Les crypto-monnaies

Rapport au Ministre de l'Économie et des Finances
Jean-Pierre Landau avec la collaboration d'Alban Genais

4 juillet 2018

Le présent rapport a bénéficié de la contribution et des travaux
de Mme Louise Frion, à laquelle nous exprimons toute notre reconnaissance.

LETTRE DE MISSION

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

LE MINISTRE

Paris, le 22 JAN. 2018

Monsieur le Gouverneur, Cher Jean-Pierre,

Le développement des Fintechs est porteur d'opportunités prometteuses pour notre économie et notre place financière. L'émergence d'un certain nombre de crypto-monnaies telles que le Bitcoin soulève toutefois des interrogations sur les risques éventuels suscités par ces monnaies pour le système financier, notamment du fait de leur forte volatilité.

Ces développements appellent à mes yeux une analyse approfondie, que j'ai décidé de vous charger de conduire.

Vous dresserez, en premier lieu, un panorama aussi complet que possible du développement et des potentialités des crypto-monnaies, en examinant notamment les crypto-monnaies les plus usitées (Bitcoin, Ripple, Ethereum). Vous vous prononcerez sur le statut juridique et financier de ces actifs, et notamment sur la possibilité de les qualifier de monnaies au vu de leurs caractéristiques.

Vous analyserez l'impact qu'un marché mature des crypto-monnaies pourrait avoir sur le fonctionnement et la stabilité des systèmes financiers et de l'économie mondiale, ainsi que sur la protection des épargnants et des investisseurs, mais aussi des intérêts financiers de l'État.

Vous proposerez des orientations sur l'évolution souhaitable de la réglementation nationale, européenne et internationale, en vue de mieux maîtriser les impacts économiques et financiers des cryptomonnaies, mais aussi d'empêcher leur utilisation aux fins d'évasion fiscale, de blanchiment, de financement d'activités criminelles ou de terrorisme. Ces propositions permettront notamment de nourrir les travaux que je souhaite soutenir dans le cadre du G20.

Vous examinerez également les mesures susceptibles d'encourager un développement bénéfique des technologies de registre distribué (*Blockchain*) et des utilisations qu'elles peuvent générer, notamment pour la place financière de Paris. Votre réflexion pourra ainsi éclairer les débats entourant d'autres formes de crypto-actifs, tels ceux issus des levées de fonds sous forme d'émission de jetons (*Initial Coin Offerings*).

Monsieur Jean Pierre LANDAU
Sous-Gouverneur honoraire de la Banque de France
19 rue de Valois
75001 PARIS

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

139 rue de Bercy - Télédoc 151 - 75572 Paris cedex 12

Pour l'accomplissement de votre mission, vous vous appuierez sur les services compétents de la Direction générale du Trésor. Vous conduirez les entretiens qui vous paraissent nécessaires avec les acteurs de marché, les organisations internationales, les régulateurs et les banques centrales.

Je vous saurais gré de me remettre un document de cadrage pour la fin janvier, et un rapport définitif pour la fin mars.

Je vous prie de croire, Monsieur le Gouverneur, à l'assurance de ma considération distinguée.

Bien cordialement,

Bruno LE MAIRE

Comment s'échangera, demain, la valeur sur Internet ? À cette question, les crypto-monnaies apportent une réponse ambitieuse. Il s'agit de créer de nouvelles monnaies, fondées sur une nouvelle technologie : la blockchain. Elle autorise une gestion décentralisée de la monnaie sans tiers de confiance, à l'opposé des systèmes hiérarchisés et centralisés des monnaies officielles.

L'innovation monétaire est encore plus profonde, voire radicale. Les crypto-monnaies sont des monnaies privées, sans cours légal, sans aucun adossement physique ou financier et totalement virtuelles : elles se créent et circulent indépendamment de toute banque et sont détachées de tout compte bancaire. Ce sont des objets monétaires nouveaux, sans véritable précédent dans l'histoire. Il existe aujourd'hui près de 1 600 crypto-monnaies pour une capitalisation de marché estimée à environ 270 milliards de dollars.

Les crypto-monnaies sont l'expression d'un mouvement de société, d'inspiration libertaire, qui rejette les systèmes centralisés et normalisés. La révolte « antisystème » s'exprime d'autant plus aisément dans le domaine monétaire que les banques et, dans une moindre mesure, les banques centrales, ont vu leur image et leur réputation écornées par la crise financière de 2008-2010 et par ses retombées économiques et sociales.

L'ambition des crypto-monnaies est belle, mais difficile à satisfaire : neuf ans après le lancement du Bitcoin, elles sont très peu acceptées et utilisées pour les paiements. Le Bitcoin représente 0,2 % du volume des transactions au sein de la zone euro. Les crypto-monnaies sont lentes et grandes consommatrices de ressources énergétiques : avec une consommation d'électricité égale à celle de la Hongrie, Bitcoin opère aujourd'hui environ 80 transactions par minute, quand Visa et Mastercard en exécutent respectivement près de 100 000. Les crypto-monnaies sont enfin affectées d'une grande volatilité et devenues un objet évident de spéculation.

La cause profonde de cette inefficacité réside dans la gestion décentralisée de la monnaie. Celle-ci impose un processus de validation des transactions lourd, long et coûteux – souvent délibérément coûteux, comme dans le cas du Bitcoin. Ce handicap est durable voire permanent : il est impossible pour un système monétaire de concilier les trois exigences de sécurité, de décentralisation et d'efficacité. D'ores et déjà, le mouvement de centralisation est perceptible dans le fonctionnement et l'architecture des crypto-monnaies les plus récentes.

En outre, la gouvernance des crypto-monnaies, héritée des systèmes d'*open source*, est très peu adaptée aux exigences d'une monnaie stable sur le long terme : le système fonctionne sur des incitations financières de très court terme et les décisions fondamentales – modifiant les algorithmes et les protocoles – sont prises informellement par la communauté des développeurs.

Il n'est pas certain que le modèle économique des crypto-monnaies soit davantage soutenable. Les gestionnaires du réseau sont rémunérés par émission de monnaie, mais celle-ci est, dans la plupart des cas, plafonnée à l'horizon de quelques années. La viabilité future des paiements reposera sur la capacité à facturer aux utilisateurs des frais de transactions qui peuvent être très élevés.

Les crypto-monnaies sont néanmoins compétitives sur certaines activités. Pour les paiements transfrontaliers qui empruntent généralement des circuits complexes et recourent à de multiples intermédiaires, elles introduisent une concurrence très bénéfique, qui pousse d'ores et déjà à la modernisation et à l'amélioration des services.

Malgré ces doutes et incertitudes, il faut prendre les crypto-monnaies au sérieux. L'engouement qu'elles suscitent aide à l'avènement – et au financement – de technologies prometteuses. Elles posent des questions essentielles et profondes sur l'avenir des paiements, de la monnaie et de la finance à l'ère digitale.

Les technologies

Il s'agit d'abord de la blockchain, dont les crypto-monnaies ne sont qu'une des applications possibles. Tant dans la finance que l'économie réelle, on utilise souvent des blockchains privées, sur des réseaux fermés, qui fonctionnent avec un nombre limité de participants. Ces blockchains autorisent des procédures plus rapides et une gestion flexible de la confidentialité. Elles offrent un cadre de gouvernance et d'action collective entre partenaires qui veulent coopérer sur un pied d'égalité. Elles connaissent potentiellement de nombreuses applications dans le règlement-livraison de titres, les paiements transfrontières, la gestion des chaînes de valeur, le financement du commerce international, la tenue des cadastres, la sécurisation des états civils et des dossiers médicaux. Dans tous ces domaines, la France dispose de nombreux atouts, grâce à un écosystème vibrant d'entrepreneurs et de développeurs.

Les crypto-monnaies annoncent également une autre innovation, moins soulignée, mais tout aussi importante : la digitalisation des actifs sous formes de jetons numériques souvent désignés par leur appellation anglaise de « *tokens* ». Il s'agit d'une représentation digitale de valeur, fongible et divisible, pouvant circuler sur Internet et être échangée de pair-à-pair *(peer-to-peer*) sans preuve obligatoire d'identité et avec une finalité de paiement. Grâce à la digitalisation, tout actif matériel ou immatériel (brevets, œuvres d'art, droits d'auteur, etc.) peut potentiellement être transformé en instruments liquides et échangeables. Toutefois les risques d'abus sont importants : le développement de la technologie devra reposer sur un cadre juridique rigoureux et des systèmes de gouvernance sans faille.

Les ICO (*Initial Coin Offerings*) illustrent bien les opportunités et les ambiguïtés de la digitalisation de la valeur. Ce sont des procédures de levées de fonds opérées directement sur Internet. Elles sont apparues en 2016 et se sont rapidement développées dans un environnement de liquidité abondante. Elles cumulent deux grandes innovations : dans la procédure d'appel à l'épargne, en dehors de toute formalité règlementaire, sur la base d'informations de qualité variable ; et dans les droits conférés qui sont très variés (propriété, usage, avantages divers) mais souvent d'une grande ambiguïté. Ce mode d'émission préfigure sans doute l'avenir mais n'offre aujourd'hui aucune garantie réelle aux souscripteurs. Les ICO sont donc des produits risqués, mais néanmoins fréquemment « cotés » dès l'émission sur des plateformes d'échange.

Les politiques publiques

Malgré les interrogations qu'elles suscitent, il n'est pas proposé de réguler directement les crypto-monnaies. Ce n'est aujourd'hui ni souhaitable, ni nécessaire.

Une règlementation directe n'est pas souhaitable, car elle obligerait à définir, à classer et donc à rigidifier des objets essentiellement mouvants et encore non identifiés. Le danger est triple : celui de figer dans les textes une évolution rapide de la technologie ; celui de se tromper sur la nature véritable de l'objet que l'on réglemente ; celui d'orienter l'innovation vers l'évasion règlementaire. Au contraire, la réglementation doit être technologiquement neutre et, pour ce faire, s'adresser aux acteurs et non aux produits eux-mêmes.

À l'exception essentielle de la lutte contre le blanchiment et le financement du terrorisme, une règlementation directe n'est pas non plus nécessaire, car les risques sont aujourd'hui circonscrits. Les encours de crypto-monnaies, élevés dans l'absolu, restent très faibles au regard de la taille des systèmes financiers mondiaux : 1,5 % seulement de la capitalisation de marché du S&P500 et 5,5 % de la valeur totale du marché de l'or. L'exposition des intermédiaires financiers au risque des crypto-monnaies est également minime et le risque de contagion inexistant.

L'écosystème des crypto-monnaies a toutefois un côté sombre évident. L'anonymat peut en faire le support naturel des activés criminelles, du blanchiment et du financement du terrorisme. Il est proposé de renforcer la lutte anti-blanchiment en transformant les actuelles lignes directrices du groupe d'action financière (GAFI) en véritables recommandations obligeant les États membres à se soumettre à un mécanisme d'évaluation par les pairs. La coopération internationale doit permettre d'éviter que la concurrence règlementaire ne conduise à des abus.

Au-delà, il faut dissocier l'innovation technologique, qu'il faut encourager et stimuler, de l'innovation monétaire et financière, qui doit être considérée avec prudence. Dans la phase actuelle, la bonne approche est de laisser les crypto-monnaies – et les innovations qu'elles portent – se développer dans l'espace virtuel qu'elles occupent. Mais, en parallèle, il faut éviter et circonscrire toute contagion. L'effort règlementaire doit donc se concentrer sur les interfaces entre le monde des crypto-monnaies et le système monétaire et financier.

Ces interfaces sont les suivantes :

– les plateformes d'échange pour lesquelles des principes minimaux de transparence, d'intégrité et de robustesse pourraient être définis au plan mondial. Il est proposé, pour la France et l'Europe, d'expérimenter, pour quelques années, un régime d'agrément unique (une « *Euro Bitlicense* ») dans lequel les gestionnaires s'engageraient à respecter les obligations existantes dans les divers statuts correspondant à leurs activités ;
– les banques, dont les activités pour compte propre en crypto-monnaies devraient être fermement dissuadées ;
– les gestionnaires d'actifs, pour laquelle des orientations rapides et claires sont nécessaires. Il existe un danger immédiat de voir les crypto-monnaies pénétrer les portefeuilles de placement des organismes de placement collectif. Elles acquéraient par ce biais une liquidité et un statut, ouvrant la voie à

de nombreux développements (construction d'indices, de produits dérivés, de fonds dédiés) propres à l'apparition d'un risque systémique. Toutes ces évolutions se manifestent d'ores et déjà aujourd'hui à l'intérieur de l'espace des crypto-monnaies. Il est important qu'elles y restent cantonnées. Conceptuellement, ce serait un changement fondamental de qualifier d'actifs financiers des instruments sans valeur d'usage et sans espérance de revenu. Pour la stabilité financière, ce serait un risque majeur. Empêcher ce mouvement doit être une priorité essentielle des politiques publiques.

Les enjeux sont d'abord internationaux, mais les entrepreneurs français engagés dans les crypto-monnaies attendent légitimement une clarification et une stabilisation du cadre comptable et fiscal applicable. Pour les crypto-monnaies elles-mêmes, cette clarification peut être réalisée par alignement du régime comptable et fiscal sur celui des devises, tant pour les personnes physiques que morales. Pour les ICO, l'objectif est d'éviter une imposition prématurée en lissant dans le temps la constatation des produits.

Enfin, les pouvoirs publics devraient promouvoir plus directement la blockchain et la digitalisation des actifs. Certains (notamment la Caisse des dépôts et consignations et la Banque de France) ont d'ores et déjà investi dans les applications liées la blockchain. Les Jeux olympiques de 2024 offrent l'opportunité d'aller plus loin : il est proposé, pour toucher un large public, qu'une partie de la billetterie de ces jeux soit digitalisée à travers des jetons émis sur une blockchain. Entre autres avantages, ce projet permettrait de fluidifier, de rendre plus transparent et de moraliser un marché secondaire toujours très actif pour de tels événements.

Les perspectives monétaires

Les crypto-monnaies visent à transformer la monnaie. Cette ambition est grande et, sans doute, peu réaliste. Mais elles soulèvent des questions fondamentales et légitimes : la monnaie change de forme, mais changera-t-elle de nature sous l'effet de la technologie ? Et si oui, quelles en sont les conséquences pour la stabilité et la politique monétaires ?

L'aspiration à des paiements plus rapides et plus souples peut être satisfaite par les systèmes existants, qui utilisent les monnaies officielles et qui ont fait des progrès considérables, y compris pour les paiements de très faibles montants.

Mais d'autres scénarios sont possibles.

Les paiements en espèces sont aujourd'hui directement affectés par la digitalisation de la monnaie, le développement accéléré des paiements par terminaux mobiles et l'évolution de la réglementation. Malgré cela, l'utilisation du cash se maintient, plus comme réserve de valeur que comme instrument de paiement. Si le cash venait toutefois à disparaître, les citoyens perdraient tout accès à la monnaie publique ayant cours légal. Politiquement, la disparition du souverain en tant que signe monétaire visible ne serait pas neutre. Avec l'extinction des billets, il n'existerait plus, en outre, aucun support pour convertir la monnaie privée en monnaie publique. La dématérialisation totale de la monnaie fragiliserait aussi l'économie et la société, si des catastrophes humaines ou naturelles

venaient à perturber ou détruire les systèmes informatiques sous-tendant la monnaie digitale.

Ces considérations pourraient justifier, de la part des Banques Centrales, la création d'une nouvelle monnaie digitale publique reproduisant exactement les caractéristiques des billets, c'est-à-dire ne portant pas intérêt et ne nécessitant pas l'ouverture d'un compte. Les ménages auraient ainsi accès, comme aujourd'hui, à la monnaie publique dans des formes adaptées à leurs aspirations et au progrès technologique.

Une autre évolution se dessine : la transformation des grands systèmes de paiement en conglomérats rassemblant, dans un même écosystème, les fonctions de banque, de e-commerce et de gestion d'actifs. Cette évolution entraînerait des bouleversements importants pour les systèmes financiers et soulèverait des enjeux majeurs pour les politiques publiques : comment superviser ces conglomérats ? Comment protéger les données privées ? Comment préserver l'efficacité de la politique monétaire ? Sur ce dernier point, des inquiétudes similaires s'étaient manifestées, il y a vingt ans, lors de l'introduction des monnaies électroniques. Elles ne se sont pas concrétisées.

Dans une étape supplémentaire, ces mêmes conglomérats pourraient émettre leur propre monnaie privée et former ainsi une quasi-zone monétaire traversant les frontières. C'est, dans un avenir proche, techniquement et économiquement possible. Des expériences ont d'ores et déjà été tentées avec des monnaies spécialisées, utilisées dans des espaces géographiques plus ou moins restreints : jeux vidéo, systèmes de crédit, attributions de bonus sous forme digitale. Dans cette phase extrême d'évolution, l'économie digitale pourrait créer une concurrence nouvelle entre monnaies privées et publiques, réalisant ainsi le rêve de Hayek d'une « dénationalisation » des monnaies.

Cependant, le facteur technologique ne peut à lui seul suffire à bouleverser les régimes monétaires. L'instabilité naturelle des monnaies privées ne disparaîtra pas nécessairement sur des réseaux larges. Elles resteront confrontées aux difficultés traditionnelles de la gestion du régime d'émission, de l'allocation du crédit et de la détermination du taux de change. Ces difficultés ne peuvent être résolues sans ressources et appui publics.

On ne peut toutefois exclure soit que des monnaies privées s'imposent dans des pays où le régime monétaire est fragile, soit que les grands systèmes de paiement servent indirectement à l'internationalisation des principales monnaies officielles, dont la diffusion et l'utilisation se répandraient au-delà de leurs frontières.

SOMMAIRE

INTRODUCTION

On dénombre aujourd'hui près de 1 600[1] « crypto-monnaies » ou présentées comme telles. Leur diffusion est très inégale. Trois d'entre elles, Bitcoin, Ether et Ripple dominent les transactions et les capitalisations (109 milliards d'euros pour Bitcoin, 50 milliards d'euros pour l'Ether et 22 milliards d'euros pour Ripple)[2].

Un large et vibrionnant écosystème se développe autour des crypto-monnaies. Elles mobilisent une population importante et active de start-ups et d'investisseurs. Elles perturbent potentiellement les banques et intermédiaires financiers traditionnels, à la fois soucieux d'en tirer les bénéfices technologiques et ne pas déstabiliser leur modèle de fonctionnement.

Le dynamisme des crypto-monnaies et l'engouement dont elles bénéficient résultent d'une triple évolution : un progrès technologique réel, un profond mouvement de société et, plus conjoncturellement, des conditions financières très accommodantes.

Le progrès technologique est celui de la cryptographie qui détermine la capacité à sécuriser les transactions sur Internet. Il est désormais possible d'opérer – dans un système ouvert – un réseau totalement sécurisé et totalement décentralisé de transactions anonymes entre un très grand nombre de participants qui ne se connaissent pas et ne se font pas mutuellement confiance. Ces progrès ouvrent des perspectives nombreuses pour le stockage et la transmission confidentielle de données sur Internet. Il est assez naturel que des entrepreneurs innovants s'appuient sur ces technologies pour développer des expériences monétaires et financières.

D'autant plus que ces expériences semblent satisfaire une aspiration forte vers plus d'indépendance, et de décentralisation. On ne doit pas sous-estimer l'influence du courant libertarien dans le développement initial du Bitcoin et le rejet des systèmes centralisés et normalisés. On dénombre, rien qu'en France, plus de 45 « monnaies locales » au développement et à l'influence très restreinte, mais reconnues comme telles depuis la loi relative à l'économie sociale et solidaire (ESS) du 1er août 2014. Internet et la blockchain permettent à ces aspirations de se développer à l'échelle planétaire.

La révolte « antisystème » s'exprime d'autant plus aisément dans le domaine monétaire que les banques et, dans une moindre mesure les banques centrales, ont vu leur image et leur réputation abimées par la crise financière de 2008-2010 et par ses retombées économiques et sociales.

Deux populations en particulier se rencontrent dans leur attrait pour les crypto-monnaies : celles des jeunes passionnés par la technologie, pour lesquels les crypto-monnaies peuvent constituer un prolongement naturel des jeux vidéo (les premières monnaies purement virtuelles se sont d'ailleurs développées à l'intérieur de tels jeux) ; celle, ensuite, des jeunes entrepreneurs et investisseurs que le goût de l'entreprise et du risque rend naturellement aptes à chevaucher de tels mouvements. Il serait imprudent pour les pouvoirs publics, quand ils décideront de leur réponse réglementaire, de négliger ces aspirations et ces soutiens.

Ces enthousiastes ont été récemment rejoints par une catégorie plus traditionnelle d'investisseurs à haut appétit pour le risque. À partir de l'été 2017, un infléchissement s'est manifesté dans la dynamique des cours des crypto-monnaies avec une progression de plus en plus rapide, puis une chute : ces évolutions sont caractéristiques des périodes de bulles. L'hypothèse est d'autant plus crédible que les conditions monétaires et financières ont été exceptionnellement accommodantes : le faible niveau des taux d'intérêt et l'abondance de liquidités poussent naturellement à la prise de risque.

[1] Source : rapport sur la stabilité financière mondiale du FMI d'avril 2018

[2] Source : CoinMarketCap.com, au 4 juin 2018 (chiffres en réduction de moitié par rapport à mi-janvier 2018).

L'actualité immédiate et les vicissitudes rencontrées par les crypto-monnaies ne doivent pas pour autant éclipser leur ambition fondamentale qui, au-delà de la dimension monétaire, est également, et peut-être avant tout, technologique et économique. Un véritable système de production et d'accompagnement se développe autour de l'activité des crypto-monnaies, dans laquelle la France possède de nombreux atouts.

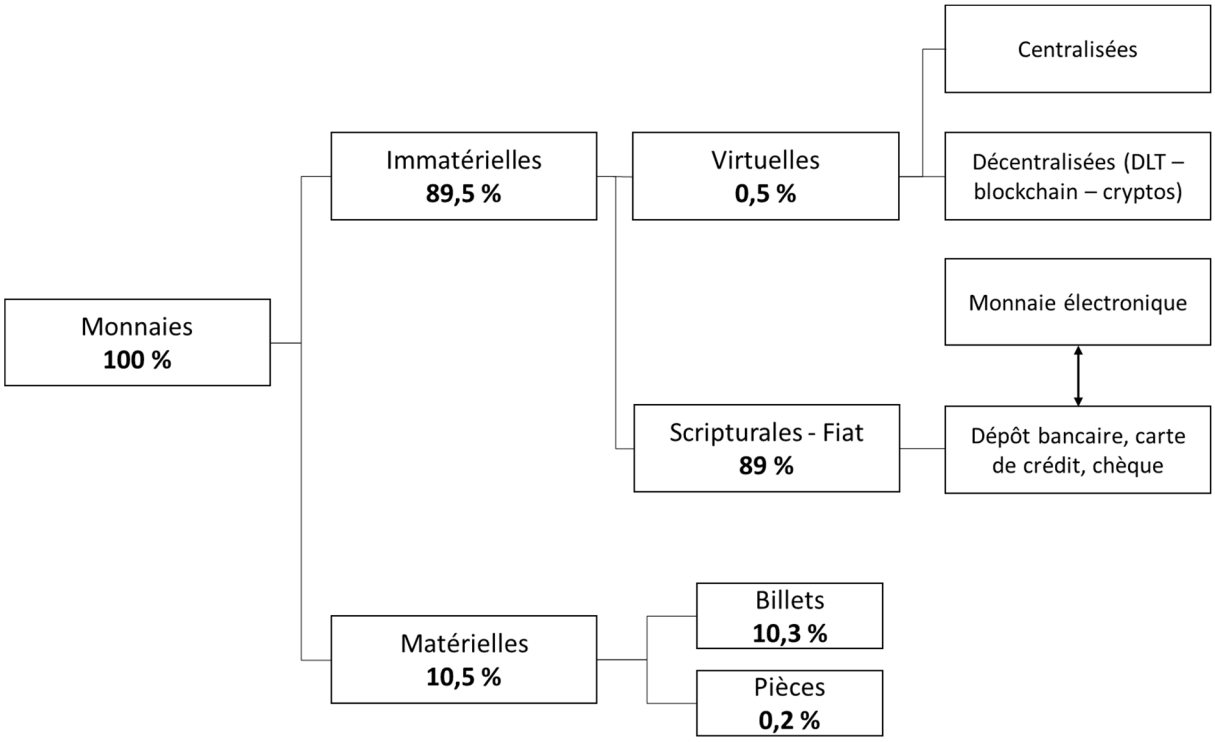
À l'heure où tous les pays s'interrogent aujourd'hui sur la meilleure manière de répondre aux défis posés par les crypto-monnaies, la France se doit de tracer une voie originale, préservant les bénéfices de l'innovation technologique et protégeant l'intégrité des marchés. Y parvenir suppose de répondre aux trois questions soulevées par les crypto-monnaies : que sont-elles ? Comment se développent-elles ? Quelles peuvent être l'attitude et l'action des pouvoirs publics ?

