europe, le Règlement eIDAS⁽²²⁾ est considéré comme étant compatible

(21) Règl. (UE) n° 2016/679, 27 avr. 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

(22) Règl. (UE) n° 910/2014, 23 juill. 2014, sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

avec la blockchain. Aux États-Unis d'Amérique, le *Federal Electronic Signatures in Global and National Commerce Act* (ESIGN Act) et le *Uniform Electronic Transactions Act* (UETA) constituent les bases légales en vigueur aux termes desquelles il convient d'apprécier la technologie blockchain en matière de signature et de *smart contract*.

Cybersécurité

De nombreux pays disposent de lois spécifiques pour traiter les crimes informatiques. Ainsi, l'Union européenne a adopté en 2016 la directive *Network and Information Security* (NIS)⁽²³⁾. Celle-ci définit ainsi la notion d'« opérateurs de services essentiels » au fonctionnement de l'économie et de la société via la définition au niveau national de règles de cybersécurité auxquelles ces derniers devront se conformer et l'obligation pour les opérateurs de notifier les incidents ayant un impact sur la continuité de leurs services essentiels. La technologie blockchain peut là encore apporter des réponses en matière de cybersécurité et les lois et règlements en vigueur doivent être évalués de manière à vérifier si la technologie blockchain est intégrée dans cet environnement légal.

Le droit de la preuve

Le caractère infalsifiable de la blockchain et de la DLT et la possibilité de disposer de tout l'historique de transaction en font des outils techniques précieux en matière de droit de la preuve en prévoyant un enregistrement de provenance immuable où les données ne peuvent être détruites ou falsifiées. Mais le recours à cette technologie devant les tribunaux dépend le plus souvent des règles probatoires prévues par les procédures civiles et commerciales, lesquelles établissent les conditions dans lesquelles les parties peuvent apporter les preuves de leurs différents devant un juge. Même en matière pénale, le recours à la blockchain comme technologie probatoire peut être envisagé. Là encore, il convient de procéder à une évaluation des règles existantes pour déterminer s'il convient ou non de les modifier pour intégrer la preuve électronique, voire pour reconnaître aux actes enregistrés dans la blockchain la même force qu'un acte authentique passé devant notaire.

Le droit de propriété

Les informations enregistrées dans les chaînes de blocs peuvent être de simples preuves de droits ou de biens. Mais il est aussi possible d'aller plus loin et de prévoir que la propriété de ces biens ou droits résulte de leur seul enregistrement dans une chaîne de blocs. Ceci est particulièrement pertinent en matière de valeurs mobilières et de titres : la France a ainsi légiféré en 2016 et 2017 pour don-

(23) Dir. 2016/1148/UE, 6 juill. 2016, concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

ner plein effet aux titres enregistrés dans une blockchain ou une DLT. C'est d'ailleurs dans ce domaine que les cas d'usage pour les banques centrales sont les plus prometteurs en prévoyant les émissions de bons du Trésor et des obligations d'État *via* la blockchain ou une DLT, aussi bien pour les procédures d'adjudication que pour la circulation des titres. Bien sûr, cela nécessite le droit des valeurs mobilières pour reconnaître la propriété des titres digitaux⁽²⁴⁾.

La qualification juridique des *smart contracts*

L'exécution automatique de transactions *via* la blockchain peut apporter de très nombreux changements pratiques dans la vie quotidienne et la vie des affaires. C'est d'ailleurs en matière de *smart contract* que les modifications législatives sont aujourd'hui les plus nombreuses. Pour une banque centrale ou un superviseur bancaire, le *smart contract* peut réaliser de nombreux avantages en matière de sécurité des transactions et des paiements. Encore faut-il que le droit national assimile jusqu'à un certain point cette exécution automatique à un contrat au sens juridique du mot. En pratique, il s'agit de vérifier s'il convient de modifier les lois existantes régissant l'utilisation des formulaires et des signatures électroniques afin d'inclure explicitement les termes « blockchain » ou « *distributed ledger* ».