I. QUE SONT LES CRYPTO-MONNAIES ?

Les crypto-monnaies[3] sont des monnaies virtuelles, utilisant la cryptographie pour être échangées en toute sécurité sur Internet et qui, pour certaines, sont gérées de manière décentralisée. Trois caractéristiques définissent donc conjointement les crypto-monnaies :

- ***Ce sont des monnaies virtuelles***, c'est-à-dire des représentations numériques de valeur purement fiduciaires : elles ne sont émises ou garanties ni par une banque centrale, ni par une institution de crédit ou monétaire[4] ;
- ***Elles utilisent la cryptographie*** : elles sont conçues et adaptées pour transmettre de la valeur sur Internet dans un environnement totalement ouvert et public, et en toute sécurité.
- ***La plupart, mais pas toutes, fonctionnent dans un système décentralisé***, où l'information est intégralement, simultanément et également distribuée entre tous les participants. Les transactions sont décidées et validées par « consensus ». Beaucoup, mais pas toutes, sont adossées à la technologie blockchain.

Le schéma ci-dessous présente la place des crypto-monnaies dans l'univers des instruments monétaires.



II ressort très clairement que le poids des crypto-monnaies est aujourd'hui minime, rapporté à l'univers des monnaies avec cours légal, dites monnaies « fiat ».

[3] Les banques centrales soulignent, à juste titre, que les crypto-monnaies ne sont pas de vraies monnaies, dans la mesure où elles n'ontpas de cours légal. Leur utilisation comme instruments de paiement et comme réserve de valeur soulève de nombreuses questions et difficultés, analysées dans le présent rapport. L'utilisation du terme de crypto–monnaie peut donc être jugée infondée. Il y est toutefois recouru dans le présent rapport par pure commodité, dans la mesure où les textes légaux y font explicitement référence, ainsi qu'indifféremment au terme de « crypto-actifs ».

[4] Banque centrale européenne (BCE), *Virtual Currency schemes*, février 2015.

A. La double innovation des crypto-monnaies

Hormis les pièces et billets de banque[5], toute monnaie est aujourd'hui dématérialisée et « digitale ». Elle existe uniquement sous forme électronique. Il en va de même des actifs et titres financiers. Les crypto-monnaies n'apportent, de ce point de vue, aucun changement.

La révolution est ailleurs et plus profonde, à la fois technologique et monétaire. Ces deux éléments sont présents dans la plupart des crypto-monnaies.

1. L'innovation technologique

Beaucoup des technologies de base utilisées par les crypto-monnaies, comme les registres distribués, les techniques cryptographiques et les signatures électroniques, existent depuis plusieurs décennies. L'innovation vient de la combinaison de ces diverses techniques dans un projet ambitieux et cohérent.

L'innovation dans les procédures et dans les registres : la blockchain

- **La technologie des registres distribués (DLT) :** ce sont des registres sécurisés, pouvant être partagés simultanément et de manière synchronisée par une multitude de participants, lesquels peuvent être ou non pré-sélectionnés ;
- **La blockchain elle-même qui est une forme particulière de registres distribués dans laquelle** :

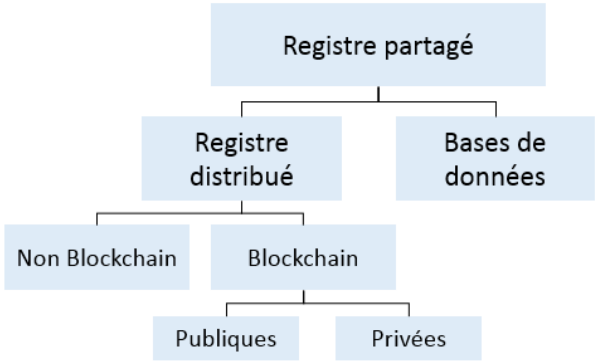
  Les données sont regroupées en blocs successifs dans un registre distribué, sur lequel l'intégralité des informations relatives aux transactions effectuées est stockée dans des blocs.

  Ces blocs sont séquentiellement liés les uns aux autres et numérotés. Un lien cryptographique est établi entre chaque bloc et le suivant. Il est rétrospectivement impossible de modifier, même infinitésimalement, un bloc de la chaîne sans que tous les suivants soient complétement bouleversés de manière immédiatement visible[6]. C'est le grand intérêt de la blockchain. Elle est immuable. On ne peut revenir sur ce qui a été inscrit.
- **Les procédures de consensus** : elles permettent aux participants au réseau de valider collectivement les transactions.

Ces trois composants ne sont pas nécessairement liés et présents dans toutes les crypto-monnaies. On les retrouve intégralement dans Bitcoin et Ether, mais pas dans d'autres crypto-monnaies. Par exemple, Ripple, la troisième plus importante crypto-monnaie, a des registres distribués et des règles de consensus, mais pas de blockchain. La crypto-monnaie IOTA ne s'appuie pas sur une blockchain et la décentralisation n'y est pas totale. Dans les blockchains privées, entre participants se faisant confiance (avec éventuellement des crypto-monnaies attachées), la décentralisation est limitée et les procédures de consensus sont moins développées voire inexistantes, car rendues moins nécessaires.

[5] Qui représentent généralement moins de 10 % de la masse monétaire totale (10 % dans la zone euro).
[6] La fonction de hachage.

Le schéma suivant permet de situer la technologie blockchain dans le cadre existant :



La digitalisation de la valeur

C'est une deuxième innovation que les crypto-monnaies contribuent à promouvoir. Elle est moins présente dans le discours public, mais probablement beaucoup plus significative pour l'avenir. Il s'agit de la capacité à représenter numériquement de la valeur et à la transférer en toute sécurité entre individus sans aucun intermédiaire – constituant ainsi une sorte de « billet de banque » digital. Les représentations digitales de valeur sont couramment appelées des « jetons » ou plus fréquemment encore, par leur nom anglais, des « *tokens* ». La cryptographie moderne permet, le cas échéant, de faire cette opération de manière anonyme. La deuxième partie du rapport discute les perspectives ouvertes par cette innovation.

2. L'innovation monétaire

Pour mieux en saisir la portée, il est utile de décrire les caractéristiques du système monétaire actuel et de mesurer en quoi les crypto-monnaies s'en distinguent.

Les banques, la banque centrale et la monnaie

Dans les économies modernes, la monnaie est majoritairement constituée de dépôts bancaires. Pour l'essentiel, la monnaie est donc créée, détruite et transférée par les banques. Cette monnaie dite « de banque » a plusieurs caractéristiques notables :

- Pour posséder la monnaie et l'utiliser, il faut disposer d'un compte bancaire, nécessaire à l'inclusion financière au sein d'une société ;
- Toute transaction monétaire s'accompagne d'un mouvement de comptes bancaires. Elle est identifiable et traçable. Elle peut être surveillée et règlementée ;
- La monnaie est une créance sur une personne morale identifiable, en l'occurrence la banque. Un dépôt bancaire confère à son titulaire des droits sur la banque, notamment celui de convertir son dépôt en billets, lesquels ont un cours légal ;
- La monnaie de banque est une monnaie « privée ». Elle est donc vulnérable à une perte de confiance dans les banques qui l'ont émise ;
- Mais elle bénéficie, à plusieurs titres, d'un soutien (« *backing* ») public, par le biais de mécanismes d'assurance et de dépôt ou d'un accès au refinancement de la banque centrale ;
- Par ailleurs, c'est la banque centrale qui émet la monnaie servant de « base » au système, ce qui lui confère son cours légal ;

La monnaie électronique et les paiements

De nombreux instruments permettent aujourd'hui d'utiliser et de mobiliser la monnaie de banque. S'agissant des paiements de détail, ces progrès ont donné naissance à de nouveaux supports : cartes bancaires, virements par Internet, monnaie stockée sur téléphones mobiles.

Qualifier ces supports de « monnaie électronique » peut donner à penser qu'ils sont différents de la monnaie « de banque » et que les crypto-monnaies s'inscrivent dans un continuum entre les différentes formes de monnaies électronique.

Cette double impression est trompeuse.

La monnaie électronique n'est pas une nouvelle forme de monnaie. Elle est une des formes modernes que prend la monnaie de banque. Techniquement, il ne s'agit pas de monnaie, mais d'instruments de paiement qui permettent de mobiliser et d'utiliser la monnaie de banque.

Les détenteurs de monnaie électronique sont parfois dispensés d'avoir eux-mêmes un compte bancaire et leurs avoirs sont conjointement regroupés dans le compte bancaire de l'opérateur. Leur identité bancaire se résume à leur numéro de téléphone. Il y a là un instrument puissant d'inclusion financière. Il n'est pas étonnant que ces innovations se développent particulièrement dans les pays émergents à faible bancarisation. Mais un téléphone mobile reflète toujours un compte bancaire : il doit être approvisionné (à partir d'un autre compte) pour être utilisable.

Les crypto-monnaies

Les crypto-monnaies sont fondamentalement différentes. Comme la monnaie de banque, elles n'ont aucune valeur intrinsèque, et sont totalement dématérialisées et digitales. Mais chacune de leurs autres caractéristiques se situe à l'opposé des monnaies existantes :

- Elles se créent et circulent indépendamment de toute banque et sont détachées de tout compte bancaire ;
- Elles ne représentent pas une créance sur une quelconque personne physique ou morale ;
- Il s'agit de monnaies purement privées, sans cours légal, qui ne sont convertibles au pair en aucune monnaie légale[7] et ne bénéficient d'aucun soutien public, direct ou indirect ;
- Elles sont libellées en unités de compte spécifiques, sans rapport avec les monnaies existantes.

Au-delà de la prouesse technologique et de l'apparente proximité avec les monnaies électroniques, il est important de mesurer que les crypto-monnaies constituent une expérience monétaire sans réel précédent. Les formes de monnaie ont constamment évolué dans l'histoire, sous l'effet de la technologie, des institutions ainsi que des conventions sociales. Néanmoins, toutes les monnaies qui se sont développées et imposées dans les économies capitalistes possédaient l'une ou l'autre – ou plusieurs – des caractéristiques suivantes :

- Soit une valeur intrinsèque (les monnaies et pièces en métal précieux) ;
- Soit une contrepartie sous forme d'actif physique ou financier servant à gager leur valeur. C'est le cas de l'étalon-or. Ce fut également le cas, sous une forme différente, des billets émis aux États-Unis par des banques privées pendant la période de « *free banking* »[8], et dont la valeur (au demeurant variable) était gagée par les actifs et le capital des banques émettrices ;
- Soit un soutien public, avec cours légal et refinancement par la banque centrale.

[7] Si les crypto-monnaies ne sont pas convertibles au pair en monnaie légale, elles demeurent convertibles en monnaie légale suivant le taux de change de marché.
[8] Entre 1837 et 1864.

Les crypto-monnaies qui circulent aujourd'hui n'ont aucun de ces trois attributs. Ce sont des objets monétaires totalement nouveaux. Pour cette raison, elles sont qualifiées de « virtuelles ». Il faut donc s'interroger, au-delà de leur volatilité actuelle, sur leur viabilité à long terme, tant d'un point de vue technologique qu'au regard de l'expérience monétaire qu'elles incarnent et représentent.

Les régimes d'émission

Les créateurs des crypto-monnaies ont accordé beaucoup d'importance et d'attention à leur régime d'émission. Ces régimes, assez divers, combinent un mélange de rigueur, d'ambiguïté et d'innovation aux conséquences parfois incertaines :

- la rigueur provient d'un encadrement de la quantité de monnaie émise. Celle-ci est souvent plafonnée, soit en montant final (Bitcoin), soit en taux de croissance (Ether), soit en montant initial (Ripple) ;
- l'ambiguïté vient des conditions dans lesquelles certains fondateurs se « réservent », à l'émission, une fraction du stock de crypto-monnaie. Quand cette fraction est significative, les fondateurs contrôlent directement l'émission effective de la monnaie en cause, dont la valeur dépendra des conditions de libération de la réserve. Ces conditions ne sont pas toujours clairement précisées lors de l'émission initiale. Sous l'hypothèse naturelle que les fondateurs maximiseront les profits qui en résultent, il se peut que les autres détenteurs se voient imposer des transferts ou des pertes ;
- de nouveaux régimes d'émission des crypto-monnaies se déploient. Certaines sont totalement adossées à un « panier » de monnaies avec cours légal, dont elles forment une représentation digitale. C'est le cas de Saga, créée en mars 2018 et adossée aux droits de tirage spéciaux (DTS), la monnaie interne du Fonds monétaire International (FMI). C'est aussi le cas de Tether, créé en 2016 et théoriquement adossé au pair au dollar pour une capitalisation de marché de 2,5 milliards de dollars. D'autres sont plus ambitieuses et visent à stabiliser automatiquement le taux de change de la monnaie virtuelle par rapport à l'une des grandes monnaies fiat. Ce sont les projets dits de « *stable coins* ». Pour ce faire, l'émission et la destruction de monnaies sont contrôlées par un algorithme qui réagit aux variations de cours. Dans les deux cas, la faisabilité des mécanismes restent à démontrer, de même que leur impact sur la stabilité monétaire et financière.

B. La diversité et l'évolution des crypto-monnaies

La conjonction de l'innovation technologique et monétaire a donné naissance à une très grande diversité de crypto-monnaies. Celles-ci se différencient :

- ***Par la technologie sous-jacente*** : toutes les crypto-monnaies sont créées et circulent sur Internet. Mais chacune d'elles utilise un protocole spécifique et recourt à des instruments cryptographiques qui lui sont propres ;
- ***du point de vue de leur architecture générale*** : certaines offrent un degré de décentralisation poussé, que leur confère la technologie blockchain sur laquelle elles sont adossées. D'autres s'organisent en plusieurs « étages » avec un nombre plus ou moins limité de « validateurs », lesquels assurent le fonctionnement du réseau et l'homologation des transactions. D'autres enfin, bien qu'utilisant des techniques cryptographiques, sont pleinement centralisées dans leur gestion ;

- ***du point de vue des fonctionnalités*** qu'elles apportent : une évolution importante est apparue, en juillet 2015 avec la création d'Ether. La blockchain Bitcoin est exclusivement dédiée à la création et la circulation de la crypto-monnaie du même nom. Ether, bien que construite sur les mêmes principes, les mêmes outils technologiques et la même architecture, incorpore des potentialités et fonctionnalités beaucoup plus développées. Elle est, en effet, conçue comme une « *Ethereum Virtual Machine* » (EVM), capable de servir de support à de multiples applications construites par les développeurs externes dans les langages les plus divers. Parmi ces applications figure notamment l'exécution de « *smart contracts* », version digitale des contrats traditionnels, formalisés par un langage informatique non-restrictif, les rendant inviolables d'une part, et capables d'exécuter très rapidement des transactions complexes et sophistiquées d'autre part.

  D'autres crypto-monnaies proposent un éventail plus large de fonctionnalités. Ainsi :

  - Nextcoin offre, d'une part, une place de marché *Peer-to-Peer* de biens et services ainsi que, d'autre part, une plateforme décentralisée d'échange d'actifs. Cette plateforme fonctionne avec des *coloured coins*, lesquels permettent d'associer des actifs réels (actions, biens immobiliers, matières premières) à des adresses Bitcoin[9] ;
  - Mastercoin, également appelé Omni, permet aux détenteurs de Bitcoin d'accéder à des fonctionnalités avancées, telles que la gestion de leurs droits de propriété ou de leur épargne ;
  - Namecoin est une blockchain dérivée de celle du Bitcoin permettant une gestion décentralisée et sécurisée des noms de domaine ;
  - Zerocoin se présente pour sa part comme une crypto-monnaie garantissant le complet anonymat des transactions sur une blockchain également dérivée de celle du Bitcoin.

Les crypto-monnaies sont évolutives et peuvent se transformer ou se multiplier à partir d'une même souche selon le processus des « *forks* ». Ce terme de « *fork* » désigne la scission d'une blockchain donnant naissance à deux nouvelles chaînes partageant le même historique mais divergeant, à partir d'un certain moment, sur leur évolution future (notamment celle des transactions enregistrées)[10]. Un *fork* peut donner naissance à une nouvelle crypto-monnaie. Les deux *forks* les plus célèbres à date ont eu lieu pour des raisons très différentes.

[9] Un «coloured coin» est une somme de bitcoin réassignée pour représenter un actif réel, un méta-protocole permettant d'encapsuler les informations relatives à cet actif sur de petites quantités de Bitcoin.

[10] Un «hard fork» permet de rompre définitivement avec la précédente version de la blockchain, en déviant de la chaîne de blocs initiale sur la base d'un nouveau protocole créé à cet effet. Le « soft fork » s'apparente pour sa part à une simple modification du protocole existant, mais sans création de monnaie nouvelle, le protocole antérieur pouvant être encore utilisé.

Encadré 1 : Principaux « *forks* »

- **Bitcoin Cash en novembre 2017** : une partie des membres du réseau a souhaité augmenter la taille des blocs, afin d'accélérer les transactions. La majorité des participants s'y est opposée, dans la mesure où cette augmentation pouvait conduire à une concentration accrue de l'activité en faveur des participants disposant de la puissance de calcul la plus importante. La minorité s'est séparée pour créer une nouvelle crypto-monnaie, Bitcoin Cash (avec des blocs huit fois plus gros). Bitcoin Cash est aujourd'hui classée au quatrième rang des crypto-monnaies les plus importantes en valeur de marché[11].
- **Ethereum Classic en juillet 2016** : un logiciel fonctionnant sur le réseau de la crypto-monnaie Ether a été piraté, ce qui a donné lieu au détournement d'une somme équivalente à 50 millions d'euros (soit à l'époque 3,6 millions d'Ether, soit plus de 3 % de la totalité des Ethers en circulation[12]). La blockchain étant publique, le détournement a été rapidement détecté. Mais la blockchain étant également immutable, il était impossible d'y remédier sans interférer avec le protocole. Il fallait, pour ce faire, une décision des acteurs du réseau. Encore aujourd'hui, il est difficile de décrire précisément le processus qui a conduit à cette décision. Elle ne fut pas unanime. La majorité a toutefois décidé d'intervenir sur le protocole et d'annuler rétrospectivement la transaction frauduleuse. La minorité s'y est opposée, probablement pour préserver l'intégrité du protocole et a créé Ethereum Classic**.** Un mois plein s'est écoulé entre le piratage (le 17 juin), et le fork (le 20 juillet). Aujourd'hui, Ethereum est la deuxième crypto-monnaie mondiale en termes de valeur de marché, un Ethereum valant 599 dollars, tandis qu'un Ethereum Classic vaut 15,3 dollars et n'est utilisé que par 2 % des membres du réseau Ethereum[13].

C. L'utilisation et la performance des crypto-monnaies

Les crypto-monnaies sont-elles économiquement viables et compétitives, notamment au regard des systèmes de paiement centralisés traditionnels, eux-mêmes en amélioration constante ? La question mérite d'être posée au regard de leurs performances actuelles suivant les trois fonctions traditionnelles des monnaies : instruments d'échange, réserve de valeur, et unité de compte.

1. Comme instruments d'échange et de paiement

Quoique non négligeable, l'utilisation des crypto-monnaies dans les paiements reste infinitésimale par rapport aux monnaies officielles. Techniquement, elles ne semblent pas aujourd'hui en mesure d'offrir une alternative efficiente.

L'utilisation des crypto-monnaies

Il n'existe pas de statistique exhaustive sur l'utilisation des crypto-monnaies. Les indications partielles montrent toutefois les limites de leur diffusion et de leur usage :

- **la détention des crypto-monnaies est très concentrée** : 2,5 % des adresses détiennent plus de 95 % des montants totaux en circulation[14], tandis que 40 % des bitcoins en circulation à fin 2017 seraient détenus par moins de 1 000 personnes[15].

[11] Au 15 juin 2018, selon le site Coinmarketcap.
[12] https://www.nextinpact.com/news/100336-the-dao-pirate-derobe-50-millions-dollars-contre-attaque-se-prepare.htm et https://www.securityinsider-wavestone.com/2016/06/ethereum-x-dao-retours-sur-lattaque-de_30.html.
[13] Coinmarketcap et Consensys.
[14] JP Morgan Perspectives, *Decrypting Cryptocurrencies : Technology, Applications and Challenges*, février 2018 (p.36).
[15] Source : Multicoin capital

- **peu d'adresses sont aujourd'hui actives** : leur nombre oscille entre 500 000 et 700 000 à fin 2017, sur un total de 28,5 millions[16] (moins de 4 % des adresses existantes sont aujourd'hui actives[17]). Ce constat est à nuancer, car une partie des transactions s'effectuent « *offline* », c'est-à-dire entre comptes tenus par des plateformes, et n'apparaissent donc jamais sur la blockchain. Pour ces transactions toutefois, les crypto-monnaies fonctionnent en réalité comme des monnaies officielles, à savoir par des virements de compte à compte.

- **le nombre des points de vente en crypto-monnaies demeure très restreint**[18] **:** il dépend des pays, des cultures et des stratégies commerciales. L'utilisation s'est particulièrement développée dans certains pays, notamment la Corée du Sud. En Europe et aux États-Unis, certaines enseignes visant un public jeune offrent la possibilité de régler en Bitcoins. En Autriche, certains bureaux de poste proposent même de l'Ether ou du Bitcoin contre du cash. Le phénomène reste toutefois marginal. La forte volatilité des cours peut rendre la moindre transaction très coûteuse, dans la mesure où les agents se prémunissent contre le risque en appliquant des marges élevées sur les prix.

  Aux États-Unis par exemple, sur environ 30 millions de petits commerces et de moyennes surfaces, un peu plus de 100 000, soit 0,3 % seulement, acceptaient d'effectuer des transactions en Bitcoin en 2017. Toujours aux États-Unis, seuls 4 des 500 principaux sites d'e-commerce acceptent les paiements en crypto-monnaies au premier trimestre 2018, contre 3 à fin décembre 2017[19]. Au total, ce sont environ 120 000 sites Internet qui acceptent actuellement le Bitcoin comme moyen de paiement à travers le monde.

  En France, aucun grand groupe n'accepte à ce jour de transactions en Bitcoin, la plus grosse société française autorisant de telles transactions étant Showroomprivé.com. Selon le site Bitcoin.fr, 289 commerces physiques acceptaient le Bitcoin à fin décembre 2017[20]. Étonnamment, le Bitcoin est davantage accepté dans les boutiques physiques que dans les boutiques en ligne ;

- **Les transactions au moyen de crypto-monnaies restent très faibles :** le Bitcoin représente, en effet, 0,2 % du volume des transactions au sein de la zone euro ; en montant, les paiements mondiaux en Bitcoin (100 millions de dollars par jour) s'élèvent à moins de 1 % des seuls paiements réalisés par Visa et Mastercard aux États-Unis (respectivement 16,5 et 9,8 milliards de dollars par jour)[21]. En effet, les crypto-monnaies sont très peu utilisées comme moyen de paiement : environ 69 000 transactions ont été réalisées en Bitcoin en 2014 dans le monde, contre 11 134 milliards de paiement par carte bancaire rien qu'en France en 2016 ;

- **Les crypto-monnaies sont principalement détenues pour motif d'investissement** : selon un sondage réalisé en novembre 2017 auprès des détenteurs de crypto-monnaies[22], il ressort que celles-ci sont principalement détenues pour motif d'investissement : sur 564 citoyens américains interrogés, 8 % seulement ont acquis des Bitcoins pour motif de transaction. Entre 2013 et 2016, plus de la moitié des utilisateurs de la plateforme d'échanges Coinbase ont utilisé du Bitcoin pour motif d'investissement et non de transaction[23].

[16] Source : https://www.bitcoinmarketjournal.com/how-many-people-use-bitcoin/ (à noter que la plateforme Coinhouse compte 13 millions d'utilisateurs en janvier 2018).
[17] Rapport précité de JP Morgan, février 2018 (p.36)
[18] Une cinquantaine à Paris, selon l'évaluation la plus courante.
[19] Source : https://www.ft.com/content/29259448-69b3-11e8-b6eb-4acfcfb08c11
[20] http://www.leparisien.fr/economie/que-peut-on-acheter-avec-des-bitcoins-11-12-2017-7446234.php
[21] Chiffres de la BCE (2014) pour les volumes et chiffres de la *Reserve Bank of New Zealand* (2016) pour les montants.
[22] LendEDU : https://lendedu.com/blog/investing-in-bitcoin
[23] https://research.ark-invest.com/hubfs/1_Download_Files_ARK-Invest/White_Papers/Bitcoin-Ringing-The-Bell-For-A-New-Asset-Class.pdf

La performance technique des crypto-monnaies

Cette performance reste globalement modeste au regard des systèmes modernes de paiement. Bitcoin traite aujourd'hui environ 80 transactions par minute, tandis qu'Ethereum, plus rapide, en opère 1 200. Dans le même temps, Visa et Mastercard en exécutent chacun près de 100 000. D'après une récente analyse de Vitalik Buterin réalisée en juin 2018[24], les écarts sont encore plus significatifs : Bitcoin et Ethereum opèreraient respectivement en pleine capacité 4 à 6 transactions par seconde, tandis que Visa est capable de gérer des pics à plus de 20 000 transactions par seconde.

On constate par ailleurs sur le Bitcoin une forte volatilité des frais de transaction que doivent régler les utilisateurs. Il en coûtait ainsi près de 30 euros en janvier 2018 pour effectuer une transaction, quel que soit son montant, contre 5 euros aujourd'hui. La même opération par carte de crédit est en revanche gratuite pour le consommateur et donne lieu à une facturation proportionnelle à la charge des commerçants. Les crypto-monnaies sont donc inégalement compétitives selon les périodes et les volumes de transactions : celles-ci étant facturées en valeur absolue et voyant leurs coûts augmenter dans les périodes de fort volume, elles sont peu compétitives pour les paiements de faibles montants et dans les périodes de forte activité.

2. Comme réserves de valeur et actifs financiers

Les monnaies sont aussi des réserves de valeur. Cette qualité est souvent déniée aux crypto-monnaies, car leurs cours sont très volatils : en moyenne vingt-cinq fois plus que les actions américaines, cinq fois plus que les matières premières et douze fois plus que la devise japonaise, le yen. Il est évident que les crypto monnaies ont nourri, au cours de la dernière année, une forte activité spéculative.

Une volatilité élevée est certainement un handicap, mais ne suffit pas en soi à qualifier la performance des crypto-monnaies comme réserve de valeur :

- une réserve de valeur se juge sur le long terme : elle doit permettre de conserver et de transmettre la richesse sur de longues périodes. Les crypto-monnaies ont peu d'histoire : on ne peut donc automatiquement préjuger de leur comportement ultérieur ;
- il existe plusieurs définitions d'une bonne réserve de valeur. En particulier, une « valeur refuge » est celle dont le prix se maintient, voire augmente, dans les périodes de difficultés et de troubles économiques. Ceci n'exclut pas nécessairement une certaine volatilité en temps ordinaire.

Que valent les crypto-monnaies ?

Les inventeurs et promoteurs des crypto-monnaies les ont dotées d'un attribut, essentiel à leurs yeux : la rareté, liée à leur régime d'émission. L'intuition est simple : la rareté crée la valeur. Les crypto-monnaies sont parfois présentées comme l'équivalent digital de l'or : la réserve ultime de valeur vers laquelle les agents économiques peuvent se tourner pour protéger leurs patrimoines. Elles seraient même supérieures à l'or car, par construction, beaucoup plus aisées à transporter transférer et manipuler

Le raisonnement qui conduit à l'équivalence entre rareté et valeur est partiel, et, dans le cas des crypto-monnaies, problématique. Très généralement, si l'abondance peut éroder la valeur, la rareté ne suffit pas à la créer. Outre l'offre, la valeur dépend de la demande. Un bien très rare mais dont personne ne veut n'a aucune valeur.

[24] https://crypto-analyse.org/2018/06/03/vitalik-buterin-lethereum-realisera-eventuellement-1-million-de-transactions-seconde/

D'où vient donc la demande de crypto monnaie ?

On peut détenir une monnaie parce qu'on pense qu'elle va s'apprécier, sans se préoccuper d'un usage éventuel. C'est une définition possible de la spéculation, qui peut soutenir la valeur d'une monnaie pendant un temps relativement long. Mais elle peut aussi conduire à des chutes brutales. La spéculation comporte des risques, illustrés aujourd'hui par la volatilité des cours. Ces risques sont plus ou moins bien mesurés et perçus par les détenteurs. La spéculation peut difficilement justifier un statut de réserve de valeur sur le long terme.

Dans le cas des monnaies, les fondements de la demande – et de la valeur – sont particulièrement subtils. Les monnaies immatérielles n'ont aucune valeur intrinsèque. Une monnaie immatérielle tire sa valeur soit de son usage, soit de ses soutiens. C'est sous ces deux dimensions – usage et soutien – qu'il faut apprécier les crypto-monnaies :

- Du point de vue de l'usage, on détient de la monnaie car on a choisi de l'utiliser en paiement. Ce ne peut être un choix individuel. Un instrument de paiement est celui qui est adopté par un grand nombre de personnes. Chacun détient la monnaie parce qu'il ou elle pense que cette monnaie sera acceptée en paiement par un grand nombre d'autres personnes, aujourd'hui et dans le futur. La valeur dépend de cette croyance. Sans usage, il n'y a plus de valeur, aujourd'hui ou demain.
- Du point de vue du soutien, une monnaie bénéficie du cours légal, de la convertibilité en billets ou d'un adossement matériel, par exemple à une matière première ou un métal précieux. Les monnaies fiat et l'or bénéficient d'un tel soutien. Pour les premières, c'est le cours légal, l'adossement à la banque centrale et, in fine, le pouvoir et les ressources de l'État souverain. Pour l'or, il s'agit de sa valeur d'usage – bijoux, utilisation industrielle, etc. – et de siècles de tradition historique, qui ont coordonné la croyance sur sa valeur.

Les crypto-monnaies, purement virtuelles et privées, ne disposent pas de ces mécanismes de soutien. Elles n'ont donc pas, aujourd'hui, d'autre limite à la baisse que leur valeur d'usage. Et celle-ci est très faible, voire inexistante car elles ne sont pas utilisées comme moyen de paiement. La valeur des crypto-monnaies est donc particulièrement fragile. Elle dépend totalement des anticipations qu'ont les acteurs de leur usage futur et de la croyance que d'autres vont aussi les utiliser en paiement.

Une acceptation plus large et générale des crypto-monnaies en paiement est donc la base sur laquelle peut se construire, le cas échéant, leur valeur. Aussi longtemps que leur usage restera limité comme aujourd'hui, les crypto-monnaies seront vulnérables et directement exposées à un effondrement de leur valeur, même avec une offre strictement rationnée. Rien, à l'exception des anticipations des acteurs, n'empêche aujourd'hui la valeur des crypto-monnaies de tomber à zéro.

L'évolution de la technologie et des mœurs peut toutefois conduire à des évolutions ou des ruptures brutales des comportements monétaires. On ne peut exclure qu'une crypto-monnaie existante ou à venir s'impose un jour dans les paiements et donc, comme réserve de valeur, présentant une concurrence et un défi pour les monnaies officielles.

En outre, à certaines époques et dans certains pays, les situations de désordre civil ou d'effondrement institutionnel provoquent un effondrement de la confiance dans la monnaie. Les agents économiques peuvent alors se tourner vers des valeurs refuges, même imparfaites, mais très supérieures à ceux qu'offrent les institutions officielles. Le dollar remplit ce rôle dans de nombreux pays. Les crypto-monnaies, dans certains cas plus accessibles, pourraient y trouver leur place.

Les crypto-monnaies comme actifs financiers

Les crypto-monnaies visent également à remplir une fonction voisine : celle d'actifs financiers. Ces actifs diffèrent de la monnaie, car ils ne servent pas directement d'instrument d'échange ; et ils procurent un revenu, certain ou contingent. Comme les monnaies, leur valeur dépend *in fine* de la propension des agents économiques à les détenir dans leurs patrimoines.

Les crypto-monnaies se répandent dans les portefeuilles d'investissement et de placement. Près de 100 fonds spécialisés en crypto-monnaies ont été lancés en 2017 pour un montant total sous gestion s'élevant entre 3 et 4 milliards de dollars[25]. Ces fonds ne prennent pas nécessairement de positions longues sur les crypto-monnaies, mais sont plutôt enclins à exploiter des différences de prix et des opportunités d'arbitrage[26]. Au total, des institutions financières régulées investissent, échangent et opèrent en crypto-monnaies ou en produits dérivés dans au moins huit juridictions. Il y a toutefois des limites. Ainsi, aucun ETF (*Exchange Traded Funds*)[27] n'a été approuvé dans le monde : dix-huit demandes sont en attente auprès de la SEC aux États-Unis.

Faut-il banaliser les crypto-monnaies et les considérer généralement comme des investissements éligibles à l'ensemble des portefeuilles de placement ? Elles sont parfois présentées comme une nouvelle classe d'actifs permettant la diversification et la recherche d'un meilleur couple rendement-risque. Elles paraissent également pouvoir se prêter à des techniques de couverture. Sur leur brève période d'existence[28], les crypto-monnaies présentent une corrélation proche de zéro en moyenne avec les autres classes d'actifs ; une allocation modeste en Bitcoin aurait donc permis d'améliorer l'efficience moyenne des portefeuilles de titres.

Mais, même sous cet angle, elles rencontrent deux limites : premièrement, ce ne sont pas des « valeurs refuge ». Pour se qualifier ainsi, il faut protéger l'investisseur en période de mauvaise conjoncture. Or, quand les marchés chutent, les crypto-monnaies chutent aussi. Deuxièmement, la liquidité des crypto-monnaies est très limitée, ce qui pénalise leur utilisation dans des portefeuilles larges.

Se pose dès lors la question de leur valorisation. Un actif financier peut être considéré sous deux angles :

- celui de sa valeur sous-jacente, définie par le flux de revenus anticipés. Ces revenus peuvent être certains ou aléatoires, conditionnels ou non. Dans le cas des produits dérivés, des options et autres produits structurés, il est souvent complexe de « remonter » au flux de revenus sous-jacent. Mais ce flux existe et peut être estimé (différemment par divers investisseurs) ;
- celui de son comportement observé et prévisible, par rapport à d'autres investissements notamment. L'actif est alors caractérisé par diverses corrélations ou régularités de mouvement qui permettent de mesurer sa contribution à l'équilibre d'un portefeuille.

Les deux approches se complètent naturellement dans les décisions d'investissement. Mais elles ne sont pas équivalentes. Il serait dangereux pour les régulateurs de fonder leurs décisions sur l'observation empirique et contingente des comportements et des régularités de prix. Cette approche peut générer des phénomènes d'anticipations auto-réalisatrices. En l'absence de valeur fondamentale (procurée par un flux de revenu anticipé), rien ne peut arrêter un processus cumulatif de baisse des prix.

Telle est la situation des crypto-monnaies[29]. Les autres actifs ont soit une valeur d'usage, soit un flux anticipé de revenus (certains ou aléatoires). Même les produits et instruments financiers les plus complexes ont cette caractéristique. Ce n'est pas le cas des crypto-monnaies : leur valeur d'usage est aujourd'hui inexistante et, surtout, elles ne génèrent – et ne génèreront jamais – aucun revenu.

[25] Source : *Autonomous Netx*.
[26] Rapport précité de JP Morgan, février 2018.
[27] Les ETF sont des OPCVM indiciels cotés sur les marchés réglementés.
[28] Ibid.
[29] Ce constat ne s'applique pas aux ICO, dont le rendement est très aléatoire et difficilement quantifiable, mais non nécessairement nul.

3. Comme unités de compte

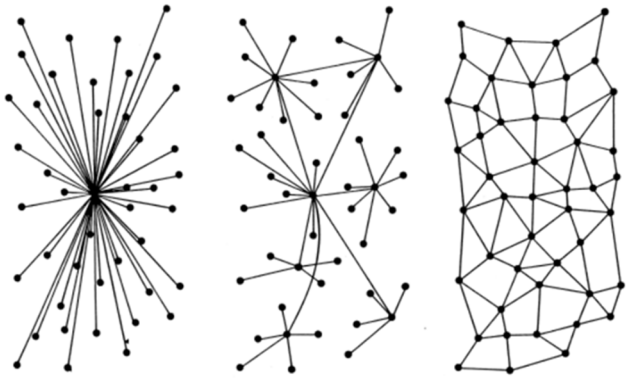
C'est la fonction centrale de la monnaie, en ce qu'elle permet de mesurer et de comparer des biens et services très différents. Une unité de compte permet de libeller les contrats et la dette et d'en fixer le prix de manière certaine à court et à long termes, la monnaie déterminant ainsi une échelle générale des prix. Or, la fonction d'unité de compte ne laisse aucun rôle pour les crypto-monnaies. Aucun exemple de contrats (de vente ou de prêt) libellés en crypto-monnaies n'est recensé à ce jour.

D. Décentralisation et consensus

La décentralisation est au cœur de l'ambition des crypto-monnaies, en rupture totale avec les systèmes monétaires existants, gouvernés par des banques centrales et organisés autour des banques. Au contraire, dans le système Bitcoin, tout le monde tient les registres distribués (DLT) et tout le monde peut proposer et valider des transactions.

C'est la conséquence de l'idéal libertaire qui anime les crypto-monnaies. C'est aussi une source de robustesse. Un système décentralisé résiste mieux aux cyberattaques, un risque dont les développeurs et informaticiens sont particulièrement informés et auquel ils sensibles.

Mais concilier une décentralisation totale et une sécurité absolue n'est pas simple. Toutes les opérations sont visibles sur la blockchain et tout le monde participe aux décisions. Il faut néanmoins que les paiements s'effectuent conformément aux souhaits des participants et sans fraude. Le système repose donc sur des procédures complexes de validation et de consensus. Ces procédures sont robustes. On n'a jamais constaté de fraudes sur le Bitcoin (les nombreux détournements se sont produits dans les systèmes périphériques, les plateformes en particulier). Mais ces procédures sont aussi extrêmement lourdes et coûteuses en ressources. Le système est incapable à ce jour d'absorber un volume croissant de transactions. La communauté du Bitcoin est mobilisée dans la recherche active de nouveaux modes de consensus ou de nouvelles architectures de réseaux. Aucune solution ne paraît s'imposer.



La difficulté du consensus

Pour valider une transaction sur un réseau pleinement décentralisé, il faut résoudre trois difficultés :

- À tout moment, il y a plusieurs milliers de participants actifs. La taille du réseau est variable. Toute personne ou entité peut entrer ou sortir à sa guise. Elle peut proposer des transactions à valider : ce qu'on appelle être un « mineur ». Elle peut participer à la validation des transactions, procédure quasi automatique opérée par les milliers (ou dizaines de milliers) de « nœuds » du réseau ;

- Avec une telle configuration, on ne peut pas prendre de décision. Un vote, par exemple, est impossible car les participants sont masqués derrière des adresses, ce qui ouvrirait la voie à toutes les manipulations. Le consensus est donc une procédure ou certains proposent (les mineurs) et ou d'autres se rallient en validant (les nœuds). Ces ralliements créent plus ou moins rapidement une situation difficilement réversible et les transactions sont validées. Mais ce n'est pas immédiat et la finalité des paiements est généralement moins rapidement assurée que dans les systèmes centralisés ;
- Les communications elles-mêmes ne sont pas instantanées. Il y a un délai de latence sur le réseau, faible mais significatif. Le processus est donc asynchrone : pendant que l'information circule, elle est disponible à certains mais pas à d'autres. Tous les participants ne disposent pas au même moment de la même information[30].

Il n'y a donc ni unité, de lieu ni unité de temps. Trouver un consensus serait aisé si tous les acteurs pouvaient se rassembler à un moment déterminé pour valider ensemble et simultanément les transactions. Ce serait également immédiat, si un seul acteur se voyait déléguer cette responsabilité. Mais la conjonction d'un réseau à configuration variable et d'un processus asynchrone rend le consensus extrêmement compliqué[31].

Ainsi formulé, le problème du consensus est insoluble. L'impossibilité du consensus dans un réseau décentralisé et asynchrone a été formellement démontrée dans un article fondateur de 1982, autour de l'allégorie de « généraux byzantins » assiégeant une ville. Ces généraux communiquent par messagers, et doivent coordonner l'heure de leur attaque malgré la présence de traîtres parmi eux, envoyant des messages erronés[32]. Par généralisation, on parle de « défaillance byzantine » pour désigner des défaillances de réseau indétectables. Les systèmes les plus robustes sont organisés autour de l'hypothèse que chaque acteur peut être « byzantin ».

Il faut donc un élément supplémentaire. C'est la vraie novation avec ces incitations.

Des incitations économiques : le « proof of work »

Il faut donc un élément supplémentaire pour faire aboutir le consensus. L'idée fondamentale des crypto-monnaies est d'introduire des incitations économiques pour susciter la convergence du système vers une solution : un mécanisme qui incite à proposer et à valider des transactions dissuade la fraude et récompense les comportements honnêtes. Cette combinaison de cryptographie et d'incitations économiques est la vraie innovation du Bitcoin[33].

---

[30] En conséquence, différentes parties du réseau peuvent se faire différentes représentations de son état et parvenir en toute honnêteté à différentes décisions, c'est-à-dire à valider différentes transactions. Différentes blockchains peuvent exister simultanément (avec des derniers blocs différents car validés en parallèle dans diverses parties du réseau). Le consensus doit permettre d'en choisir une, les autres devenant « orphelines ».

[31] Velde, F, (2013), « Bitcoin : A primer », Chicago Fed Letter

[32] « *Imaginons que plusieurs divisions de l'armée byzantine soient campées en dehors d'une cité ennemie, chaque division étant commandée par son propre Général. Les généraux communiquent entre eux par messages. Après avoir observé l'ennemi, ils doivent se mettre d'accord sur un plan d'action. Toutefois, des traitres sont parmi eux et essayent d'empêcher les généraux loyaux de parvenir à un accord. Les généraux doivent mettre au point un algorithme pour se prémunir contre toute défaillance : tous les généraux loyaux doivent se mettent d'accord sur un plan d'action commun et faire en sorte qu'un petit nombre de traitres ne puissent les conduire à adopter un mauvais plan…. On démontre que si les messages sont uniquement transmis par oral, aucune solution n'est possible, dès lors qu'il existe un tiers de « traitres ».* «

[33] Ces incitations n'apportent pas une garantie absolue. Les recherches montrent qu'une défaillance est théoriquement possible (Biais). Mais cela ne s'est pas produit jusqu'ici.

La solution économique au problème byzantin précité repose sur deux principes (qui ont des conséquences essentielles sur l'efficacité du système) :

- si on ne peut éliminer la fraude, on peut la rendre extrêmement coûteuse ;
- le coût doit être consenti avant chaque transaction en raison de l'impossibilité d'imposer des pénalités *a posteriori* ;

En application de ces principes pour faire valider une transaction, un mineur doit démontrer qu'il a beaucoup « travaillé ». Concrètement :

- les mineurs souhaitant faire valider un bloc doivent consentir un coût ;
- en pratique, cela revient à consacrer beaucoup de puissance de calcul pour être le premier à résoudre un problème de cryptographie ;
- si le bloc est validé par le réseau, le « gagnant » perçoit une rémunération par attribution de Bitcoins créés à cet effet ;
- si un autre mineur trouve plus rapidement une solution ou si le bloc n'est pas validé, ce coût est perdu.

Le minage génère donc un profit si le bloc est validé et une perte s'il ne l'est pas. Parce que le coût est toujours supporté d'avance, il existe une réelle incitation à produire des blocs valides. Essayer de tromper le réseau coûte cher d'emblée sans grandes chances de succès.

Le problème cryptographique est ainsi construit qu'il est très difficile à résoudre, mais la vérification de la solution (par le réseau) est très facile. En outre, il n'existe pas d'autre moyen de trouver qu'en essayant successivement un très grand nombre de solutions. La seule arme dans cette concurrence entre mineurs est donc la « force brute », c'est-à-dire la puissance de calcul. Dès qu'un bloc est validé, le processus recommence à égalité entre tous les mineurs. Sur la durée, la probabilité pour un mineur de gagner en validant des blocs est donc à peu près proportionnelle à la puissance de calcul mise en œuvre. Pour des raisons de sécurité, la difficulté du problème est ajustée régulièrement en fonction de la puissance de calcul disponible sur le réseau : toute augmentation (diminution) de la puissance de calcul est ainsi neutralisée pour maintenir approximativement constant le débit des transactions.

Encadré 2 : Comment fonctionne le Bitcoin ?

Dans le système Bitcoin, il n'existe pas de compte, pas de soldes, pas de « position », pas de « titulaires » de Bitcoin à un moment déterminé. Seule apparait une succession de transactions inscrites dans la blockchain (par des messages). Les utilisateurs du système ne peuvent être identifiés que par leur adresse électronique. « Posséder » un bitcoin signifie simplement qu'on dispose de la clé privée permettant d'accéder à une adresse où sont précédemment arrivées des transactions en bitcoin[34]. Selon la FED, détenir des Bitcoins ne signifie rien d'autre que d'être en mesure de les déplacer au sein de l'écosystème. Le détenteur de la clé privée peut considérer les transactions arrivées sur l'adresse et enchainer à la suite d'autres transactions vers d'autres adresses. C'est ainsi que l'on « utilise » des Bitcoins.

La création de Bitcoin s'effectue par une transaction spécifique, dont le point d'arrivée est l'adresse bénéficiaire.

C'est pourquoi, la perte de la clé privée est irréparable, dans la mesure où personne ne peut avoir accès à l'adresse et utiliser les Bitcoins qui y sont parvenus. Ceux-ci sont effectivement détruits. On estime qu'une fraction importante (peut-être 30 %) des Bitcoins créés depuis l'origine est ainsi « démonétisée »[35].

À tout moment, des transactions sont proposées à la validation – et diffusées sur le réseau – par des personnes cherchant à échanger des Bitcoins. Ceux des participants qui le souhaitent peuvent agir comme « mineurs » en travaillant (simultanément et en parallèle) à la constitution de blocs rassemblant plusieurs transactions et répondant à des critères stricts de validité définis par le protocole. Supposons définis, à ce stade, ces critères de validité. Quand un mineur pense avoir trouvé un bloc valide, il le diffuse immédiatement en vue de son acceptation par tous les autres membres du réseau.

Le processus pour choisir un nouveau bloc est simple[36]. Le premier « mineur » qui a trouvé un bloc valide l'annonce sur le réseau. Les autres participants vérifient (automatiquement) la validité. Un bloc non valide, au sens du protocole, est aisément détecté par les participants au réseau. Si le bloc est valide, les mineurs qui le souhaitent commencent immédiatement à construire le bloc suivant. Il n'y a pas de « décision ». La validité est consacrée par la décision collective de certains membres du réseau de prolonger la chaîne en construisant un bloc se plaçant à la suite du bloc validé.

La convergence nécessite un délai et il peut exister, pendant quelque temps, une incertitude sur la chaîne – et donc les transactions – valides. Le protocole contient des mécanismes – décrits ci-dessous – qui font en sorte que, lors d'un *fork*, les mineurs ont intérêt à se reporter sur la branche la plus longue, en abandonnant la chaîne courte, qui devient orpheline. Mais deux chaînes peuvent néanmoins coexister temporairement. Pour cette raison, un commerçant réglé d'avance en Bitcoin et dont le paiement a été validé, attendra néanmoins quelque temps pour livrer ce qui lui a été commandé, afin de s'assurer que le bloc contenant son paiement ne deviendra pas orphelin en raison du développement d'une chaîne plus longue. C'est une des frictions inhérentes au système décentralisé.

Une transaction en Bitcoin ne s'efface pas (et n'est donc pas finalisée) avant d'avoir été rajoutée au consensus de la blockchain. Comparée à une monnaie centralisée, cela la rend immutable, mais il est moins certain qu'elle pourra être finalisée, et elle est ainsi irréversible.

L'économie de la production de Bitcoin est peu adaptée à l'émission et la circulation d'une monnaie

Le fonctionnement du « *proof of work* » produit les conséquences suivantes :

Une consommation (délibérément) élevée de ressources

Les ressources dépensées sur les blocs non validés (les plus nombreux) le sont finalement en pure perte. En outre, le protocole neutralise les gains d'efficacité et de rapidité qui auraient pu résulter d'une forte puissance de calcul sur le réseau.

[34] Des logiciels annexes incorporés dans les *wallets* permettent de reconstituer, hors de la blockchain, la position en Bitcoin associée à une adresse.

[35] 800 000 Bitcoins (d'une valeur totale de 6,4 milliards de dollars au 15 mai 2018) sont ainsi immobilisés depuis plusieurs années dans une adresse réputée appartenir à Satoshi Nakamoto.

[36] Bonneau J, A Miller, J Clark, A Naranayan, J A. Kroll and A W. Felten, (2015), «SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies.

Un mode de production très capitalistique

C'est le résultat d'une concurrence par la puissance de calcul. Cette concurrence :

- favorise les mineurs (économiquement et financièrement) les plus puissants, qui sont capables d'investir dans des installations importantes. Afin d'atteindre la taille critique, beaucoup de mineurs se regroupent en « *pools* » qui partagent les capacités de calcul, les coûts et les profits. Une fraction très importante du minage est aujourd'hui effectuée par ces pools ;
- incite à la mise en place de capacités informatiques spécialement dédiées au minage, utilisant des ASIC (*Application Specific Integration Circuits*) plus rapides (mais également plus couteuses) que les CPU (*Central Processing Unit*), à vocation universelle.

La production de Bitcoin est devenue une industrie à part entière, avec des unités de production, véritables « usines » à Bitcoin[37], rassemblant une grande puissance de calcul et géographiquement concentrées dans un nombre limité de pays (Chine et Géorgie notamment).