VIII. – La blockchain et les régulateurs

L'une des principales questions consiste à dessiner les contours de l'intervention/attitude du législateur, de la banque centrale, ou du superviseur bancaire face à cette nouvelle technologie qui semble s'installer durablement dans le paysage économique et financier.

Il semble se dessiner un relatif consensus sur le fait que ce n'est pas la technologie blockchain elle-même qui doit être régulée, mais les usages et les conséquences de celle-ci.

Peu de pays se sont lancés dans une législation permettant d'appréhender les conséquences de la blockchain et des cryptomonnaies. Ce sont, la plupart du temps, les régulateurs qui sont amenés à se pencher sur la question de la régulation au regard de leur propre champ de compétence.

De ce fait, les solutions apportées le sont le plus souvent en fonction des rôles et des missions de ces autorités. Ainsi, une banque centrale n'aura pas la même approche qu'un régulateur bancaire ou une organisation en charge de la lutte contre le blanchiment et financement du terrorisme, ou une administration fiscale. Chacun essaie d'appréhender ces cryptomonnaies ou la blockchain selon son propre angle de vue.

(24) V. H. de Vauplane, Des titres papiers aux titres digitaux, Revue d'économie financière, 2018/1, n° 129, p. 336.

Dans le domaine bancaire et financier, les usages de cette technologie blockchain ou DLT peuvent être mis en œuvre par des établissements régulés ou non régulés. Un nombre de plus en plus important de banques et de sociétés d'assurances mettent en place des projets utilisant la technologie blockchain ou DLT. Mais cette technologie permet aussi aux nouveaux acteurs de la FinTech de lancer des produits ou des services à destination des clients bancaires ou assuranciers. Se pose alors la question de savoir comment réguler ces nouveaux acteurs.

Bien sûr, dès lors que ceux-ci se livrent à des activités bancaires ou financières régulées, ils doivent disposer du statut ou de la licence correspondant à ces activités. Mais bien souvent, ces statuts ou licences sont assez lourds en termes de moyens humains, techniques et financiers pour de jeunes sociétés. L'interrogation consiste alors de savoir si ces FinTech doivent appliquer, de la même manière que les acteurs traditionnels, la réglementation qui leur est applicable, ou bien s'il est possible de prévoir un cadre adapté et temporaire d'adaptation de ces nouveaux acteurs à cette réglementation.

En pratique, l'examen des différentes approches nationales permet de considérer que deux solutions sont possibles :

- la première consiste à ne pas accorder de régime dérogatoire aux FinTech mais considérer une approche pragmatique et factuelle selon le principe de proportionnalité ;
- la seconde prévoit un cadre adapté aux FinTech.

L'approche proportionnelle

Selon cette approche, le principe de base est que la réglementation applicable est la même pour tous les acteurs. Mais cette affirmation est immédiatement tempérée par le principe de proportionnalité : la même réglementation doit être appliquée de façon différente selon le degré de risque présenté par les acteurs. Moins un intervenant présente de risque systémique ou de risque opérationnel vis-à-vis de la clientèle, plus son superviseur devra faire preuve de proportion dans le respect et l'application de la réglementation qui lui est applicable.

Le principe de proportionnalité fait aujourd'hui partie du mode de fonctionnement de la surveillance de la Banque centrale européenne⁽²⁵⁾. En matière de FinTech et d'usage des technologies liées à la blockchain, l'application de ce principe revient à considérer que les nouveaux acteurs doivent se soumettre à l'ensemble de la régulation en vigueur (en particulier en matière de protection de la clientèle et de lutte contre le blanchiment), mais que le superviseur bancaire doit tenir compte du fait qu'il s'agit le plus souvent d'acteurs jeunes et disposant de peu de moyens.

(25) V. principe 7 du Guide relatif à la surveillance bancaire, nov. 2014.

C'est l'approche adoptée en France par l'AMF et l'Autorité de contrôle prudentiel et de résolution (ACPR).