Ces évolutions marquent une divergence par rapport à l'ambition initiale, décentralisatrice et libertaire du Bitcoin[38]. Elles expliquent également son impact écologique négatif Les chiffres sont connus : la consommation annuelle d'électricité du Bitcoin est actuellement de 40,64 Twh, supérieure à celle de la Hongrie. Elle est 75 fois supérieure à celle de Visa qui, on l'a vu, traite 1 500 fois plus de transactions.

Enfin, cette concentration met en danger la sécurité même du réseau. On sait en effet que si un mineur parvient à détenir seul 51 % des capacités de calcul, il est en mesure, avec le temps, de prendre le contrôle et, en validant à son profit des transactions frauduleuses, de détourner des sommes considérables. Il est possible que certains pools (quatre *pools* chinois concentrent à eux seuls 52 % de la puissance de minage Bitcoin) atteignent aujourd'hui ce seuil mais évitent de se manifester. Un détournement se verrait instantanément et provoquerait un effondrement des cours.

Des cycles de coûts et de prix

Le « *proof of work* » crée dans la dynamique du réseau un enchaînement naturel, qui rappelle beaucoup les cycles de matières premières. Quand la récompense est forte (le prix du Bitcoin est élevé), le minage devient très profitable et la puissance de calcul investie sur le réseau augmente. Cette puissance de calcul additionnelle n'améliore ni l'efficacité, ni la rapidité du système, car elle est automatiquement neutralisée par le protocole pour préserver la sécurité du réseau[39]. Par contre, les coûts s'élèvent et il faut de plus en plus de ressources pour assurer le même nombre de transactions.

Cet enchaînement s'est manifesté pour le Bitcoin[40] pendant le deuxième semestre 2017 et les premiers mois de 2018. Comme l'illustre le graphique ci-dessous, l'augmentation du volume des transactions a entraîné une hausse parallèle des capacités de calcul (le « *hash rate* ») mais également une croissance des coûts unitaire de transaction.

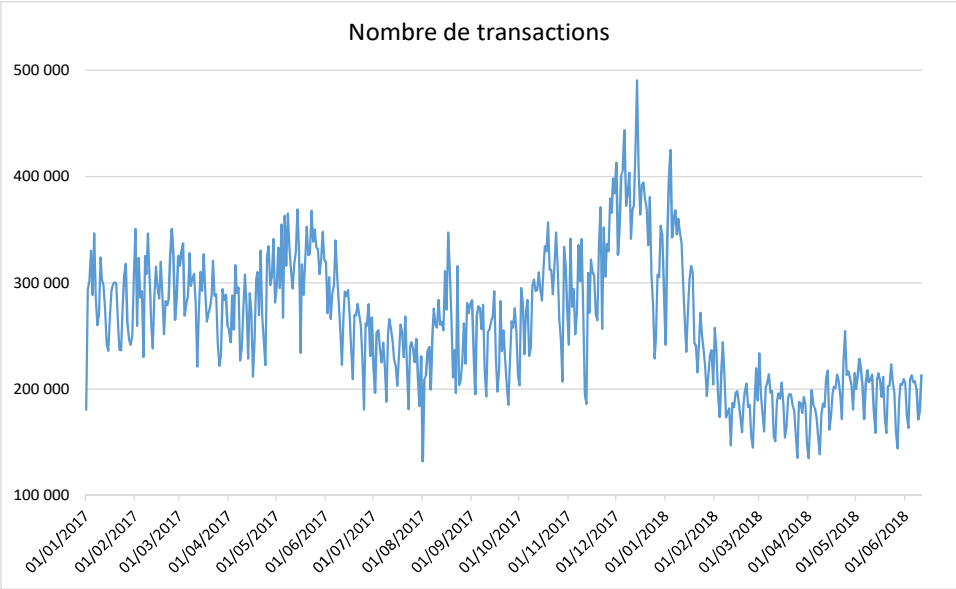
Économiquement, le Bitcoin se comporte alors comme un système monétaire et un système de paiements à coûts marginaux croissants : chaque unité monétaire nouvelle coûte plus chère à produire et à transférer que la précédente. Par contraste, les systèmes de paiements traditionnels fonctionnent à coûts décroissants. Ils deviennent plus compétitifs quand les volumes augmentent : chaque billet supplémentaire coûte moins cher à imprimer et à mettre en circulation que le précédent ; il en va de même pour chaque virement bancaire ou chaque paiement électronique additionnel. Pour les crypto-monnaies en tant qu'instruments d'échanges, c'est évidemment un très gros handicap.

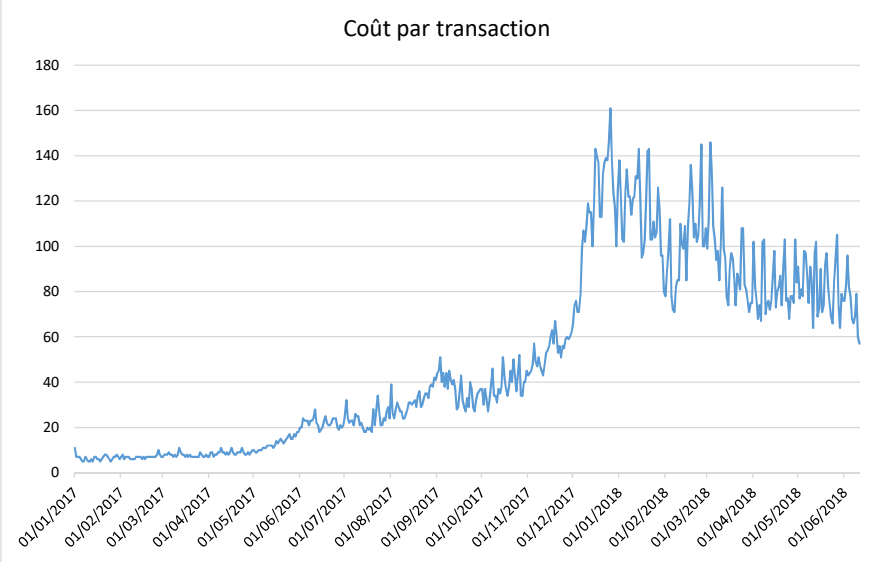
[37] Ensembles d'ordinateurs dédiés au minage.

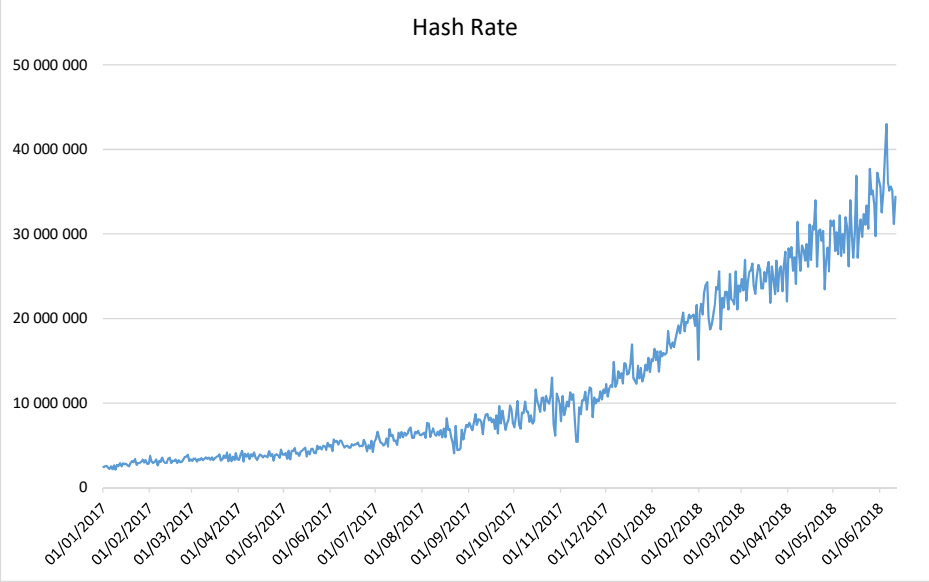
[38] Une leçon économique plus générale. Penser aux effets indésirables ou inattendus quand on construit un système purement basé sur des incitations individuelles.

[39] Il s'agit de la procédure d'ajustement par la difficulté.

[40] Mais pas pour l'Ether et d'autres crypto monnaies.







Source : Mission, Blockchain.info.

L'impossible montée en puissance

Les crypto-monnaies sont confrontées à un double problème de congestion : congestion future du réseau car la taille de la blockchain augmente avec chaque nouvelle transaction et elle doit être intégralement recopiée sur des milliers d'ordinateurs[41]. Mais surtout congestion immédiate du processus en raison du « *proof of work* » : la sécurité qu'il procure se paye d'une impossibilité de traiter des volumes élevés de transactions à des coûts compétitifs vis-à-vis des systèmes de paiement existants.

Ce problème est reconnu par la communauté des développeurs, qui s'est engagée dans un effort de grande ampleur pour trouver des solutions, plus ou moins radicales. Celles-ci s'inspirent d'approches diverses (voir annexe n° 9) :

- améliorer les paramètres techniques du réseau sans changer le « *proof of work* » : par exemple, s'agissant du Bitcoin, augmenter la taille des blocs[42] .
- modifier la structure du réseau, en créant un réseau de « deuxième couche » en dehors de la blockchain pour les paiements de petits montants (« le *lightning* ») ;
- changer le consensus lui-même – cette évolution étant la plus radicale – en abandonnant le « *proof of work* » pour lui substituer un « *proof of stake* ». L'idée fondamentale est simple : la validation des transactions serait déléguée à ceux qui accepteraient de mettre en gage de leur honnêteté (dans une adresse dédiée) les avoirs qu'ils possèdent en crypto-monnaies. Chacun de ces validateurs volontaires posséderait un pouvoir de vote proportionnel à ses dépôts. On éviterait ainsi la consommation de ressources imposée par le « *proof of work* ».

L'impossible conciliation

Aucune de ces solutions n'est mûre et toutes semblent nécessiter des compromis avec les objectifs initiaux. Le « *proof of stake* » donne le pouvoir aux détenteurs de la monnaie et peut accroître *in fine* la concentration et la vulnérabilité aux attaques. Le « *lightning* » et le « *proof of stake* » nécessitent l'immobilisation de liquidités préalablement à l'exécution des transactions. Le « *lightning* » recrée un système de paiement à deux niveaux « hiérarchiques » qui ressemble à l'architecture des systèmes existants.

Les crypto-monnaies se heurtent donc à beaucoup des problèmes rencontrés depuis quelques décennies par les systèmes de paiements centralisés, que ceux-ci ont jusqu'ici résolus avec beaucoup de succès. Elles s'orientent probablement vers des solutions similaires.

Globalement, le mouvement de recentralisation est clair : dans la production de crypto-monnaies et le minage ; dans les procédures de consensus avec le « *proof of stake* » ; dans l'architecture même des réseaux, les crypto-monnaies les plus récentes (Ripple, IOTA) fonctionnant avec des réseaux à plusieurs niveaux et un nombre limité de validateurs pré-désignés.

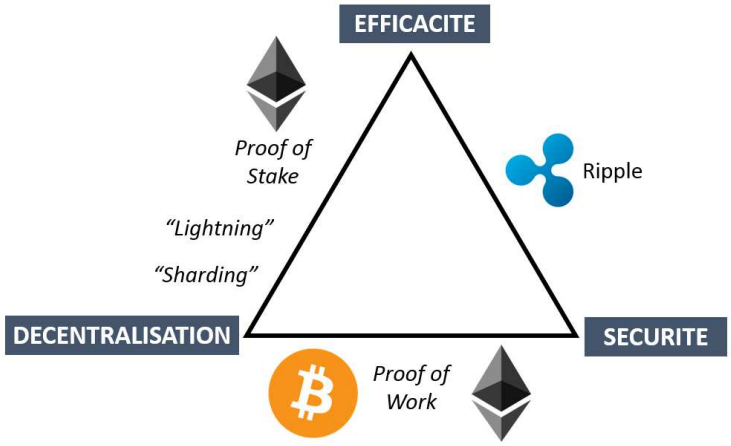
L'expérience semble dégager un enseignement fondamental. **Il est impossible à un système monétaire et de paiement de concilier pleinement les trois objectifs de (1) sécurité, (2) rapidité et (3) décentralisation[43].** Un choix est nécessaire. Cette intuition[44] est illustrée dans le « triangle d'incompatibilité » ci-dessous :

[41] Cf. rapport annuel BRI

[42] Un débat anime depuis trois ans la communauté sur l'augmentation de la taille des blocs. Les divergences ont donné lieu en août 2017 au seul « *fork* » majeur ayant affecté cette crypto-monnaie avec la création de Bitcoin Cash, pour lequel la taille de chaque bloc est portée à 8 Mo, contre une taille de 1 Mo pour Bitcoin ;

[43] Le « *proof of work* » assure, dans les faits, une très grande sécurité et une décentralisation totale mais ne pourra jamais élever sa performance. D'autres monnaies font des choix différents : Ripple, par exemple, fonctionne sur des registres distribués et des validateurs désignés.

[44] Exprimée à diverses reprises par Vitalik Buterin, le fondateur d'Ether, lui-même



Ce « trilemme » ne peut être résolu par les progrès anticipés dans la transmission des données. Ces progrès, quand ils viendront, bénéficieront tout autant aux systèmes centralisés qu'aux monnaies décentralisées, et n'élimineront donc pas le handicap de ces dernières.

E. Le modèle économique

Le seigneuriage privé

Le coût de production d'un signe monétaire est très généralement inférieur à sa valeur nominale. Produire de la monnaie génère donc un profit, un revenu, appelé seigneuriage. Historiquement, le seigneuriage sur les monnaies publiques est une source significative de revenus pour les États. Il en va de même pour les monnaies privées : leur émission engendre donc un seigneuriage privé. Il est très difficile à évaluer précisément pour les crypto-monnaies, car leur valeur nominale est incertaine. Les valorisations actuelles fournissent un ordre de grandeur et indiquent qu'à l'échelle de patrimoines privés, ce seigneuriage est, pour les émetteurs, une source de revenus considérables. Il est probable que son appropriation constitue, dans certains cas, une motivation essentielle de la création de crypto-monnaies.

Les modes d'allocation – les « *business models* » – sont toutefois très différents selon les monnaies :

- le seigneuriage peut être affecté au fonctionnement du système. C'est le cas du Bitcoin, de ce point de vue totalement transparent et intègre. Toute nouvelle émission de Bitcoins est utilisée pour rémunérer les mineurs ;
- le seigneuriage peut être – totalement ou partiellement – approprié par les créateurs ou développeurs de la crypto-monnaie. Par exemple, la totalité de la monnaie peut faire l'objet d'une émission unique, dont une part est réservée aux fondateurs. Le *business model* consiste alors, pour ces derniers, à laisser la monnaie se valoriser en développant son utilisation et à bénéficier de son appréciation ;
- c'est une composante essentielle de beaucoup d'ICO dont, finalement, la logique est de partager d'emblée un seigneuriage (aléatoire et futur) entre souscripteurs et entrepreneurs. Si le projet réussit, la monnaie qui le sous-tend gagne en valeur ;
- cette pratique peut être problématique, car elle donne aux fondateurs un pouvoir important sur la valeur future de la monnaie, s'ils conservent un pouvoir discrétionnaire sur son émission (c'est-à-dire les conditions dans lesquelles ils céderont leurs réserves). Si les règles d'émission futures ne sont pas claires, les autres détenteurs peuvent se trouver « dilués ». Cette incertitude affecte beaucoup de crypto-monnaies et pèse sur la valorisation des ICO.

Au total, le *business model* de certaines crypto-monnaies comporte un mélange de rigueur monétaire apparente (l'émission est plafonnée) et d'incertitude (voire de manipulation) financière qui peut porter atteinte à l'image des crypto-monnaies et compromettre la confiance.

La question des frais de transaction

Le minage dispose d'une seconde source potentielle de revenus. Quand une transaction est enregistrée, le vendeur et l'acheteur peuvent proposer de payer des frais de transactions, avec un paiement sous la forme de bonus pour le mineur qui résoudra le problème permettant de vérifier la transaction. Ces frais sont optionnels, mais 97 % des transactions en 2014 les incluaient. Les frais permettent aux utilisateurs d'indiquer l'urgence de leur transaction : naturellement, les mineurs donnent la priorité aux transactions proposées avec les frais les plus élevés.

Pour le Bitcoin, la dynamique des frais de transaction suit très étroitement celle des coûts : ils augmentent et diminuent avec les volumes. Entre octobre 2017 et janvier 2018, ils sont ainsi passés d'environ 3 euros[45] à plus de 30 euros par transaction, avant de redescendre en dessous de 5 euros. C'est une source de friction et un possible handicap de compétitivité supplémentaire face aux monnaies officielles.

Le part des frais de transaction dans la rémunération des mineurs est appelée à s'accroître avec l'épuisement progressif de la création de Bitcoin. Les frais de transactions deviendront les seules sources de revenus une fois que tous les bitcoins auront été créés. Il n'est pas évident que le modèle soit robuste face à de tels changements dans son environnement et dans les incitations auxquelles sont soumis les mineurs. On peut imaginer des situations dans lesquelles les usagers seront réticents à payer en frais de transaction les coûts réels du minage (actuellement financés par seigneuriage), auquel cas le système s'arrêtera. Il est fondamental de comprendre si le Bitcoin fonctionnera encore « en pratique », si la pratique elle-même est appelée à évoluer[46].

F. La gouvernance des crypto-monnaies

L'histoire, l'expérience et la théorie ont apporté de nombreux enseignements sur la bonne gouvernance des monnaies. Les fonctions de la monnaie, notamment comme réserve de valeur, imposent des exigences spécifiques : un horizon de très long terme, une prise en compte du bien public et une capacité à réagir aux chocs. Un horizon de très long terme est nécessaire pour que les agents économiques acceptent de détenir la monnaie et l'utiliser, le cas échéant, comme instrument d'échange. La considération du long terme exclut, par définition, l'opportunisme. L'autorité responsable de la monnaie ne doit pas être incitée à rechercher des profits ou des avantages immédiats. Le succès des politiques monétaires depuis trois décennies doit beaucoup à un cadre institutionnel qui exclut le « court-termisme » grâce, notamment, à l'indépendance des banques centrales :

- Une monnaie est un bien public. L'ensemble des agents économiques, pas seulement ses détenteurs, ont un intérêt à sa stabilité. La gestion de la monnaie produit des effets directs sur le bien-être de ceux qui n'en détiennent pas ou peu ;

[45] http://assistance.bitconseil.fr/support/solutions/articles/31000135178-frais-de-transactions-trop-faibles
[46] Bonneau.

- la gouvernance doit permettre de réagir à des chocs imprévus sur la demande de monnaie et de liquidité. Les mandats de certaines banques centrales mentionnent la nécessité d'une « offre élastique de monnaie ». Il peut être pénalisant que cette offre soit contrainte en toutes circonstances[47].

La gouvernance des crypto-monnaie est exactement symétrique :

- Les incitations des mineurs sont à très court terme, à l'horizon de quelques blocs. Une fois leur rémunération perçue et, le cas échéant, convertie en monnaie officielle, ils n'ont aucun intérêt direct à la gestion de la monnaie ;
- Les décisions fondamentales – celles modifiant les algorithmes et les protocoles – sont prises informellement par la communauté des développeurs, selon le mode traditionnel de la gestion des protocoles en *open source*. Il existe diverses modalités : des forums réguliers en ligne, des conférences exceptionnelles, des procédures plus ou moins organisées de consultation. Dans le cas d'Ether, une fondation suisse assume *de facto* la gouvernance en provoquant et en suscitant les décisions d'organisation nécessaires.
- L'émission des crypto monnaies est réglée par un algorithme, en principe immuable.

La gouvernance des crypto monnaie est donc souple là où celle les monnaies officielles est rigide ; inversement, elle est figée là où (règles d'émission) les monnaies officielles sont flexibles.

Cette gouvernance est-elle soutenable ? Elle repose essentiellement sur l'engagement informel de la communauté des développeurs, et la permanence d'un réseau de mineurs. Ces deux ancrages sont fragiles :

- Les développeurs sont motivés mais souvent divisés. Les protocoles régulant les crypto-monnaies sont très fréquemment modifiés ou amendés : on recense ainsi, depuis 2017, 31 modifications, dont 8 pour le seul Bitcoin. Pour la plupart, ces amendements sont techniques et visent à corriger ou à améliorer le fonctionnement du réseau. D'autres, plus rares, transforment en profondeur les caractéristiques de la crypto-monnaie. Ils ne sont pas toujours consensuels et, en l'absence de règles de décision, donnent lieu à des scissions au sein des systèmes monétaires, les « *forks* », qui sont peu fréquents mais témoignent néanmoins de la fragilité inhérente à une gouvernance informelle et décentralisée ;
- L'incertitude majeure vient de l'absence d'acteur garantissant, dans la durée, la pérennité de la monnaie. L'hypothèse implicite, mais centrale, est que la combinaison des protocoles et des incitations économiques données aux mineurs est suffisante pour assurer cette pérennité ;

  Cette hypothèse est probablement insuffisante. Elle néglige, par exemple, les rapports de force au sein du réseau, de plus en plus manifestes avec la concentration tant des capacités de minage que de la détention des crypto-monnaies. Dans un sondage récent, plus de 60 % des mineurs estiment, en effet, avoir une influence sur la définition et les caractéristiques des protocoles ;

[47] Un débat anime toutefois depuis longtemps les économistes et responsables de la politique monétaire sur l'opportunité de soumettre celle-ci à des « règles ». L'approche par les règles a de nombreux et éminents partisans (qui peuvent se retrouver dans une gestion algorithmique de la monnaie). La majorité des responsables estiment néanmoins nécessaire de préserver la « discrétion » des décisions monétaires, dans le cadre de mandats bien définis et avec les garanties institutionnelles nécessaires.

> Les incitations elles-mêmes sont fragiles. Pour le Bitcoin par exemple, la rémunération des mineurs est libellée en Bitcoins, tandis que les coûts le sont en monnaie officielle. Une chute des cours de Bitcoin peut donc rendre le minage non profitable, conduisant à une hausse des frais de transactions voire à un abandon de l'activité, une paralysie du réseau signifiant la disparition de la crypto-monnaie considérée. Il paraît hasardeux de postuler, dans une telle circonstance, que l'intérêt bien compris de quelques mineurs les amènerait à assurer à perte le fonctionnement du réseau, dans l'anticipation d'un retour à la normale.

Les crypto-monnaies sont donc probablement confrontées à un dilemme de gouvernance pour l'avenir : soit vivre dans l'informalité actuelle et en accepter la fragilité et les aléas (avec un risque permanent pour la survie des systèmes) ; soit évoluer vers une gouvernance plus formelle et donc probablement plus centralisée. Ce dilemme peut apparaître rapidement quand des décisions importantes devront être prises soit pour modifier les régimes d'émission sous la pression de la demande, soit pour changer les protocoles pour assurer la croissance du nombre de transactions[48].

[48] Une échéance importante interviendra pour Ether en 2019, date à laquelle la difficulté du *Proof of Work* est programmée pour atteindre des niveaux insoutenables, contraignant à un basculement vers un autre protocole (problème connu sous le nom de « *time bomb* »).

II. L'UNIVERS DES CRYPTO-MONNAIES

La dimension monétaire est importante dans le projet qu'incarnent les crypto-monnaies. Mais elle n'est pas exclusive. L'ambition est également, et peut-être d'abord, technologique et économique. Un véritable système de production et d'accompagnement se développe autour de l'activité des crypto-monnaies, dans laquelle la France possède de nombreux atouts. La blockchain elle-même offre de nombreuses perspectives. La possibilité de stocker et de transférer de la valeur sur des unités virtuelles, divisibles et fongibles (les « *tokens* ») peut changer le paysage de la finance, des échanges et de la production. Dans le foisonnement actuel d'initiatives et de projets, il est important de bien identifier les opportunités et d'en mesurer les risques.

A. Deux nouveaux horizons technologiques : la blockchain et la digitalisation de la valeur

1. Les applications et perspectives de la blockchain[49]

L'innovation progresse par vagues successives, avec des phases d'accélération où la diffusion des idées suscite une mobilisation des initiatives, des énergies et des financements. C'est une telle phase que traverse aujourd'hui la technologie des DLT et de la blockchain, grâce, en partie au moins, à l'intérêt et l'engouement que suscitent les crypto-monnaies.

Celles-ci utilisent des blockchains publiques avec accès universel et, donc, des procédures très développées de consensus. Au contraire, beaucoup des applications « non monétaires », dans la finance et l'économie réelle, utilisent des blockchains privées, « avec permission », c'est-à-dire des réseaux fermés, avec un nombre limité de participants.

Ces blockchains privées se construisent autour d'architectures très diverses et présentent plusieurs avantages :

- Des procédures de consensus très allégées avec beaucoup moins de contraintes de validation, puisque les participants sont sélectionnés et se font mutuellement confiance. Les mouvements sont moins coûteux et plus rapides. La technologie peut alors rivaliser en performance avec celle des systèmes centralisés ;
- Une gestion flexible de la confidentialité : s'agissant des données individuelles, elle est souvent imposée par la loi ou la règlementation. Les règles d'accès doivent être conçues en conséquence. Il est possible que les personnes habilitées à « écrire » sur la blockchain – ou d'autres registres distribués – c'est-à-dire celles habilitées à la modifier et la mettre à jour, soient différentes de celles autorisées à la lire. La technologie, qui doit évoluer et se perfectionner, offre déjà une grande flexibilité d'adaptation ;
- Offrir un cadre de gouvernance et d'action collective entre partenaires qui veulent coopérer, mais dont aucun ne veut laisser le leadership aux autres. La blockchain peut servir de support à des projets de place.

Pour ces blockchains, ou registres distribués, fermés, on voit donc se développer aujourd'hui plusieurs voies prometteuses d'applications.

[49] Cette section s'inspire des travaux du CMBI (*The Potential Impact of Blockchain Technology on Finance: Small, Significant, or Completely Transformative*, en cours de publication) et de Lael Brainard, « *Cryptocurrencies, Digital Currencies, and Distributed Ledger Technologies: What Are We Learning?* », 15 mai 2018.

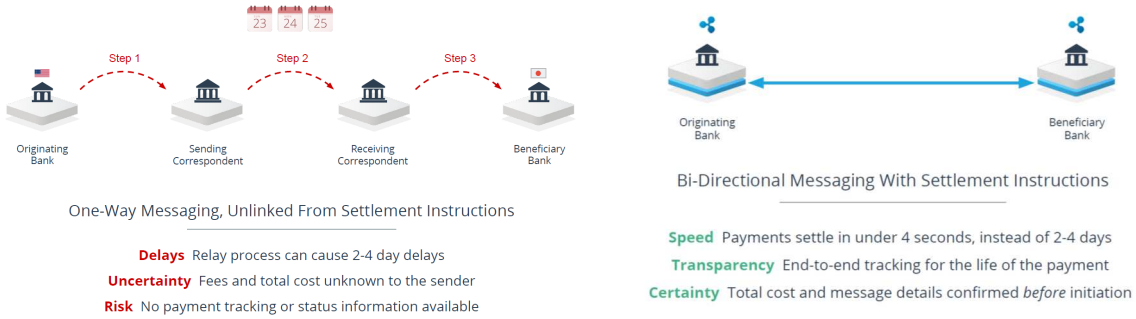
Là où les systèmes traditionnels sont peu efficaces ou peu compétitifs

C'est le cas des paiements transfrontières. Aujourd'hui encore, ces paiements empruntent le plus souvent des circuits complexes, mettant en jeu de nombreux intermédiaires et contreparties, y compris pour les opérations de change. Cette complexité accroît les coûts et multiplie les risques opérationnels. Comparées aux paiements domestiques, les transactions transfrontières restent longues et onéreuses pour les consommateurs, surtout pour les transferts de faibles montants.

Il est donc naturel qu'une fraction de ces paiements – transferts familiaux ou opérés par les migrants – s'effectue déjà par le biais des crypto-monnaies. Des systèmes de « *peer-to-peer* », opérant sans intermédiaire et pouvant fonctionner sur une infrastructure Internet existante, se révèlent très compétitifs.

Plusieurs développements sont en cours. Ripple est un protocole de paiement, décentralisé et semi-fermé, dont la technologie (DLT plus une forme allégée de la blockchain) et la propre crypto-monnaie (dénommée XRP) permettent la transmission très rapide de messages de paiement, dans toutes les monnaies (crypto ou officielles) entre toute localisation dans le monde. Ripple est de plus en plus utilisé, y compris par les banques internationales et systèmes de paiements.

Protocole de paiement offert par Ripple pour les transactions interbancaires



Source : Ripple, Transforming global payments*, avril 2018.*

La plateforme distribuée Corda, développée par le consortium R3, auquel participent des banques françaises, est gérée conjointement par un nombre limité de participants (avec des « validateurs » désignés). Elle rassemble 22 banques dans le double objectif de développer et de tester ses possibilités de paiements transfrontières en temps réel (*real time settlements*) et ce, grâce à l'interopérabilité des réseaux blockchains.

Ces évolutions ont poussé SWIFT, le système mondial de messagerie pour paiements interbancaires à développer son propre système le « *Global Payments Innovation Initiative* » (GPI). En cours de test avancé et de commercialisation auprès de 73 banques participantes, cette initiative propose une utilisation des fonds le jour même, une transparence et prévisibilité des frais, le suivi des paiements de bout en bout et un transfert d'informations de paiement plus riches. Le 24 mai 2018, SWIFT a annoncé qu'un quart des paiements transfrontières qui lui étaient confiés étaient désormais réalisés par l'intermédiaire de GPI, soit un peu plus de 100 milliards de dollars par jour et une moitié des paiements réalisés en moins de trente minutes. C'est un exemple extrêmement significatif des progrès qui peuvent être réalisés quand la technologie, se développant dans un environnement concurrentiel, suscite et impose l'innovation.

Là où la résilience aux cyber-attaques est importante

Le grand avantage des registres distribués est leur redondance naturelle. L'ensemble des données est disponible en plusieurs points du réseau. Ils permettent à un système de continuer à fonctionner quand certains de ses éléments sont compromis. Tous les systèmes de paiement et de règlements de gros montants ont besoin de cette robustesse. Elle est aujourd'hui assurée, pour les registres centralisés, par la duplication de tous les éléments essentiels. Une technologie DLT peut apporter des économies substantielles à cet égard.

Là où apparaissent des points de congestion opérationnelle

Les processus industriels et financiers sont des systèmes complexes, dont les acteurs sont nombreux et doivent se coordonner en permanence. Chaque étape peut nécessiter le recueil et la réconciliation de données avant de passer à l'étape suivante. Si des délais de transmission apparaissent, la congestion s'installe et les coûts augmentent. Disposer d'une base de données distribuée permettant de partager en temps réel une information constamment mise à jour procure des gains d'efficacité.

Toutes les opérations de règlement et de livraison de titres nécessitent de telles réconciliations, mobilisant séquentiellement plusieurs intervenants et s'avérant ainsi très coûteuses en ressources et en temps. Ces réconciliations peuvent durer plusieurs jours – retardant d'autant la certitude de la finalité de la transaction et générant un risque de contrepartie. Un registre distribué, actualisé en temps réel, permet aux acteurs de partager à tout instant une vue commune de l'état du système, ce qui accélère le processus et réduit les risques d'erreur[50].

Un champ d'application plus complexe, mais prometteur, paraît être la gestion des prêts aux entreprises ainsi que l'émission de titres par celles-ci. La documentation juridique, les flux d'intérêt, les procédures d'amendement et de réconciliation sont parfois encore opérées manuellement sur la base d'échanges d'informations par e-mail, avec de nombreuses réconciliations préalablement à tout paiement (Genève).

Le financement du commerce international (*trade finance*) sera significativement transformé par la blockchain. Il repose sur la coordination de nombreux intervenants (armateurs, autorités portuaires, compagnies d'assurances, banques, autorités douanières) qui, tous, jouent un rôle dans la chaîne de traitement et d'exécution d'une transaction transfrontière (import-export). Pour que la chaîne fonctionne, il faut que tous les acteurs puissent tout à la fois localiser les biens couverts et suivre leur évolution. Le partage en temps réel d'un même registre distribué entraînera d'immenses gains d'efficacité.

La même logique s'applique aux « *supply chains* » autour desquelles s'organisent l'internationalisation et la division de la production industrielle. Dans ces véritables « usines transfrontières » (Baldwin), la capacité (procurée par la blockchain) à suivre en temps réel les flux de produits et à coordonner par la même information l'action de centaines de sous-traitants est source de gains majeurs de productivité.

Un enregistrement daté et immuable des données et événements, notamment pour des raisons juridiques et de sécurité

Les progrès de la cryptographie permettent, dans ce cas, de préserver la confidentialité des données ainsi authentifiées, d'en réserver l'accès aux personnes autorisées et, surtout, de vérifier l'authenticité des informations sans prendre connaissance de leur contenu.

Des institutions financières s'apprêtent ainsi à rationaliser la gestion de leurs obligations administratives au regard de la lutte contre le blanchiment et le financement du terrorisme (*know your client* ou KYC). Les données individuelles et attestations certifiées stockées sur une blockchain pourront ainsi être « exportées » par leur titulaire à destination d'autres institutions, selon un processus assurant la confidentialité tout en préservant la certification. D'importantes simplifications et économies sont à attendre.

La même possibilité (partager en toute confidentialité des informations certifiées) peut permettre des améliorations majeures dans la gestion des dossiers individuels de santé. Chaque patient, pourrait conserver et actualiser, sous sa responsabilité, son dossier individuel sur un blockchain, avec les informations certifiées par les médecins ordonnateurs. Ce dossier pourrait être communiqué aisément, au moyen de clés cryptographiques, en totalité ou en partie, à ceux des professionnels de santé pour lesquels il serait nécessaire dans le respect du secret médical, garanti par la cryptographie.

D'autres usages émergent pour tirer parti du double avantage de la confidentialité et de l'authenticité des données qu'offre un registre distribué. En effet, alors que l'usurpation d'identité – numérique ou bancaire – est un mal endémique, la blockchain permet de :

- se prémunir contre la falsification de l'état civil, des titres de propriété (cadastre), des droits d'auteurs et de certificats divers ;
- suivre les transactions liés au transfert de ces droits, afin d'en établir la propriété en temps réel ;
- s'assurer de la parfaite identification des auteurs à l'origine de ces transactions.

Enfin, les blockchains les plus récentes supportent l'exécution de « smart contracts »

On désigne par « *smart contracts* » la version « blockchain » d'applications déjà anciennes, dans lesquelles un algorithme exécute automatiquement des opérations entre personnes différentes à la réception d'informations spécifiées (les « oracles »). Dans les blockchains associées à des monnaies, ces *smart contracts* opèrent des transferts d'unités de valeur entre les participants.

Les smart contracts ne sont généralement pas des contrats, au sens juridique du terme, mais l'application par protocole et par algorithmes de conventions conclues entre les participants.

L'intérêt des *smart contracts* vient de ce qu'ils ne nécessitent l'intervention d'aucune tierce partie. L'exécution s'opère sur la blockchain dès que les conditions sont réalisées. Il faut toutefois qu'il n'existe aucune ambigüité sur l'interprétation de ces conditions et qu'aucun jugement humain ne soit nécessaire préalablement à l'exécution du contrat.

Sous ces limites, les *smart contracts* peuvent connaître des applications nombreuses, notamment dans le secteur financier (gestion du collatéral, appels de marges, paiements d'intérêts, etc.). Il est possible que les clauses d'exécution de nombreux contrats dérivés (en tout cas les plus standardisés) soient insérées, à l'avenir, dans des *smart contracts*.

2. La digitalisation de la valeur

Au-delà de la blockchain, les crypto-monnaies annoncent une autre innovation, moins publiquement soulignée, mais plus importante encore : la digitalisation de la valeur et des actifs. La technologie offre la capacité de représenter numériquement de la valeur et à la transférer en toute sécurité entre individus sans aucun intermédiaire – constituant ainsi une sorte de « billet de banque » digital. Les représentations digitales de valeur sont couramment appelées des « jetons » ou plus fréquemment encore, par leur nom anglais, des « *tokens* ». La cryptographie moderne permet, le cas échéant, de faire cette opération de manière anonyme. On peut donc créer des monnaies et des actifs financiers digitaux « au porteur ».

[50] Lael Brainard, « *Cryptocurrencies, Digital Currencies, and Distributed Ledger Technologies: What Are We Learning?* », 15 mai 2018.

Les potentialités et les risques de la digitalisation de la valeur

Les applications sont multiples. Les crypto-monnaies, qui sont des « tokens » monétaires, sont l'exemple le plus connu. Mais tout actif, réel ou financier, peut potentiellement être digitalisé. La *tokenisation* pourrait s'avérer particulièrement prometteuse pour les actifs rares et peu liquides, dont la valorisation est pénalisée par la faible profondeur de marché dans des proportions importantes. Sont notamment concernés l'immobilier commercial et résidentiel, le *private equity* ou bien encore les œuvres d'art. Dans ce cas d'espèce, des particuliers seront en mesure d'acquérir collectivement un tableau de valeur grâce à l'achat de *tokens*, bien qu'aucun d'entre eux ne soit individuellement en mesure d'acheter seul ce tableau.

Selon une étude du Nasdaq[51], la digitalisation s'appliquerait particulièrement bien à deux grandes catégories d'actifs :

- les actifs incorporels, que sont notamment les brevets, les droits carbone ou bien encore les droits d'auteur. Compte tenu de leur absence d'existence physique, ces actifs apparaissent plus faciles à convertir en *tokens*, bien que les différences de juridictions puissent rendre leurs transferts ultérieurs difficiles ;
- les actifs fongibles, susceptibles de se prêter plus facilement au processus de tokenisation, dans la double mesure où ils peuvent le plus souvent être divisés en plusieurs unités et où l'ensemble des *tokens* peuvent ensuite être associés à un ensemble général de composants d'actifs interchangeables (par exemple, dix kilos d'or).

En convertissant en tokens des actifs rares ou faiblement liquides, la digitalisation ouvrira les marchés correspondants à davantage d'investisseurs et accroîtra le volume global d'échanges. Le développement de la « *tokenisation* » est parfois présenté comme inéluctable, un mouvement dans lequel Internet a vocation à devenir à terme le plus grand marché d'actifs du monde, aussi sûrement qu'Internet est devenu la plus grande bibliothèque du monde. La digitalisation des actifs sous forme de jetons ne fait que prolonger la digitalisation de l'information permise par Internet.

Les risques, bien évidemment, sont à la hauteur des opportunités que présentent ces formes de « titrisation digitale ». Ils apparaissent à deux niveaux :

- Celui de la gouvernance et de la sécurité juridique : attacher (et faire respecter) des droits définis dans des législations nationales à des actifs immatériels circulant sur Internet est un défi non résolu. Ceci d'autant plus que, théoriquement, plusieurs types de droits peuvent être attachés et transférés aux jetons : doits d'usage et non de propriété, comme dans le cas des baux, droits incorporels, comme les droits musicaux. L'exercice des droits inscrits sur un jeton suppose d'en connaître le détenteur effectif, de manière formelle et inconstatable. C'est possible sur une blockchain mais plus complexe dans d'autres cas. En l'absence de cadre juridique et de règles de gouvernance, tous les abus sont aujourd'hui possibles et probables ;
- Celui de la stabilité financière : en émettant des jetons échangeables en contrepartie d'actifs illiquides, on procède en fait à une activité de transformation, dont les risques sont bien identifiés et connus. En particulier, les jetons liquides sont exposés à des « *runs* », dans lesquels la perte subite de confiance conduit à un afflux de demandes de conversion en actifs sous-jacents illiquides qui ne peut être satisfait. Les crypto monnaies adossées à des actifs physiques ou financiers, dont la création est envisagée par de nombreux entrepreneurs, sont particulièrement exposées à ce risque.

[51] Addison Cameron-Huff, *How Tokenization Is Putting Real-World Assets on Blockchains*, 30 mars 2017.

Les ICO, reflet des ambiguïtés de la digitalisation de la valeur

Les ICO (*Initial Coin Offerings*) reflètent parfaitement les opportunités et les ambigüités de la digitalisation des actifs. Cette pratique de levée de fonds sur Internet – apparue en 2016- est en développement rapide dans un environnement de liquidité abondante. Elle cumule deux grandes novations par rapport aux émissions traditionnelles :

- la procédure d'appel à l'épargne : La procédure des ICO reproduit, dans ses principales étapes, celle des émissions d'actions, mais sans aucune des formalités et garanties dont s'accompagne celle-ci. Il n'y a pas de prospectus visé par les autorités boursières, mais simplement un document (le « *White Paper* ») posté sur Internet, qui n'engage pas juridiquement l'émetteur – lequel parfois n'est même pas établi en tant que société – et n'est pas standardisé. Ce mode d'émission préfigure sans doute l'avenir mais n'offre aujourd'hui aucune garantie réelle aux souscripteurs ;
- la nature très variée des droits que confèrent les « jetons » émis : beaucoup d'acteurs privés et publics tentent aujourd'hui de promouvoir une classification entre jetons dits « financiers » et jetons dits « d'utilité ». En réalité, ces jetons d'utilité sont très ambigus. Il est probable que dans plus de trois-quarts des cas, l'émission de tels jetons est en réalité celle d'une nouvelle crypto-monnaie destinée au paiement de services qui n'existent pas encore, dont l'apparition est subordonnée au succès du projet et dont le prix futur est inconnu. Ce sont donc des produits particulièrement risqués, qui cumulent plusieurs niveaux d'aléas, mais dont la plupart sont néanmoins « cotés » sur des plateformes d'échange.

Les ICO ont connu un succès croissant à compter de l'été 2017 : le montant total des levées de fonds par ICO dans le monde a représenté entre 4 et 6 milliards de dollars en 2017 (les sommes levées se concentrant principalement sur les derniers mois de l'année), contre 100 millions de dollars en 2016. Par comparaison, l'investissement réalisé par les fonds de capital-risque dans le premier tour de financement de start-ups a représenté, à l'échelle mondiale, 13 milliards de dollars en 2017.

Tableau 1 : Baromètre des ICO en France et dans le monde au 31 décembre 2017

ICO	Monde[52]	France[53]	France (en % du monde)
Nombre	372	16	4,30
Montants levés à l'émission (en milliards de dollars)	4,00	0,13	3,25

Source : Mission.

Les volumes émis par ICO ont continué d'augmenter depuis le début de l'année 2018, le total des fonds levés entre le 1er janvier et le 1er juin s'élevant à 9,5 milliards de dollars[54], soit près de 2 milliards de dollars par mois.

Au total, les émissions de *tokens* se répartissent assez également entre l'Amérique du Nord, l'Europe et l'Asie[55], avec toutefois un pays dominant : la Suisse, où 25 % des ICO mondiales ont été réalisées. Le canton de Zoug, a été surnommé la « *Crypto Valley* » par sa position de « *hub* » de référence dans le monde sur les crypto-monnaies. De son côté, l'Asie compte plusieurs pays particulièrement dynamiques, tels que la Corée du Sud, Singapour, le Japon, la Chine et Hong-Kong.

[52] EY research, *Initial coin offerings (ICOs)*, décembre 2017.
[53] Avolta Partners, *Baromètre des ICO en France*, juin 2018.
[54] Chain Tech et France digitale, *Towards a regulatory framework on crypto-assets*, juin 2018.
[55] Voir visuellement la répartition géographique des montants levés en ICO : https://elementus.io/blog/token-sales-visualization.

Encadré 3 : Panorama des ICO réalisées en France entre 2014 et 2018

On estime aujourd'hui à 16 le nombre d'ICO domiciliées en France et possédant une équipe française, à la date du 1er juin 20016. Le montant total des fonds levés à l'émission s'élève à 130 millions de dollars, aujourd'hui valorisés à 340 millions de dollars sur le marché. Le montant moyen d'une ICO française s'établit ainsi à 8,1 millions de dollars à l'émission et à 21,4 millions de dollars une fois prise en compte la valorisation de marché. Par comparaison, la plus grosse ICO réalisée et connue à ce jour à l'étranger, en l'espèce Telegram, a permis de lever 850 millions de dollars.

Sur ces 16 ICO domiciliées en France, la détention des jetons émis est très concentrée, puisque deux tiers des jetons offerts sont détenus par dix souscripteurs seulement. Il convient à cet égard de souligner qu'en moyenne seuls deux tiers des jetons sont offerts à l'émission, le reste demeurant en réserve.

Les jetons émis sont à 70 % des jetons d'utilité ou « *utility tokens* », contre 25 % pour des jetons de titre ou « *security tokens* ». Les jetons émis le sont également dans plus de la moitié des cas (56 %) sur une blockchain hydride, contre un quart sur une blockchain publique et un peu plus de 6 % sur une blockchain privée.

La liquidité des jetons émis par ICO est aujourd'hui relativement faible, puisque le volume de *tokens* échangés sur le mois de mai 2018 ne représente, en moyenne quotidienne pondérée, que 0,6 % du nombre total de *tokens* en circulation. Le ratio de liquidité varie toutefois très fortement d'un jeton à l'autre, puisqu'il va de 0,1 % à 8,91 %.

Peu liquides, les jetons émis voient également leur prix être particulièrement volatiles. En effet, le multiple de volatilité, mesuré par le rapport entre le prix maximal et le prix minimal, s'établit en moyenne à 6,6 et varie très fortement (allant de 0,2 à 285), attestant de la non-maturité du marché.

Source : Mission, d'après une étude réalisée par Avolta Partners.

Les technologies qui sous-tendent les ICO sont encore dans une phase d'apprentissage, et les acteurs et projets sont souvent éphémères. Selon une étude de l'Académie chinoise des technologies de l'information et de la communication (CAICT) rendue publique le 28 mai 2018, sur les 80 000 projets « blockchain » lancés dans le monde, seuls 8 % d'entre eux sont encore actifs à ce jour, les start-ups développant de tels projets ayant une durée vie moyenne de 450 jours, soit 1,25 année. Sur les 902 start-ups ayant lancé une ICO en 2017, 46 % d'entre elles ont d'ores et déjà disparu, selon une étude réalisée par le site Bitcoin.com. Le fondateur d'Ethereum, M. Vitalik Buterin, a publiquement reconnu que neuf start-ups sur dix émettant des *tokens* sont vouées à l'échec.

Les Jeux olympiques de 2024, terrain d'expérimentation de la digitalisation de la valeur

Si la digitalisation de la valeur pose des défis importants aux régulateurs, elle est avant tout porteuse d'opportunités majeures pour la sphère économique, mais également pour la sphère publique. Mieux appréhender et, le cas échéant, réguler les applications dont les crypto-monnaies sont porteuses, exigent des entités publiques qu'elles soient elles-mêmes en capacité d'anticiper et de s'approprier les développements technologiques à venir. Si les administrations et les régulateurs ont d'ores et déjà investi dans les technologies liées la blockchain (notamment la Caisse des dépôts et consignations ainsi que la Banque de France), elles peinent à en appréhender toutes les potentialisés, en particulier celles liées à la digitalisation de la valeur.

De simples investisseurs dans la blockchain, les autorités publiques doivent prendre le leadership et se muer en véritables développeurs de nouvelles applications permises par la blockchain, telles que la digitalisation de l'accès à un service donné. En effet, développer de telles applications offrira aux acteurs publics la possibilité d'incuber les évolutions technologiques les plus récentes et de mieux en appréhender les risques et les opportunités.

Des expérimentations peuvent, à cet égard, être envisagées à brève échéance. Ainsi, sous réserve de leur engagement ou de leur participation à la réalisation d'un service public, les usagers pourraient se voir distribuer en retour des *tokens* qu'ils pourraient échanger contre l'accès à un autre service. Parce que l'amélioration de la propreté dans les grandes villes passe par l'engagement de ses habitants, ceux-ci pourraient par exemple, en contrepartie de la réalisation d'opérations volontaires de nettoyage, se voir rétribuer par l'octroi de *tokens* qu'ils pourraient ensuite convertir pour accéder à une offre de vélos ou de voitures en libre-service.

Afin de toucher un public plus large, les autorités publiques pourraient s'engager à digitaliser une partie de la billetterie des Jeux olympiques organisés par la France en 2024. Les *tokens* donnant accès à cette cérémonie seraient émis sur une blockchain au bénéfice des personnes ayant contribué à la préparation et à l'organisation d'événements populaires autour des jeux. Ces *tokens* pourraient être ensuite échangés de manière transparente sur cette même blockchain, sécurisant ainsi les transactions et réduisant d'autant les risques liés à la revente au marché noir, à la contrefaçon ainsi qu'à la fraude.

B. Un écosystème dynamique

Le développement des crypto-monnaies s'accompagne de la constitution d'une chaîne de valeur avec plusieurs catégories d'acteurs : les mineurs, les *wallet providers* et autres fournisseurs de services ainsi que les start-up technologiques (souvent financées à l'aide d'ICO). Ce paysage n'est toutefois pas figé, ni dans la délimitation de ces activités, ni surtout dans leur localisation. S'appuyant sur une technologie décentralisée et distribuée, les acteurs de l'écosystème de la crypto-finance sont particulièrement mobiles, n'hésitant pas à transférer leur activité au gré des évolutions réglementaires notamment.

Graphique 1 : Chaîne de valeur des acteurs de la crypto-finance

Source : Mission.

Les mineurs

Les mineurs occupent une place centrale dans l'émission et la gestion des crypto-monnaies. Ce sont, en effet, les mineurs qui valident les transactions et qui sont donc à l'origine de la création monétaire. En théorie, chacun peut devenir mineur en mettant à la disposition du réseau la puissance de calcul de son ordinateur. L'hébergement à distance et les services de minage par le biais du « *cloud* » ont également émergé, offrant la possibilité aux particuliers de contribuer à la procédure de minage sans avoir à faire fonctionner l'équipement eux-mêmes.