Le bac à sable réglementaire

La technique du bac à sable réglementaire (*Sandbox*) consiste à mettre à disposition d'entreprises innovantes une palette réglementaire dérogatoire du droit commun et un environnement d'essai permettant aux entreprises éligibles de tester des nouvelles technologies ou de nouveaux services innovants dans un environnement encadré par des règles adaptées.

L'image parle d'elle-même : il s'agit pour les « jeunes pousses » de jouer dans un espace bien limité sous l'œil de leurs régulateurs, comme les jeunes enfants jouent sous le regard de leurs parents. Le principe du bac à sable réglementaire est d'être limité dans le temps. Cette approche part du constat que dans le cycle d'évolution classique d'une start-up, les premières phases sont consacrées à concevoir et tester sur le marché une série d'itérations d'un MVP (« *Minimum Viable Product* » ou « *Produit Minimum Viable* »), qui doit converger le plus rapidement possible vers une solution répondant à une attente client avérée et pouvant ensuite être industrialisée.

En matière de blockchain et de cryptomonnaie, cette technique a été d'ores et déjà utilisée par un certain nombre de pays pionniers comme le Royaume-Uni, le Canada, la Suisse ou Hong Kong. Les résultats de cette démarche ont été semble-t-il probants. Au Royaume-Uni, selon le rapport *Regulatory sandbox lessons learned report* publié par la Financial Conduct Authority (FCA) en octobre 2017, 90 % des entreprises qui ont complété avec succès les tests à l'intérieur du bac à sable continuent d'opérer actuellement sur le marché britannique.

IX. – La lutte contre le blanchiment et contre le terrorisme

L'un des risques principaux mis en avant à propos des cryptomonnaies est le caractère opaque des transactions enregistrées sur des registres anonymes, facilitant ainsi les techniques de blanchiment d'argent sale. Le Groupe d'action financière (GAFI) a d'ailleurs souligné, dès 2014, les risques d'utilisation de ces cryptomonnaies dans des

schémas de financement du terrorisme ou de blanchiment d'argent⁽²⁶⁾.

Les dispositifs législatifs nationaux existants ne tiennent généralement pas compte de l'apparition des cryptomonnaies dans leur champ d'application. C'est pourquoi on voit de plus en plus apparaître des projets de réforme de ces régimes afin d'intégrer dans leur champ de compétence ces cryptomonnaies. Ainsi, au niveau Européen, la directive 2015/849/UE relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ne permet d'appréhender que de façon limitée les opérations en cryptomonnaies. C'est la raison pour laquelle la Commission européenne a publié une communication le 5 juillet 2016 afin d'intégrer dans le champ de cette directive les cryptomonnaies. Celles-ci sont définies par la communication comme les « *représentations numériques d'une valeur qui ne sont émises ni par une banque centrale ni par une autorité publique, qui ne sont pas nécessairement liées non plus à une monnaie à cours forcé mais qui sont acceptées comme moyen de paiement par des personnes physiques ou morales et qui peuvent être transférées, stockées ou échangées par voie électronique* ».

La communication de la Commission européenne propose en outre de rendre applicables les dispositions de la directive 2015/849/UE à deux nouvelles catégories de prestataires actuellement actifs dans le domaine des cryptomonnaies : « *les prestataires se livrant principalement et à titre professionnel à des services de change entre monnaies virtuelles et monnaies à cours forcé; et les fournisseurs de portefeuilles offrant des services de stockage des identifiants nécessaires pour accéder aux monnaies virtuelles* ».

Cette communication de la Commission européenne propose aussi de soumettre les deux prestataires ci-avant mentionnés à un agrément ou une immatriculation.

Ceci souligne l'importance pour les banques centrales et les régulateurs nationaux de vérifier si leur législation nationale permet bien d'inclure dans le champ des dispositifs de lutte contre le blanchiment et le financement du terrorisme les cryptomonnaies, à tout le moins pour s'assurer que les obligations de vigilance et de déclaration de soupçon pèsent bien sur les intermédiaires (plateformes d'échange notamment) qui proposent l'achat et la vente de cryptomonnaies. ■

(26) FATF, *Virtual currencies : key definitions and potential AML/CFT risks*, June 2014.