En réalité, le secteur du minage a rapidement évolué d'une activité de loisir effectuée sur des ordinateurs personnels à une industrie professionnelle et très capitalistique avec ses propres sous-traitants :

- l'activité de minage a généré, en 2017, un chiffre d'affaires de deux milliards de dollars sans compter la vente de matériel de minage ;

- le minage est de plus en plus organisé en « *pools* », formels ou informels, qui mettent en commun leur puissance de calcul et se partagent les profits. Ces *pools* de minage sont de plus en plus professionnalisés et offrent, entres autres, des services après-vente à leurs utilisateurs ;
- les *pools* de minage sont localisés, à près de 60 % en Chine[56], suivie par les États-Unis qui en accueillent 15 % de son côté. Au premier trimestre 2018, quatre *pools* chinois concentrent à eux seuls 52 % de la puissance de minage Bitcoin[57], créant ainsi la possibilité (théorique) d'une attaque du réseau ;

Les plateformes

L'échange de crypto-monnaies contre des monnaies avec cours légal ou d'autres crypto-monnaies s'est accompagné d'une diversification des infrastructures de marché. En effet, les plateformes d'échange permettant l'achat et la vente de crypto-monnaies sont essentielles à leur fonctionnement.

Elles assurent une grande part des transactions en crypto-monnaies ainsi que la conversion de celles-ci en monnaies avec cours légal (et réciproquement). Elles constituent à ce titre l'interface principale entre l'univers de la crypto-finance et le système financier traditionnel. Les plateformes présentent donc un caractère « systémique » à plusieurs titres : comme infrastructures de marché et comme systèmes de paiement, c'est par leur intermédiaire que se diffusent à l'économie réelle les perturbations et dysfonctionnements éventuels de la sphère des crypto-monnaies. La plupart des failles de sécurité et des cyber-attaques ont également lieu sur les plateformes d'échange.

Une population nombreuse, mobile et changeante[58]

Entre 130 et 180 plateformes[59] sont aujourd'hui actives dans le monde. Elles sont très concentrées géographiquement : en juin 2018, Hong-Kong, Malte, les États-Unis, le Royaume-Uni, Singapour et le Japon assurent 92 % des volumes d'échanges. Mais l'activé de ces plateformes est particulièrement mobile, comme en atteste l'évolution très rapide de la hiérarchie entre les cinq principaux pays en fonction des volumes d'échanges journaliers.

Tableau 2 : Classement des cinq principaux pays en fonction des volumes d'échanges journaliers sur les plateformes de crypto-monnaies

Mars 2018	Juin 2018
1. Hong Kong (31 %)	1. Hong Kong (30 %)
2. États-Unis (29 %)	2. Malte (26 %)
3. Corée du Sud (15 %)	3. États-Unis (11 %)
4. Royaume-Uni (14 %)	4. Royaume-Uni (11 %)
5. Japon (5 %)	5. Singapour (10 %)

Source : Mission, d'après JP Morgan, mai 2018, et cryptocoincharts, juin 2018.

Toutefois, deux pays relativement modestes en taille – Malte et Belize[60] – accueillent respectivement les deux plus grosses plateformes d'échanges de crypto-monnaies en termes de volumes, à savoir Binance[61] et OKEx. À titre de comparaison, la France ne compte pour l'instant qu'une seule plateforme, sur laquelle s'échangent chaque jour 60 000 euros en crypto-monnaies (soit 0,001 % du volume total).

[56] Selon une étude de Bloomberg de décembre 2017 (CITER LA REFERENCE)
[57] BCG, *Livre blanc sur la blockchain pour les entreprises*, 2017.
[58] Source : https://cryptocoincharts.info/markets/info
[59] En fonction des sources
[60] Belize est le 1er pays au monde en volumes échangés, mais le 24e pays au monde en nombre de plateformes d'échange de crypto-monnaies présentes dans sa juridiction, car ce pays accueille peu de plateformes, mais parmi les plus importantes au monde.
[61] Binance a transféré son siège du Japon à Malte en mars 2018.

Le secteur des plateformes connaît, en outre, une mortalité élevée : depuis l'avènement du Bitcoin, 45 % des plateformes d'échanges créées et opérant dans cette crypto-monnaie ont cessé leur activité. La moitié des disparitions de ces plateformes est liée au piratage : tandis que la fermeture de plateformes de grande taille est généralement due à des problèmes de sécurité, celle des plateformes de taille modeste est essentiellement liée à une absence d'activité. Au total, 46 % des plateformes des plateformes ayant disparu n'ont jamais remboursé les clients qui y avaient déposés des fonds.

Des fonctions très diversifiées et inégalement développées selon les plateformes

Les plateformes peuvent offrir l'un ou plusieurs des services suivants :

- la cotation et l'échange de crypto-monnaies contre des monnaies officielles ;
- le dépôt et la conservation des avoirs en crypto-monnaies de leurs clients ;
- le dépôt et la conservation des mêmes avoirs en monnaies officielles ;
- l'exécution de paiements et de transactions en crypto-monnaies (activité de paiement, d'intermédiaire et d'infrastructure de marché).

Il existe un grand nombre de combinaisons variables et changeantes entre ces diverses fonctions, dont les délimitations ne sont pas toujours claires et les supports technologiques variés.

Dans l'exécution des transactions et des opérations de change, certaines plateformes se bornent à opérer un système en ligne (« *online* ») qui organise la rencontre directe des offreurs et demandeurs. D'autres jouent un rôle plus complet de teneur de marché : elles tiennent un « *order book* », rapprochent les offres et demandes et déterminent un prix. Dans cette activité, l'intégrité du processus est essentielle pour la protection des intervenants. L'évolution récente semble favoriser, au moins pour les petites plateformes, la première forme d'activité, physiquement moins « localisée » et nécessitant moins d'investissement initial. Certaines plateformes fournissent également des données statistiques (comme les montants échangés ou la volatilité des cours).

Pour les plateformes les plus importantes, la fonction de conservation et de tenue de compte (en crypto-monnaies et en monnaies officielles) apparaît centrale. En effet, 73 % des plateformes d'échange sont habilitées à prendre possession des fonds de leurs utilisateurs, qui laissent le contrôle de leurs clés privées à 23 % d'entre elles[62]. Dans un cas au moins, ces activités se combinent à l'émission d'une crypto-monnaie : la plateforme Bitfinex émet ainsi la crypto-monnaie Tether. Ces plateformes s'apparentent d'assez près à des systèmes de paiement, voire à des « banques ». Une fraction importante (mais non connue) des transactions en crypto-monnaies s'effectue ainsi par virement de compte à compte au sein du bilan des plateformes et n'apparaissent jamais sur la blockchain, ce qui conduit à la fois à surestimer la concentration des avoirs en crypto-monnaies parmi leurs détenteurs et à sous-estimer les volumes de transactions.

Ces activités pseudo-bancaires ne sont pas exemptes de risques. En l'absence de publication des bilans, il est impossible d'apprécier les risques financiers localisés dans les plateformes non régulées. Il est également impossible, d'une part, de savoir si celles-ci entretiennent des comptes réciproques (avec le risque de contrepartie qui s'y attache) et, d'autre part, de vérifier que tous les dépôts conservés au nom de leurs clients ont bien une contrepartie exacte sur la blockchain (pour les comptes en crypto-monnaies) ou dans le système bancaire officiel (pour les comptes en monnaies avec cours légal). Si tel n'était pas le cas, les plateformes se livreraient de fait à une activité de crédit bancaire avec les risques de transformation et de solvabilité qui l'accompagnent.

[62] Garrick Hileman et Michel Rauchs, *Global Cryptocurrency benchmarking study*, Cambridge Center for Alternative Finance, 2017.

Un secteur inégalement régulé

Entre 30 et 50 % des plateformes détiennent une licence officielle d'exploitation dans leur pays d'établissement[63]. Les proportions sont très variables selon les régions : 85 % des plateformes implantées en Asie-Pacifique ne détiennent pas de licence, tandis que 78 % des plateformes ayant leur siège en Amérique du nord détiennent une licence gouvernementale officielle ou une autorisation. En Europe et en Amérique latine, ce pourcentage est de respectivement 47 % et 43 %. Bien que non soumises à une licence officielle, les plateformes localisées en Chine semblent étroitement surveillées par les autorités.

Une concurrence réglementaire intense s'exerce entre les pays et ce, au bénéfice des plateformes elles-mêmes, qui migrent des pays les plus régulés vers ceux qui le sont moins. Ainsi, la plateforme Binance, initialement basée au Japon, a transféré son activité à Malte en mars 2018, après un refus d'agrément des autorités japonaises.

Le principal lieu de piratage

Beaucoup d'utilisateurs confient aux plateformes leurs clés privées, leur déléguant ainsi la gestion de leur adresse et les mouvements de fonds. Ces clés privées sont stockées soit dans un fichier accessible sur Internet (« *hot storage* »), soit sur un périphérique isolé (« *cold storage* »). Le premier est évidemment très vulnérable au piratage, tandis que 92 % des plateformes d'échange déclarent utiliser un système de « *cold storage* ».

Les plateformes sont confrontées à un nombre élevé et croissant de fraudes. Depuis 2011, 19 incidents graves ont été recensés pour un montant estimé des pertes s'élevant à 1,2 milliards de dollars. Les causes de ces incidents sont multiples. La plus courante vient de la falsification des clés privées, suivie par l'introduction de logiciels malveillants. Le hack de la plateforme Coincheck au Japon, en janvier 2018, pour une perte totale estimée à 530 millions de dollars illustre la faiblesse de la protection du système de « *hot storage* ».

Deux incidents suivants peuvent être considérés comme emblématiques au sein de la sphère crypto[64] : les hacks successifs de Mt Gox (2011 puis 2014) ayant conduit à la perte d'environ 4870 millions de dollars[65] et le hack de Coincheck (2018) ayant conduit à la perte d'environ 530 millions de dollars.

Encadré 4 : Historique des principales cyber-attaques et sur le marché des crypto-monnaies depuis 2014

- Titanium : 21 millions de dollars (avril 2018) ;
- LoppX : 4,5 millions de dollars (février 2018) ;
- Coincheck : 530 millions de dollars (janvier 2018) ;
- PlexCoin : 15 millions de dollars (décembre 2017) ;
- Bitfinex : 72 millions de dollars (août 2016) ;
- Bitstamp : 5,2 millions de dollars (janvier 2015) ;
- Mt. Gox : 487 millions de dollars (février 2014).

Source : Morgan Stanley.

[63] Garrick Hileman et Michel Rauchs, *Global Cryptocurrency benchmarking study*, Cambridge Center for Alternative Finance, 2017.
[64] Voir annexe n° X pour davantage de détail.
[65] Abrams, Matthew et Tabuchi, 2014.

La spécialisation des plateformes à des fins frauduleuse : l'exemple de la Silk road

En février 2011, le pseudonyme « *Dread Pirate Roberts* » a lancé la Silk Road, une place de marché sur Internet permettant aux utilisateurs d'acheter et de vendre des biens ou services illicites avec ou contre du Bitcoin. Ces transactions étaient notamment liées au trafic de stupéfiants. En octobre 2013, le FBI a arrêté Ross William Ulbricht, soupçonné d'être le « *Dread Pirate Roberts* », entraînant la fermeture de la *Silk Road*. Environ 15 millions de dollars ont été saisis durant cette procédure.

Peu de transparence et des risques notables pour l'intégrité des marchés

De manière générale, les utilisateurs de plateformes ne bénéficient d'aucune des garanties qui s'attachent aux marches régulés : les cotations ne sont pas transparentes et aucune règle n'encadre le traitement des transactions. Sur le Bitcoin, plusieurs études[66] documentent l'existence de transactions suspectes s'apparentant à des manipulations directes de cours[67] ou de pratiques d'investisseurs informés, de type « *frontrunning* »[68].

À titre d'exemple, beaucoup de rumeurs, bien qu'ayant été constamment démenties par les responsables de Tether, ont affecté cette crypto-monnaie, qui présente la particularité d'être adossée à 100 % sur des réserves en dollars et de permettre ainsi aux plateformes d'effectuer des transactions adossées à la devise américaine. Les rumeurs sont d'une double nature : l'adossement de Tether au dollar ne serait pas intégral et cette crypto-monnaie serait émise périodiquement pour financer des achats de soutien des cours du Bitcoin. Une étude récente[69], elle-même contestée, souligne la causalité statistique entre les flux de transactions sur Ether et la variation des cours du Bitcoin. Il est certain que le rassemblement, entre les mains des mêmes personnes, de la propriété d'une plateforme et de la gestion d'une crypto-monnaie n'offre pas toutes les garanties institutionnelles souhaitables.

Les « wallet providers »

Dans le sillage des activités de plateformes d'échange se multiplient des prestations de services en matière de conservation des crypto-monnaies, assimilables à des activités de dépositaires. Certains prestataires, dénommés « *wallet providers* », proposent, en effet, un service de conservation pour compte de tiers des clés privées permettant d'accéder aux crypto-monnaies, de les stocker et de les transférer de manière sécurisée. Ces clés privées sont conservées soit au sein de portefeuilles connectés à Internet (ou « *hot wallet* »), soit au sein de portefeuilles physiques (ou « *cold wallet* »).

Encadré n° 5 : Clés publiques *versus* clés privées

La détention des crypto-monnaies sur la blockchain se caractérise par la connaissance de deux clés cryptographiques :

- l'une publique, qui est accessible à tous et permet d'identifier les différents portefeuilles sur lesquels les crypto-monnaies ont été transférées (mais pas leurs propriétaires qui ne sont pas identifiés) ;
- l'autre privée, qui permet au détenteur du portefeuille sur lequel sont inscrites les unités de crypto-monnaies, de les utiliser et de les transférer vers un autre portefeuille.

Les *wallets* contiennent également une interface permettant à l'utilisateur de suivre le solde de ses avoirs en crypto-monnaies et proposent, pour une majorité d'entre eux, des fonctionnalités et services additionnels, qui dépassent le simple stockage. Le service d'échange en crypto-monnaies intégré est la fonctionnalité la plus populaire : elle permet aux utilisateurs de s'échanger des crypto-monnaies par une interface unique. 52 % des *wallets* fournissent un service intégré de change, ce qui souligne le fait que la frontière entre les *wallets* et les plateformes d'échange est de plus en plus floue.

La plupart des *wallets providers* ont pour objectif d'étendre le champ des services qu'ils offrent, et d'ajouter davantage de fonctionnalités dans un futur proche (par exemple, automatisation de l'offre de frais de transactions en fonction du volume en cours sur le réseau et de l'urgence du paiement).

À ce jour, 42 % des *wallet providers* sont en Europe (dont beaucoup au Royaume Uni), 39 % en Amérique du nord et 19 % en l'Asie-Pacifique[70]. Le nombre total de *wallets* a été multiplié par quatre de 2013 à 2016, passant de 8,2 à 35 millions.

Les services annexes

Autour des échanges de crypto-monnaies, se développent des services d'information financière et de fournitures de données, de conseil en investissement ou encore de *trading*. Se déploient aussi des distributeurs physiques de crypto-monnaies, semblables à des distributeurs automatiques de billets : ils sont situés aux trois-quarts en Amérique du Nord, tandis que l'Europe[71] n'en accueille que 20 % et l'Asie 2 % seulement.

L'écosystème français de la crypto-finance

L'écosystème français en matière de crypto monnaies et de services associés est particulièrement dynamique. Si la France compte peu de plateformes d'échange et si les ICO y demeurent encore relativement faibles tant en nombre qu'en montant, la France a su faire émerger des entreprises en pointe, notamment en matière de conservation de crypto-monnaies, la société Ledger née à Vierzon et spécialisée dans la production de « *cold wallets* » pouvant prétendre au rang de potentielle Licorne.

En outre, de nombreux projets d'applications décentralisées reposant sur la blockchain et les crypto-monnaies ont émergé en France, attestant du dynamisme de son écosystème, porté par de multiples start-ups de renom. Les levées de fonds réalisées par ces nouvelles sociétés telles que Ledger (75 millions de dollars), Centrifuge (3,8 millions de dollars), iEx.ec (12,5 millions de dollars) ou encore Stratumn (7,8 millions de dollars) en sont une parfaite illustration.

S'il est encore difficile d'avoir une vision précise de cet écosystème naissant, il existe toutefois quelques indicateurs éclairants. La Chaintech a notamment regroupé 400 acteurs français lors de sa consultation publiée le 11 juin 2018 sur les crypto-monnaies, parmi les plus significatifs figurent NeuroChain, Consensys, Paymium, Ark, Blockchain Partners, Coinhouse, iEx.ec, Legder ou encore Moneytrack.

Les projets développés en France sont également porteurs de nouveaux emplois sur le territoire : le nombre d'emplois créé par l'écosystème français de la crypto-finance a été multiplié par dix entre 2016 et 2017, passant ainsi d'environ 15 à près de 160. Ces emplois concernent majoritairement le secteur des télécommunications (58 %, notamment Atos, Orange et Safran) et le secteur de la finance (20 %, notamment Natixis, la Banque de France et la Société Générale).

Les emplois créés dans ces différents secteurs sont principalement à ce jour des offres de stages (58 %, contre 36 % de contrats à durée indéterminée) et sont, dans tous les cas, quasi-exclusivement destinés à des profils techniques spécialisés : développeurs, architectes, etc. Les grandes entreprises de l'économie conventionnelle cherchent également à développer des équipes (de 5 à 15 personnes) dédiées aux crypto monnaies et aux applications qui leur sont liées.

---

[66] Price Manipulation in the Bitcoin Ecosystem, Gandal & al, May 2017 / Bitcoin and cryptocurrency technologies, Narayanan & al, February 2016.

[67] En 2013, le cours du bitcoin a fortement augmenté avant le piratage de la plateforme Mt Gox.

[68] Le « *frontrunning* » est une technique boursière permettant à un courtier d'utiliser un ordre transmis par ses clients afin de s'enrichir. La technique consiste à profiter des décalages de cours engendrés par les ordres importants passés par les clients du broker (courtier).

[69] John M. Griffin et Amin Shams, *Is Bitcoin Really Un-Tethered ?*, Université du Texas, 13 juin 2018).

[70] Garrick Hileman et Michel Rauchs, *Global Cryptocurrency benchmarking study*, Cambridge Center for Alternative Finance, 2017.

[71] La France ne compte que deux distributeurs physiques de Bitcoin sur les 3 239 recensés dans le monde, à la date du 12 juin 2018, soit 0,0006 % des ATM de Bitcoin.

La France dispose à cet égard d'ingénieurs et de mathématiciens de haut niveau, lui conférant des avantages comparatifs notables dans la course au développement de technologies de rupture. Le bon fonctionnement de la blockchain et de ses applications repose sur la recherche cryptographique et l'ingénierie, qui exigent des compétences mathématiques et informatiques, domaines de recherche dans lesquels la France a une position de leader.

L'environnement financier français est également favorable au développement de cet écosystème. La politique volontariste engagée depuis plusieurs années permet ainsi aux jeunes entreprises innovantes d'accéder à une gamme complète de financements de haut et de bas de bilan, gamme qui est notamment portée par BPI France et le plan d'investissement d'avenir (PIA).

C. Des risques circonscrits qui doivent le rester

Un faible risque pour la stabilité financière globale

À ce stade, les risques pour la stabilité financière ne paraissent pas avérés, ainsi que l'a confirmé le rapport du FMI sur la stabilité financière dans le monde, publié le 9 avril 2018. Le FMI note toutefois que « *si leur utilisation des monnaies virtuelles devait se généraliser en l'absence de garde-fous satisfaisants, la donne pourrait changer* ». Plusieurs facteurs permettent d'affirmer que le risque que les crypto-monnaies font peser sur la stabilité financière globale est aujourd'hui faible.

Les sommes en cause restent peu importantes

La valeur de capitalisation des crypto-monnaies est actuellement relativement faible comparativement au poids du système financier global : avec 432 milliards de dollars au 22 février 2018, ces instruments représentent 1,5 % seulement de la capitalisation de marché de l'indice S&P500 et 5,5 % de la valeur total du marché de l'or. Les crypto-monnaies ont également une taille de marché bien inférieure à celles des récentes bulles spéculatives[72].

L'exposition du secteur financier traditionnel reste limitée à ce stade

Les crypto-monnaies ne présentent pas de risque systématique du point de vue de la stabilité financière globale, compte tenu de leur intégration encore limitée à ce jour au système financier traditionnel ainsi que dans les produits financiers existants (ETF, dérivés, *futures*).

L'exposition des institutions et acteurs financiers traditionnels aux risques liés aux crypto-monnaies pourrait prendre plusieurs formes :

- la détention directe de crypto-monnaies par les institutions financières, soit au titre d'opérations en comptes propres, soit dans le cadre de la conservation de crypto-actifs pour comptes de tiers ;
- l'octroi de crédit et de facilités financières aux plateformes d'échanges et aux *wallet providers* pour financer la croissance de leurs activités ;
- l'octroi de crédits aux entreprises acceptant les crypto-monnaies comme moyen de paiement ainsi qu'aux particuliers investissant dans ses instruments, exposant les établissements prêteurs à un risque de crédit ;

Selon le *Financial Security Board* (FSB), il n'existe aujourd'hui aucune indication attestant d'une éventuelle exposition des banques et des acteurs financiers traditionnels aux crypto-monnaies. Il n'en demeure pas moins important de préserver cette étanchéité à l'avenir.

Les vulnérabilités se développant au sein de la sphère des crypto-monnaies y restent circonscrites

[72] Ainsi, lors de la bulle spéculative dite « Dotcom » (1997-2001), les valeurs technologiques ont atteint jusqu'à 3 000 milliards de dollars. Dans la période précédant l'éclatement de la crise des *subprimes*, le volume total de prêts hypothécaires titrisés était de 7 300 milliards de dollars.

Le système des crypto-monnaies a vu apparaître en son sein des vulnérabilités qui, si elles y restent aujourd'hui circonscrites, n'en méritent pas d'être soulignées et surveillées par les régulateurs :

- la volatilité, vingt-cinq fois plus élevée que celle du marché américain des actions, cinq fois plus forte que celle des matières premières et douze fois supérieure à celle du yen. Cette volatilité à laquelle les investisseurs sont exposés rend particulièrement difficile l'utilisation des crypto-monnaies en tant que moyen de paiement et menace la viabilité des plateformes d'échange (« *flash crashes* ») ;
- le recours au prêt pour l'achat de crypto-monnaies : on estime ainsi à 20 % la part des utilisateurs ayant recours à la dette pour financer leurs achats de crypto-monnaies soit au moyen de cartes de crédit ou de prêts hypothécaires[73], soit au moyen de prêts ayant des crypto-actifs pour collatéral[74] ;
- les effets de levier, qui amplifient la transmission des risques à l'économie réelle, car les investisseurs disposent alors de moins de capital pour absorber les pertes en cas de fluctuations de marché. Ainsi, les opérations sur marge (ou « *margin trading* ») avec effet de levier sont actuellement autorisées sur les crypto-monnaies dans un certain nombre de pays[75].

Encadré 6 : Effets de leviers sur les principales plateformes d'échange de crypto-monnaies

La plateforme d'échange américaine, Poloniex, offre à ses clients des opérations sur marge avec un effet de levier de 2,5, effet de levier qui peut s'élever à 100 fois la mise initiale sur la plateforme Bitmex basée aux Seychelles. La plateforme japonaise, Bitflyer, offre pour sa part un effet de levier atteignant jusqu'à 15 fois le dépôt en cash de ses clients.

Le montant total des contrats bénéficiant de cet effet de levier sur les plateformes n'est pas connu. Les entités susceptibles de financer ce levier ne sont pas davantage connues. Certains régulateurs ont toutefois fait état de plateformes offrant des prêts aux investisseurs.

Source : Financial Stability Board (FSB).

- le développement produits dérivés et d'instruments d'échange à terme (swaps) portant sur des crypto-monnaies : contrairement aux premiers, les seconds impliquent la livraison effective de crypto-actifs et, par voie de conséquence, leur détention et leur comptabilisation au bilan, avec le risque sous-jacent d'une transmission plus facile de la volatilité de ces actifs et du risque afférent à l'économie réelle.

Un risque de perte de confiance en cas d'effondrement rapide et général

Un choc négatif au sein de la sphère des crypto-monnaies pourrait affaiblir durablement la confiance que le public place aujourd'hui dans le système financier et ses infrastructures de marché. En effet, si les institutions financières traditionnelles venaient à être davantage exposées aux crypto-monnaies et si les craintes sur la viabilité de celles-ci venaient à se matérialiser, la confiance placée par les épargnants et les investisseurs dans le système financier en serait durablement amoindrie.

Ainsi, une brutale perte de valeur des crypto-monnaies, sous l'effet des fluctuations de marché, de la fraude ou de l'action des régulateurs, ferait peser sur l'ensemble du système financier un fort risque réputationnel. Par conséquent, il est essentiel pour les régulateurs – dont la crédibilité ne manquerait pas d'être mise à l'épreuve en cas d'effondrement rapide et général – d'avoir un discours ferme et clair sur la nécessité de limiter l'exposition des acteurs financiers traditionnels aux crypto-monnaies.

[73] Michelle Fox, "People are taking out mortgages to buy bitcoin, says securities regulator," CNBC, 11 décembre 2017.
[74] Olga Kharif, "These Guys Want to Lend You Money Against Your Bitcoin," Bloomberg, 14 décembre 2017.
[75] Yuval Gov (2018), "Bitcoin and Altcoins margin trading for beginners," January.

Les risques liés à l'anonymat et à la lutte anti-blanchiment

Les crypto-monnaies peuvent être utilisées, dans certains cas, pour dissimuler l'origine ou la destination des fonds. En effet, les mécanismes anonymes et décentralisés d'émission et de transfert de la plupart des crypto-monnaies peuvent favoriser l'utilisation de ces instruments à des fins criminelles (vente sur Internet de biens ou services illicites) ou à des fins de blanchiment ou de financement du terrorisme.

Les risques d'usage des crypto actifs à de telles fins sont liés au fait que les détenteurs de monnaies virtuelles ne sont pas identifiés, les clés privées de détention des crypto actifs étant en effet anonymes. Par analogie, cela revient à une situation dans laquelle aucun nom ne correspondrait à un IBAN, mais que toutes les opérations réalisées avec cet IBAN seraient visibles par tous.

En France, l'organisme de traitement du renseignement et d'action contre les circuits financiers clandestins (Tracfin) identifie l'utilisation de crypto-monnaies, comme étant à l'origine d'un risque spécifique en matière de blanchiment des capitaux et de financement du terrorisme. Cet organisme a ainsi reçu des banques, en 2017, quelques 351 déclarations de soupçon liées à l'utilisation des crypto-monnaies, contre 28 seulement en 2014.

Encadré 7 : L'activité de Tracfin en matière de crypto-monnaies

En 2016, Tracfin a reçu 178 déclarations de soupçon directement liées à des transactions en monnaie virtuelle pour un total de près de 5 M€.

Dans plus de la moitié des cas, l'utilisation de monnaies virtuelles (achat ou vente) est l'élément à l'origine de la déclaration de soupçon. La majorité des déclarations ont pour motif un doute sur l'origine ou la destination de fonds sans caractérisation précise du soupçon.

Les phénomènes les plus régulièrement recensés par les déclarants sont des cas d'intermédiation ou d'exercice illégal d'une profession réglementée. Ces dossiers font état d'individus collectant des fonds en provenance de nombreux particuliers dans le but de procéder à des opérations d'achat/revente de monnaies virtuelles sur des plateformes d'échange européennes pour le compte de tiers.

Source : Rapport annuel d'activité de Tracfin pour 2016.

À ce jour, si les cas de blanchiment d'argent au moyen de crypto-monnaies demeurent peu documentés et les cas répertoriés de financement du terrorisme par le biais de ces instruments demeurent relativement anecdotiques, le groupe d'action financière (GAFI) a récemment souligné l'utilisation croissante de ces produits à des fins criminelles. Outre le trafic de drogue à petite échelle et la fraude, le lien entre les crypto-monnaies et d'autres crimes semblent, en effet, se développer selon les conclusions du GAFI[76].

Les risques associés à l'usage du cash sont sans commune mesure avec ceux associés aux crypto-monnaies. Comme l'a indiqué Europol, « *bien que tous les usages du cash ne soient pas criminels, tous les criminels utilisent du cash à un moment donné dans le processus de blanchiment d'argent* »[77], ce qui n'est pas le cas avec les crypto-monnaies. Europol a également précisé que l'utilisation à des fins criminelles des crypto-monnaies exige toujours le recours au cash, soit pour l'encaissement, soit pour le décaissement des sommes en jeu.

Dans ce prolongement, le GAFI considère que les risques les plus significatifs en matière de lutte anti-blanchiment et de financement du terrorisme sont concentrés aux interfaces de conversion entre crypto-monnaies et monnaies ayant cours légal, soulignant ainsi la nécessité de réguler notamment les plateformes d'échange et autres intermédiaires de conversion.

[76] GAFI, *Rapport au G20*, juillet 2018.

[77] Europol, *Why is cash still a king? A strategic Report on the use of cash by Criminal groups as a facilitator for money laundering*, 2015.

L'Union européenne, dans sa dernière analyse supranationale des risques liés au blanchiment de capitaux et au financement du terrorisme en date de juin 2017[78], estime qu'en matière de lutte contre le blanchiment et de financement du terrorisme, les risques liées au cash sont « très significatifs », alors que ceux liés aux crypto-monnaies sont « modérément significatifs ». De ce point de vue et même du point de vue de la lutte contre la criminalité en général, l'analogie entre crypto-monnaies et cash n'est pas parfaite.

De fait, les rares études réalisées en la matière montrent que les activités illicites représentent une fraction limitée des échanges de bitcoins. Le *think tank* américain « Fondation pour la défense de la démocratie » a publié en janvier 2018 une étude détaillée sur le réseau Bitcoin de 2013 à 2016. Ses résultats montrent que les fonds d'origine illicite représentent moins de 1 % du volume des transactions du réseau Bitcoin, et qu'ils n'ont fait que diminuer au fil des années pour atteindre 0,1 % sur la dernière année considérée[79]. Une étude d'Europol corrobore pour partie ce constat : l'agence européenne estime ainsi que la part des transactions en bitcoins liées à un commerce illégal représentent 3 % à 6 % de l'ensemble des transactions.

L'intégrité des marchés et la protection des épargnants

Bien qu'assez peu souligné, le risque d'intégrité des marchés est un risque essentiel. L'enthousiasme pour la technologie des registres distribués et de la blockchain n'incite, en effet, pas au discernement et à la discrimination entre les produits. Il s'agit en cela d'un phénomène similaire à celui observé lors de la bulle dite « dot.com » dans les années 2000.

Aggravé par les conditions monétaires et financières accommodantes, le risque d'intégrité des marchés tient également pour une large part à l'écosystème des crypto-monnaies, à la fois opaque et très évolutif, avec des acteurs souvent mal identifiés et particulièrement mobiles.

En outre, la cyber-sécurité reste pour les investisseurs et les épargnants une préoccupation majeure. En effet, la conservation des crypto-actifs est confrontée à des cyber-risques importants, comme en attestent les risques avérés de piratage des portefeuilles électroniques assurant le stockage des crypto-actifs.

Dans ce contexte, les détenteurs n'ont aucun recours en cas de vol de leurs avoirs par des pirates informatiques. Les épisodes répétés de fraudes importantes (piratage de Coincheck en janvier 2018 pour 534 millions de dollars américains, faillite retentissante en 2015 de la première plate-forme mondiale d'échange de bitcoin, MtGox 3[80]), illustrent la vulnérabilité de l'écosystème des crypto-actifs et le niveau élevé des risques associés, en l'absence de mécanismes de garantie.

Le phénomène des ICO n'échappe pas à cette préoccupation de cyber-sécurité. Dans une étude de janvier 2018, le cabinet Ernst & Young a estimé que plus de 10 % des fonds levés par ICO avaient été soit perdus, soit volés à la faveur d'attaques de pirates informatiques. Ainsi, sur 372 ICO étudiées pour un total de 3,7 milliards de dollars levés, 400 millions de dollars ont disparu.

Le contournement des contrôles de capitaux et de changes

Si les crypto-monnaies facilitent les paiements transfrontières, en particulier dans les pays émergents, elles offrent, en contrepartie, la possibilité de contourner les règles nationales en matière de contrôle de capitaux et de changes.

[78] http ://ec.europa.eu/newsroom/document.cfm ?doc_id=45653

[79] http://www.defenddemocracy.org/media-hit/yaya-j-fanusie-bitcoin-laundering/

[80] À la suite d'une fraude interne ayant entraîné le détournement de 650 000 bitcoins pour une contrevaleur d'environ 360 millions de dollars américains.

En effet, les crypto-monnaies peuvent être utilisées pour transférer des monnaies avec cours légal en dehors des systèmes de paiement traditionnels, soumis dans certaines juridictions à de strictes limitations, comme en Chine par exemple. Alors que la question de l'applicabilité des régimes de contrôles de changes aux crypto-monnaies demeure incertaine ainsi que l'a souligné le FMI[81] dans une étude récente, ces instruments monétaires présentent un potentiel important en termes d'évasion de mouvements de capitaux et ce, au mépris des règles nationales de contrôle, lorsqu'elles existent.

Ce phénomène de contournement des contrôles de capitaux et de change tire profit tout à la fois :

- des atouts offerts par les registres technologiques distribués (DLT) et la blockchain, lesquels conjuguent rapidité d'exécution, faibles coûts de transaction et anonymat ;
- de la facilité avec laquelle les crypto-monnaies peuvent être achetées sur Internet, ce qui les rend particulièrement attractives dans des régimes monétaires où les systèmes de paiements traditionnels obéissent à des coûts élevés et à des contraintes réglementaires fortes.

De nombreux schémas d'évasion fondés sur les crypto-monnaies ont d'ores et déjà permis de transférer des capitaux hors de Chine, du Venezuela, de Chypre et de Grèce, justifiant en retour que certains de ces pays aient pris des mesures très restrictives à l'égard des crypto-monnaies[82].

Dans ces divers schémas d'évasion, au lieu d'acheter une monnaie ayant cours légal assujettie à des limitations en droit interne, les acteurs de marché ont acheté des crypto-monnaies sur Internet avant de les utiliser sur des bourses d'échange de pair-à-pair ou sur des plateformes d'échange en ligne et ce, afin de le convertir en monnaie étrangère ayant cours légal et ainsi de pouvoir transférer des capitaux qui n'auraient pu l'être au regard des règles de droit interne.

Encadré 8 : Crypto-monnaies et contournement des sanctions internationales

Certains pays cherchent à exploiter l'avantage de l'anonymat que procure les crypto-monnaies pour contourner les sanctions internationales auxquelles ils sont soumis.

Le Venezuela a ainsi annoncé, le 31 janvier 2018, son intention d'introduire sa propre crypto-monnaie, dénommée *Petro* et ayant pour sous-jacent les ressources naturelles du pays (pétrole, or et diamants). L'objectif visé par la création de cette crypto-monnaie est de contourner les sanctions imposées au Venezuela sur ses échanges commerciaux et financiers.

La Russie envisagerait également le lancement d'un « crypto-rouble », une crypto-monnaie adossée aux réserves de pétrole du pays, là aussi pour contourner le régime de sanctions internationales, bien que la banque centrale de Russie ait publiquement fait part de ses réserves sur l'usage des crypto-monnaies[83].

[81] FMI, *Virtual Currencies and Beyond: Initial Considerations*, janvier 2016, p. 31.

[82] La Chine a récemment interdit les ICO ainsi que les transactions en Bitcoin.

[83] Source: https://www.nytimes.com/2018/01/03/technology/russiavenezuela-virtual-currencies.html et https://www.bloomberg.com/news/articles/2017-12-15/whatthe-world-s-central-banks-are-saying-about-cryptocurrencies

III. LES POLITIQUES PUBLIQUES

Tous les pays s'interrogent aujourd'hui sur les crypto-monnaies. Beaucoup ont pris des mesures, parfois très radicales. Lors du G20 des 19 et 20 mars 2018, la France et l'Allemagne ont appelé dans une lettre conjointe les régulateurs internationaux à formuler des propositions. Cette partie présente en conséquence des lignes directrices pouvant guider les politiques publiques vis-à-vis des crypto-monnaies. Il est évident que les réponses nationales ne seront pas pleinement identiques. Un socle minimum de principes et de procédures de coopération accroîtrait toutefois l'efficacité des actions entreprises.

A. Une approche générale

Les crypto-monnaies sont dans une phase d'expérimentation technologique et économique. Leur avenir est encore incertain. Plusieurs scénarios sont envisageables : celui, très possible, d'un effondrement total et d'une disparition ou d'une marginalisation de toutes les monnaies existantes ; celui d'une sélection naturelle « darwinienne » dans laquelle émergeraient une ou deux monnaies dominantes ; celui, enfin, de l'apparition de nouveaux acteurs, issus du monde digital, des réseaux sociaux, ou du e-commerce, qui développeraient leurs propres systèmes de paiement, voire leurs propres monnaies internes.

Dans cette phase particulière, trois principes devraient guider les politiques publiques : (1) ne pas réguler directement les crypto-monnaies ; (2) créer un environnement favorable au développement la technologie ; (3) en contrepartie, circonscrire étroitement les risques ce qui impose de limiter strictement l'exposition du secteur financier aux crypto- monnaies.

1. Ne pas réguler directement les crypto-monnaies

Malgré les interrogations qu'elles suscitent, il n'est généralement pas souhaitable de réguler les crypto-monnaies – à l'exception essentielle de la lutte anti blanchiment.

Le statut juridique actuel des crypto-monnaies est très incertain et variable selon les pays. La situation est inconfortable pour les régulateurs, pour lesquels il est nécessaire de pouvoir nommer un objet et le classer dans une catégorie existante en vue de déterminer le régime (juridique, fiscal, prudentiel) auquel il est soumis.

Mais réguler suppose de définir, classer et, souvent, rattacher à une catégorie existante. Ce peut être nécessaire quand des décisions s'imposent, en matière fiscale notamment. Pour le reste, il faut sans doute accepter de vivre temporairement dans une certaine ambiguïté. En effet, le danger de la classification est triple : celui de figer dans les textes une évolution rapide de la technologie ; celui de se tromper sur la nature véritable de l'objet que l'on réglemente ; celui d'orienter l'innovation vers l'évasion règlementaire. Il parait beaucoup plus important – mais difficile – d'examiner en profondeur les caractéristiques économiques fondamentales et le profil de risque des objets en cause et déterminer en conséquence la réponse adaptée.

2. Créer un environnement favorable au développement la technologie

Il est essentiel de laisser les crypto monnaies – et les innovations qu'elles portent – se développer dans l'espace virtuel qu'elles occupent. La règlementation doit être « technologiquement neutre ». Les principales blockchains ont moins de trois ans. Des expériences intéressantes se développent sur des blockchains privées, notamment dans le secteur financier. En dehors de la finance, la technologie offre des perspectives pour la conservation et la transmission sécurisée des monnaies. Normaliser aujourd'hui les acteurs et la technologie conduiraient à paralyser ces progrès.

Pour se développer, la technologie a besoin de clarté. Les entrepreneurs de l'écosystème des crypto-monnaies et de la blockchain sont en droit d'attendre un cadre comptable, fiscal et prudentiel clair et lisible pour leurs activités. La place financière de Paris tirerait pleinement profit d'un tel cadre.

Dans le contexte de concurrence réglementaire qui tend à se développer autour de ces activités, il faut toutefois résister à la tentation du « moins disant ». La France n'a pas vocation à aligner ses standards réglementaires sur ceux des « paradis » qui existent sur les divers continents. À long terme, l'attractivité d'un cadre réglementaire ne s'apprécie pas à l'aune de sa permissivité, mais bien au regard de la sécurité juridique qu'il apporte aux acteurs de marché.

3. Limiter strictement l'exposition du secteur financier aux crypto-monnaies

C'est l'enjeu central des semaines et mois à venir. L'industrie de la gestion d'actifs ne s'est pas encore pleinement engagée dans les crypto monnaies qu'elle observe d'un œil prudent. Mais les pressions concurrentielles sont vives. Des projets existent, visant à créer des fonds d'investissements dédiés aux crypto-monnaies. Les grandes banques ont créé ou envisagent de créer des « trading desks » spécialisés dans les crypto-monnaies.

C'est donc un moment particulier, où la position des régulateurs aura un impact décisif sur l'évolution des comportements et du système. L'inertie réglementaire pourrait aviver la concurrence sur les marchés et conduire, par défaut, à banaliser et généraliser la place des crypto-monnaies dans le système financier.

Or, il s'agit d'instruments, dont le flux de revenus anticipés est soit nul (pour les crypto-monnaies), soit très incertain (pour les ICO). Ces caractéristiques fondamentales ne justifient pas leur inclusion, directe ou indirecte, dans les portefeuilles des particuliers. Elles n'ont pas vocation à s'insérer dans les portefeuilles à l'exception de ceux des investisseurs informés et dotés d'un appétit élevé pour le risque.

En effet, autoriser ou tolérer une exposition des intermédiaires financiers et des investisseurs institutionnels au risque des crypto-monnaies aurait trois conséquences graves :

- affaiblir la sécurité de l'épargne ;
- permettre un transfert de risque des investisseurs informés vers les particuliers. La détention de crypto-monnaies est aujourd'hui très concentrée entre les mains d'un nombre limité d'investisseurs. L'ouverture à l'épargne institutionnelle créerait une demande nouvelle, accroîtrait (au moins temporairement) la liquidité apparente des marchés et permettrait aux détenteurs actuels de céder, à un prix favorable, leurs avoirs aux nouveaux entrants qui supporteraient désormais le risque d'effondrement des cours ;
- créer un risque général pour la stabilité financière. Une fois reconnues et admises comme supports de placement, les crypto-monnaies serviraient aisément de base pour des montages avec effet de levier et transformation de maturité, créant potentiellement un risque systémique. Tout choc dans l'univers crypto affecterait immédiatement les bilans des intermédiaires financiers avec le risque d'une contagion et d'une amplification à l'ensemble du système.

B. Des principes minimaux de coopération internationale

1. La position des régulateurs internationaux et des instances européennes

Les recommandations du GAFI

Dès 2015, le groupe d'action financière (GAFI) ou *Financial Action Task Force* (FATF), organisme intergouvernemental de lutte contre le blanchiment d'argent et le financement du terrorisme réunissant 35 États, a publié des lignes directrices, intitulées *Guidance for a Risk-Based Approach to Virtual Currencies*.

Parce que ces lignes directrices sont aujourd'hui inégalement mises en œuvre dans les différentes juridictions, les États membres du GAFI ont appelé, en février 2018, à la mise en place de nouvelles dispositions pour renforcer la lutte contre le blanchiment de capitaux, lorsqu'elle est liée à l'usage de crypto-monnaies.

Le communiqué final du G20 des 19 et 20 mars 2018 a appuyé l'action du GAFI, l'appelant à mettre à jour les standards internationaux de lutte contre le blanchiment et le financement du terrorisme en matière de crypto-monnaies et à veiller à une plus large application de ces mêmes standards révisés.

Les avertissements de l'ESMA et des autres autorités européennes

L'autorité européenne des marchés financiers ou *European Securities and Markets Authority* (ESMA) a publié, le 13 novembre 2017, deux communiqués relatifs aux ICO :

- le premier mettant en garde les investisseurs sur les risques particulièrement élevés encourus dans le cadre des ICO, lesquelles proposent, selon l'ESMA, des investissements hautement spéculatifs, compte tenu notamment de la volatilité très forte du prix des *tokens* émis ;
- le second définissant les règles applicables aux entreprises émettant des *tokens* dans le cadre d'ICO. L'ESMA a rappelé à cet égard que les émetteurs devaient apprécier si les *tokens* ayant vocation à être émis étaient assimilables à des instruments financiers. Lorsqu'au sein d'un État membre, les ICO et les *tokens* qui en sont issus sont qualifiés d'instruments financiers, il est « probable » que les entreprises considérées réalisent des opérations d'investissement, soumises à la législation européenne applicable à ces services financiers[84].

Plus récemment, le 12 février 2018, les trois autorités européennes de supervision bancaire et financière, que sont respectivement l'ESMA, l'EBA (European Banking Authority) et l'EIOPA (*European Insurance and Occupational Pensions Authority*), ont publié un avertissement conjoint à l'attention des consommateurs européens sur les risques liés à l'achat et à la vente de crypto-monnaie.

Dans ce même communiqué, les autorités européennes rappellent que les crypto-monnaies et les plateformes sur lesquelles elles s'échangent ne sont pas régulées à ce jour, privant ainsi les consommateurs des garanties et de la protection prévues par la législation européenne en matière de services financiers. Elles soulignent également les risques d'intégrité de marché de ces plateformes compte tenu des attaques informatiques récurrentes dont elles sont l'objet.

Ces avertissements des régulateurs et superviseurs européens s'inscrit dans un contexte d'initiatives engagées par les institutions européennes :

- en février 2018, la Commission européenne a installé un observatoire européen de la blockchain, dans le cadre duquel elle présentera dans le courant de l'année 2018 un rapport sur les défis et les opportunités des actifs cryptographiques ;

[84] Directive prospectus, directive MiFID II, quatrième directive révisée sur le blanchiment d'argent, directive AIFMD.

- en avril 2018, le Conseil et le Parlement européen ont définitivement adopté la révision de la 4ème directive sur le blanchiment d'argent. Cette révision fait ainsi entrer dans le champ des assujettis à la lutte contre le blanchiment des capitaux et le financement du terrorisme les plateformes de conversion entre monnaies virtuelles et monnaies légales ainsi que les prestataires de services de portefeuilles de conservation de clés cryptographique. Ces deux entités doivent également faire l'objet d'une immatriculation. La directive prévoit enfin une définition de « monnaies virtuelles » et des « *wallet providers* ».

Les recommandations de l'IOSCO

Dans une communication rendue publique le 28 janvier 2018[85], l'*International Organisation of Securities Commissions* (IOSCO) a rappelé que le statut juridique des ICO et des *tokens* issus dans ce cadre devait l'objet d'une appréciation au cas par cas, en fonction des circonstances et des conditions propres à chaque ICO.

L'IOSCO a toutefois mis en garde les investisseurs et les épargnants sur les risques inhérents aux ICO, pouvant dans certains cas être considérés comme des investissements hautement spéculatifs faisant supporter aux souscripteurs un risque potentiel de perte complète de leur capital. Considérant que certains émetteurs offraient des opportunités d'investissements réelles et légitimes pour financer des projets destinés à la fourniture de biens ou services innovants, l'IOSCO a toutefois rappelé la nécessité de protéger les investisseurs, devenus la cible d'un démarchage croissant en ligne par des émetteurs le plus souvent installés à l'étranger à la faveur d'arbitrages réglementaires.

La position du FSB

Le 18 mars 2018, le *Financial Stability Board* (FSB) a défini ses priorités d'action pour la présidence argentine du G20. Parmi ces priorités d'action, figurent notamment :

- l'appréhension des risques liés à la protection des consommateurs et des investisseurs, ainsi que l'usage illicite des monnaies virtuelles à des fins de blanchiment de capital et de financement du terrorisme ;
- la prise en compte du potentiel offert par les technologies sous-tendant les crypto-monnaies, en ce que la blockchain et les registres distribués peuvent améliorer l'efficience et l'intégration des systèmes financiers ;
- le développement d'outils de mesure statistique, afin d'assurer un suivi renforcé des risques que font peser les crypto-monnaies sur la stabilité financière ;
- le renforcement de la coopération internationale compte tenu du caractère désormais mondialisé des marchés d'émission et d'échange des crypto-monnaies comme des *tokens*.

Dans un discours sur l'avenir de la monnaie en date du 2 mars 2018, le président du FSB, M. Mark Carney, a identifié trois approches possibles à l'égard des crypto-monnaies : les isoler, les réguler, les intégrer. Parce que, selon lui, l'isolement des crypto-monnaies emporte le risque d'entraver le développement des technologies sous-jacentes, la régulation lui semble être une meilleure approche, aux fins de combattre les activités illicites, de promouvoir l'intégrité des marchés et de garantir la sécurité ainsi que la stabilité du système financier.

[85] https://www.iosco.org/news/pdf/IOSCONEWS485.pdf

2. L'état de la réglementation étrangère et internationale[86]

Un tour d'horizon des mesures réglementaires prises à ce jour met en lumière le fait que ces mesures ont davantage été motivées par la volonté de limiter les risques liés à l'intégrité des marchés et à la protection des investisseurs que par le souci soit d'interdire, soit d'encourager le développement des activités liées aux crypto-monnaies.

Parmi les juridictions membres du *Financial Stability Board* (FSB), cette volonté de limiter les risques inhérents aux crypto-monnaies s'est traduite par le recours privilégié au « *soft law* » des lignes directrices publiées par les régulateurs nationaux et, dans une moindre mesure, par l'adoption de normes législatives visant à clarifier le statut des crypto-monnaies et à autoriser ponctuellement certaines activités qui leur sont liées.

Régimes juridiques actuels et tentative de classification des crypto-monnaies et des jetons

La définition et la classification des crypto-monnaies en général et des jetons en particulier constituent également un instrument de politique publique à la disposition des autorités nationales. Dans dix des juridictions interrogées (soit 40 % d'entre elles), la classification juridique des crypto-monnaies n'a pas été tranchée. C'est notamment le cas en Corée du Sud, dont les autorités n'ont pas, à ce jour, défini la nature juridique des monnaies virtuelles (titre, moyen de paiement ou bien).

Par conséquent, faute de classification juridique à portée générale, les autorités fiscales ont le plus souvent préempté la classification des crypto-monnaies, afin de clarifier leur régime fiscal. Ainsi, en 2014, l'*Internal Revenue Service* (IRS) américain a assimilé les crypto-monnaies à une propriété assujettie en cette qualité à la fiscalité sur les plus-values[87].

Toutefois, certains pays ont cherché à clarifier le statut juridique des crypto-monnaies et des jetons numériques. Le régulateur suisse, en l'espèce la FINMA, est probablement celui qui a réalisé, à ce jour, l'exercice de classification des *tokens* le plus abouti.

[86] La présente section a été rédigée sur la base des travaux du *Financial Stability Board* (FSB) actuellement en cours de publication ainsi que de l'analyse des réponses au questionnaire adressé par les services économiques régionaux de la direction générale du Trésor (DGT) en Chine, au Royaume-Uni, en Suisse, aux États-Unis, à Singapour, à Hong-Kong, en Corée du Sud, en Australie et au Japon.

[87] Cette doctrine de l'IRS s'est traduite, en 2016, par la communication aux services fiscaux américains des données de plusieurs millions de clients de la principale plateforme de conversion, Coinbase.

Encadré 9 : Classification des jetons et réglementation financière applicable en Suisse

Dans un contexte de développement soutenu des ICO en Suisse et en l'absence de dispositions légales spécifiques aux ICO, les émetteurs ont été de plus en plus nombreux à demander des clarifications sur leur assujettissement ou non à certaines dispositions du droit suisse des marchés financiers.

Dans ce contexte, la FINMA a publié en septembre 2017 un communiqué de cadrage sur l'applicabilité du droit des marchés financiers aux ICO puis, en février 2018, un guide pratique, lequel ne porte que sur l'applicabilité du droit commun des marchés financiers.

Pour déterminer le droit des marchés financiers applicable aux ICO, la FINMA estime qu'"*aucune évaluation abstraite d'ordre général et définitive concernant le droit des marchés financiers applicable n'est possible, notamment en raison des formes très différentes que peuvent prendre les jetons et les ICO. Toutes les caractéristiques du cas particulier doivent plutôt être prises en compte, sur la base des informations minimales à remettre par les organisateurs. Dans le sens d'une approche économique, la FINMA se base sur la teneur effective d'un ICO, a fortiori s'il existe des indices laissant à penser qu'il s'agit de structures de contournement*".

Les dispositions du droit des marchés financiers auxquelles un organisateur d'ICO est soumis dépendent de la fonction économique des jetons qui sont émis lors de l'ICO, la FINMA distinguant trois catégories de jetons ou tokens :

- les *tokens* considérés comme des moyens de paiement à titre non accessoire (jetons de paiement et jetons d'utilité pouvant servir de moyens de paiement à titre non accessoire) sont soumis à la législation anti-*blanchiment* lors de leur émission ;
- les *tokens* considérés comme des valeurs mobilières sont assujettis à la législation sur les valeurs mobilières lors de leur émission ;
- les *tokens* donnant accès à un usage ou à un service numériques dès le moment de l'émission et qui s'appuient sur l'utilisation d'une infrastructure de type blockchain peuvent être assujettis (i) soit à la législation suisse sur les valeurs mobilières s'ils ont en outre un but d'investissement au moment de leur émission, (ii) soit à la législation anti-blanchiment si la principale raison pour les émettre est leur utilisation à des fins de moyens paiement.

En l'absence de toute classification juridique, le statut des *tokens* fait le plus souvent l'objet d'une appréciation au cas par cas, en fonction des circonstances et des conditions propres à chaque ICO. C'est notamment l'approche retenue aux États-Unis par la SEC, dont la jurisprudence tend toutefois à assimiler assez largement les *tokens* émis lors d'ICO à des actifs financier soumis, à ce titre, à la législation fédérale américaine sur les titres financier. Exprimée en 2017, cette position a été rappelée en juin 2018, le SEC considérant que si le Bitcoin et l'Ether ne sont pas des valeurs mobilières, les levées de fonds en monnaies virtuelles (ICO) sont, dans certaines conditions, assimilables à des introductions en bourse et ont donc vocation à être réglementées comme telles.

Publication de lignes directrices par les régulateurs nationaux

L'option privilégiée, à ce jour, par les États membres du FSB est celle de la publication par les régulateurs nationaux de lignes directrices destinées notamment à clarifier l'application aux crypto-actifs de la législation sur les valeurs mobilières ou à informer les consommateurs des risques qui leur sont liés. En effet, 84 % des membres du FSB[88] ont pris ou envisagent d'édicter de telles lignes directrices. Les régulateurs nationaux et, plus largement, européens ou internationaux ont émis de nombreux avertissements autour des crypto-monnaies, ainsi que cela a été rappelé dans la section précédente (voir *supra*).

Définition d'un cadre réglementaire

Dix-sept juridictions membres du FSB, soit plus des deux tiers d'entre elles, ont d'ores et déjà adopté ou envisagent d'adopter un cadre législatif ayant pour objet soit d'autoriser certaines activités réglementées en lien avec les crypto-monnaies, soit à clarifier le statut juridique de celles-ci.

[88] Dix-sept juridictions membres du FSB l'ont d'ores et déjà fait, tandis que quatre autres l'envisagent activement.

De la même manière, quinze autres États membres du FSB, soit 60 % d'entre eux, ont mis en place ou envisagent de mettre en place une « *sandbox* » ou tout autre cadre réglementaire, destiné à faciliter toute activité portant sur les crypto-monnaies[89].

Sanctions réglementaires et actions judiciaires

Un quart des régulateurs nationaux des juridictions membres du FSB – en l'espèce, les régulateurs américain, chinois, français, allemand, hongkongais et suisse – ont déclaré avoir d'ores et déjà prononcé des sanctions administratives à l'encontre d'un émetteur de crypto-monnaies. Une telle action est à l'étude dans cinq autres juridictions membres du FSB (soit 20 % d'entre elles).

Les actions judiciaires demeurent toutefois moins nombreuses que les sanctions administratives. En effet, seules deux juridictions membres du FSB – en l'espèce, les États-Unis et le Canada – ont engagé des actions en justice contre les promoteurs ou les émetteurs de crypto-monnaies. Aux États-Unis, le *Department of Justice* (DoJ), en collaboration avec la CFTC, a ouvert, le 27 mai 2018, une enquête judiciaire sur d'éventuelles manipulations des cours du Bitcoin et d'autres crypto-monnaies.

Interdictions des activités, produits et services financiers liés aux crypto-monnaies

Les juridictions membres du FSB déclarent :

- pour un plus d'un tiers d'entre elles, avoir rejeté ou envisager de rejeter une ou plusieurs demandes d'ETF portant sur des crypto-monnaies ;
- pour un peu moins d'un tiers d'entre elles, avoir interdit ou envisager d'interdire une ou plusieurs ICO ;
- pour un quart d'entre elles, avoir interdit ou envisager d'interdire à une ou plusieurs institutions financières réglementées de fournir des services de paiement à des plateformes d'échange de crypto-monnaies ;
- pour un autre quart d'entre elles, avoir interdit ou envisager d'interdire un ou plusieurs prêts accordés par une institution financière réglementée en garantie d'un ou de plusieurs crypto-actifs ;
- pour 16 % d'entre elles, avoir rejeté ou envisager de rejeter la demande d'agrément d'une ou de plusieurs plateformes d'échanges de produits dérivés portant sur des crypto-actifs.

Il convient également de souligner l'exemple du Japon, qui a interdit aux banques et aux gestionnaires d'actifs, dès août 2016, de réaliser des opérations en comptes propres en crypto-monnaies. Au-delà du Japon, deux pays – la Chine et la Corée du Sud – se distinguent plus particulièrement par leur politique d'interdiction progressive des activités ou services liés aux crypto-monnaies.

Dans le cas de la Chine, les autorités ont successivement interdit, en 2013, aux banques et aux autres institutions financières de détenir et de réaliser des transactions en crypto-monnaies (seules les personnes privées sont autorisées), puis en 2017, les financements par ICO et fait fermer les des plateformes de conversion de Bitcoin installées sur le territoire chinois ; en 2018 stratégie de fermeture des fermes de minage de Bitcoin.

[89] La politique de règles adaptées, dite politique du bac à sable (ou de la « sandbox » en anglais), consiste à définir et à appliquer aux nouveaux acteurs d'un marché des règles spécifiques moins contraignantes que les règles générales appliquées aux acteurs traditionnels.

Encadré 10 : État de la réglementation en Corée du Sud

- **Position de la *Financial Services Commission* (FSC) FSC sur l'exposition des acteurs financiers aux crypto-monnaies :**

En décembre 2017, la FSC coréenne a pris plusieurs décisions destinées à limiter strictement l'exposition des acteurs financiers aux crypto-monnaies. Ainsi, les contrats à terme sur le bitcoin ont été interdits. Interdiction a également été faite :

- aux institutions financières coréennes de détenir ou d'échanger des monnaies virtuelles pour leur propre compte ;
- aux mineurs et aux étrangers d'investir dans les monnaies virtuelles.

Les détenteurs d'un compte en monnaie virtuelle ont été contraints de s'enregistrer sous leur vraie identité pour limiter les risques liés au blanchiment d'argent ou à la fraude fiscale. Plus largement, les banques ont désormais l'obligation de signaler aux autorités les transactions en monnaies virtuelles jugées suspectes et, de façon plus générale, de mettre en place des procédures de « *due diligence* » précises pour contrôler les transactions effectuées avec les plateformes d'échange de monnaies virtuelles.

Le gouvernement a finalement annoncé le 21 janvier 2018 que les plateformes d'échange de monnaies virtuelles seraient contraintes de partager le détail des transactions effectuées par chacun de leur utilisateur avec les banques auprès desquelles elles disposent de comptes[90].

- **Position de la FSC sur les ICO :**

La *Financial Services Commission* (FSC) a d'abord interdit les levées de fonds en monnaies virtuelles (ICO) le 30 septembre 2017 pour décourager la spéculation et limiter la fraude[91].

- **Position de la FSC sur les plateformes :**

Les plateformes d'échange de monnaies virtuelles sont quant à elles légalement enregistrées comme des sites d'e-commerce selon la loi coréenne et ne nécessitent pas de licence spécifique. Cependant, le ministre de la Justice a annoncé le 15 janvier 2018 qu'un projet de loi était en préparation pour interdire tout échange de monnaies virtuelles et fermer les plateformes d'échange.

Interdiction d'utilisation des crypto-monnaies en tant que moyen de paiement

En septembre 2017, la *Reserve Bank of India* a indiqué que le Bitcoin et les autres crypto-monnaies n'étaient pas des moyens de paiement légaux et ne pouvaient donc être utilisés à cet effet. Un mois plus tard, en octobre 2017, la *Bank Indonesia* a également interdit l'utilisation des monnaies virtuelles à des fins de paiement.

Régulation des intermédiaires et des plateformes d'échange

Plusieurs juridictions membres du FSB ont différencié les règles respectivement applicables aux intermédiaires et plateformes d'échange de crypto-monnaies, reflétant ainsi les différentes fonctions économiques exercées par ces acteurs.

Le cas des États-Unis est révélateur de cette volonté de réguler de manière différenciée les différents acteurs de la chaîne de valeur de la crypto-finance. Dès 2013, la *Financial Crimes Enforcement Network* (FinCEN) a assujetti les plateformes de conversion aux règles relatives à la lutte contre le blanchiment et le financement du terrorisme. En 2015, le *Department of Financial Services* de l'État de New-York a pour sa part créé la Bitlicense pour les activités de détention et de conversion de crypto-monnaies.

De la même manière, le Japon s'est également efforcé de réguler les intermédiaires et les plateformes d'échange.

[90] À partir du 30 janvier, les utilisateurs des plateformes d'échange devront disposer d'un compte personnel auprès de l'une des banques utilisées par leur plateforme pour pouvoir effectuer des transactions.
[91] La Corée est le deuxième pays à interdire les ICO, après la Chine au début du mois de septembre.

Encadré 11 : État de la réglementation applicable au Japon

- **Avril 2017** : adoption du *Virtual Currency Act*, qui reconnaît les crypto-monnaies comme des moyens de paiement n'ayant pas cours légal. Les crypto-monnaies sont ainsi définies comme des valeurs financières utilisables pour le paiement à des personnes non-déterminées et pouvant être acquises ou vendues à des personnes non-déterminées ;
- **Septembre 2017** : octroi par la *Financial Services Authority* des onze premiers agréments d'exploitation à des plateformes japonaises, les assujettissant ainsi à des exigences de KYC, à un montant minimal de capital de 85 000 €, à une obligation de solvabilité (actif net positif), à une gestion séparée des comptes en cash et de ceux en crypto-monnaies, à la publication d'un rapport annuel et d'un *reporting* trimestriel des encours au superviseur, ainsi qu'à des règles de sécurité des systèmes informatiques et de traitement de données. Pour s'assurer du bon respect de ces règles, les autorités de régulation japonaises disposent d'un pouvoir de contrôle sur place ;
- **Octobre 2017** : recommandation non-contraignante sur les risques liés aux ICO en matière de volatilité des prix et de fraude :
- **Février 2018** : octroi du seizième agrément d'exploitation à une plateforme d'échange.

D'autres pays envisagent de mieux réguler les intermédiaires et les plateformes d'échange de crypto-monnaies. Ainsi, l'Australie va prochainement introduire un système d'immatriculation des plateformes d'échange. La *Monetary Authority of Singapore* (MAS) pourrait également, d'ici un an, renforcer les contraintes réglementaires portant sur les intermédiaires impliqués dans les transactions de monnaies virtuelles, en particulier en matière de lutte anti-blanchiment.

Si les crypto-monnaies ne présentent à ce jour pas de risque du point de vue de la stabilité financière, il est souhaitable que les différents États membres du FSB coordonnent plus largement l'élaboration de leurs réponses politiques aux défis posés par les crypto-monnaies. Une coordination internationale dans le cadre du G20 s'avère à cet égard indispensable, comme le détaille le présent rapport dans la section suivante (voir *infra*).

3. Les perspectives de coopération internationale

L'échange d'informations

Progresser vers une compréhension commune des crypto-monnaies

En effet, le manque de données statistiques sur les montants financiers émis sur le marché primaire des ICO et échangés sur le marché secondaire des plateformes est régulièrement dénoncé. Cette situation rend délicate mise en place d'une protection des épargnants adaptée en l'absence de connaissance précise du périmètre et de la liquidité de ce marché ainsi que de ses acteurs

Ce suivi statistique est aujourd'hui laissé à l'initiative d'acteurs privés, sur la base d'informations ne pouvant être vérifiées et dont il n'est pas interdit de penser qu'elles peuvent contribuer dans certains cas à influencer, voire à manipuler, les cours. Le communiqué du G20 du 20 mars 2018 a posé, à cet égard, un premier jalon, puisqu'il dispose : « *Nous comptons sur les organismes internationaux de normalisation compétents pour poursuivre leur travail de supervision des crypto-actifs et des risques associés, conformément à leurs mandats respectifs, et pour évaluer les réponses multilatérales en fonction des besoins* ». Les pays du G20 pourraient renforcer le mandat des organismes internationaux compétents – FSB, IOSCO et GAFI – dans cette perspective.

Favoriser l'échange de données fiscales entre juridictions

La taxation des gains tirés de l'achat et de la vente de crypto-monnaies demeure conditionnée au recouvrement effectif des sommes correspondantes. Or, les transactions étant réalisées le plus souvent sur des plateformes non-régulées et situées dans des juridictions non-coopératives, il est essentiel de renforcer la coopération internationale en matière fiscale.

Ainsi, les pays du G20 pourraient prendre l'engagement de soumettre les plateformes d'échanges de crypto-monnaies présentes sur leur territoire à deux obligations :

- d'une part, l'obligation de collecter le numéro d'identification fiscale de leurs clients lors du KYC, sur le modèle de qui est exigé lors d'un KYC bancaire traditionnel ;
- d'autre part, l'obligation d'échanger toute donnée relative aux revenus et gains réalisés auprès des administrations fiscales nationales de référence. L'échange automatique d'informations, tel qu'il est aujourd'hui prévu par l'OCDE pour les seuls avoirs bancaires et financiers traditionnels, serait ainsi étendu aux crypto-actifs échangés sur les plateformes.

Le financement des entreprises et des projets à l'ère d'Internet

Internet conduira à une profonde transformation des modes de financement de l'innovation et des entreprises. Les émissions et levées de fonds transfrontières sur le réseau vont se développer rapidement. Tirer les bénéfices de cette technologie en protégeant les épargnants représente un immense défi. Nul ne peut dire s'il peut être relevé dans un environnement où les règlementations et préférences nationales différent. Le sujet mérite une réflexion approfondie et prospective, dont la responsabilité pourrait être confiée au FSB ou IOSCO par le G20. Les thèmes suivants pourraient être couverts : gouvernance des émetteurs et des projets, contenu des *white papers*, obligations de KYC, protection générale des épargnants et transparence.

La lutte contre le blanchiment et le financement du terrorisme

Le travail de coopération a d'ores et déjà été largement engagé au niveau européen et multilatéral pour prévenir les risques de blanchiment de capitaux et de financement du terrorisme que peuvent présenter les crypto-monnaies de manière générale et les plateformes d'échange en particulier.

Ce sont 70 pays qui se sont engagés, lors de la conférence mondiale de lutte contre le financement du terrorisme du 27 avril 2018, à promouvoir la mise en œuvre des normes internationales du GAFI relatives à ces technologies. L'Union européenne a pour sa part adopté une nouvelle directive européenne renforçant les règles applicables aux plateformes d'échanges.

Encadré 12 : Principales dispositions de la directive (UE) 2018/843 du 30 mai 2018 modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme

La directive 2018/843 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme fait entrer dans le champ des assujettis à la lutte contre le blanchiment des capitaux et le financement du terrorisme :

- les prestataires de services d'échange entre monnaies virtuelles et monnaies légales ;
- les prestataires de services de portefeuilles de conservation.

Ces deux entités doivent également faire l'objet d'une immatriculation, procédure qui comprend a minima un examen de la compétence et à l'honorabilité des personnes qui exercent une fonction de direction au sein de ces entités.

La directive prévoit en outre une définition de « monnaies virtuelles » et des « *wallet providers* ».

Malgré les récentes avancées notables dans ce domaine, il faut poursuivre la coopération à tous les niveaux – international, européen et français – pour renforcer la démarche de lutte anti-blanchiment et de financement du terrorisme sur l'ensemble de la chaîne de la crypto-finance.

Au niveau international : transformer les lignes directrices du GAFI en recommandation

Compte tenu de l'inégale application des standards internationaux en matière de lutte contre le blanchiment et le financement du terrorisme, les pays du G20 pourraient s'engager à faire des lignes directrices actuelles du GAFI sur les crypto-monnaies[92] une recommandation à part entière. Cette recommandation aurait le mérite de soumettre les États membres à un mécanisme d'évaluation par les pairs et *in fine* à améliorer l'effectivité des standards internationaux en matière de lutte contre le blanchiment de capitaux.

Au niveau européen : étendre les règles de la directive 2018/843 aux émetteurs d'ICO

Alors que la directive 2018/843 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme vient tout juste d'être adoptée, il est souhaitable que les règles qu'elle contient soit étendues à l'ensemble des intermédiaires de la chaîne de valeur des crypto-monnaies, dès lors qu'ils manipulent[93] les clés cryptographiques privées permettant d'accéder aux crypto-actifs, de les stocker et de les transférer.

Encadré 13 : Modalités d'extension des règles de la directive 2018/843 aux émetteurs d'ICO

L'application des règles de la directive 2018/843 aux émetteurs d'ICO soulève deux questions :

- en premier lieu, il convient de déterminer si les émetteurs d'ICO doivent être assujettis, de manière générale, à la lutte contre le blanchiment et le financement du terrorisme et si ces ICO représentent ou non un risque avéré de ce point de vue. En raison du caractère récent du phénomène, il est difficile de répondre de manière définitive à cette question pour tous les types d'ICO. Il n'en demeure pas moins que certaines de ces procédures d'émission peuvent, ainsi que l'a récemment rappelé le GAFI[94], présenter un risque non nul lié aux conditions d'anonymat ainsi qu'à la facilité tant de levée des fonds que de conversion des *tokens* en monnaies avec cours légal. Considérant que ces risques devaient être traités, seize pays – dont la Suisse, laquelle est également réputée pour attirer un grand nombre d'ICO – ont d'ores et déjà assujettis les émetteurs d'ICO aux règles relatives à la lutte contre le blanchiment et le financement du terrorisme ;
- en second lieu, se pose la question de savoir si les ICO pourraient être soumises ou pas à l'ensemble des règles prévues par la directive 2018/843. Deux cas de figure doivent, à cet égard, être distingués. Si une ICO conduit à l'émission d'une « monnaie virtuelle »[95] au sens de la directive, elle a naturellement vocation à rentrer dans son champ d'application. En revanche, si la procédure d'ICO a pour objet l'émission d'un *token* ne pouvant être assimilé à une monnaie virtuelle au sens de la directive 2018/843, il convient alors de déterminer le régime applicable, à savoir un assujettissement partiel ou un assujettissement optionnel. Alors que le premier emporte le risque de détricoter l'actuel dispositif européen de lutte contre le blanchiment pour n'en retenir que les seules mesures susceptibles d'être appliquées de manière *ad hoc* aux émetteurs concernés, le second permet d'appliquer un dispositif global et cohérent, mais de manière optionnelle, afin d'en exonérer à bon droit les professionnels, dont l'activité ne présente pas de risque particulier de ce point de vue.

[92] http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html

[93] Excluant ainsi *de facto* les *cold wallet*, qui fournissent des appareils électroniques physiques de stockage, mais ne détiennent ni ne contrôlent directement ou indirectement des clés cryptographiques privées.

[94] GAFI, *Crypto-assets: Review of FATF Standards and Guidance*, 11 juin 2018.

[95] Par « monnaies virtuelles », la directive 2018/843 entend toute représentation numérique d'une valeur qui n'est émise ou garantie ni par une banque centrale ni par une autorité publique, qui n'est pas nécessairement liée non plus à une monnaie établie légalement et qui ne possède pas le statut juridique de monnaie ou d'argent, mais qui est acceptée comme moyen d'échange par des personnes physiques ou morales et qui peut être transférée, stockée et échangée par voie électronique.

Plus largement, il est essentiel que soit rapidement mis en place un mécanisme européen d'échange de données électroniques entre autorités nationales de régulation et supervision, en particulier dans le cadre d'enquêtes judiciaires, sur les transactions réalisées au sein de la seule sphère crypto. Un tel mécanisme pourrait être intégré au projet de directive présenté par la Commission européenne le 17 avril 2018 et fixant les règles facilitant l'utilisation d'informations financières aux fins de prévention et de détection de certaines infractions pénales.

Au niveau national : renforcer les moyens technologiques des services d'enquête en matière de lutte contre le blanchiment

Dans le prolongement de ce mécanisme européen d'échange de données entre autorités nationales, il est indispensable de renforcer les moyens technologiques d'investigation dont disposent les services d'enquête en matière de lutte contre le blanchiment et le financement du terrorisme (Tracfin et cyberdouane notamment).

En effet, les outils d'investigation actuellement utilisés par ces services ne sont compatibles qu'avec la seule blockchain du Bitcoin, ne leur permettant pas de suivre les transactions illicites réalisées au moyen d'autres crypto-monnaies, telles qu'Ether, Monero ou Saga. Il est donc essentiel de prolonger les avancées permises par l'évolution du cadre juridique européen par un effort d'investissement accru dans les capacités technologiques d'investigation des services de lutte anti-blanchiment, afin d'étendre leur champ d'intervention sur l'ensemble des crypto-monnaies.

La régulation des plateformes

À l'heure où les États s'interrogent sur les réponses susceptibles d'être apportées aux défis posés par les crypto-monnaies, les plateformes sont le lieu où s'exerce la concurrence réglementaire. Si certains pays ont fait le choix de les réguler – en les soumettant à une procédure d'agrément, en leur imposant des règles prudentielles et en les assujettissant à la lutte contre le blanchiment – d'autres États misent délibérément sur un environnement permissif.

Parce que ce déséquilibre ne peut que nuire à la crédibilité et à la viabilité des crypto-monnaies, il est indispensable de rétablir, à l'échelle internationale, les conditions d'une concurrence équitable reposant sur un socle de principes minimaux, que sont la transparence dans la négociation et la formation des prix, l'intégrité des marchés et la robustesse. Les règles de lutte anti-blanchiment, telles qu'elles sont définies par le GAFI, sont également incontournables.

L'exposition des intermédiaires financiers

S'agissant des banques

Leur exposition est aujourd'hui inexistante ou très limitée. Les banques n'accordent pas de crédit pour l'achat de crypto-monnaies et certaines ont prohibé l'utilisation de cartes de crédit à cet effet. Elles n'interviennent pas davantage pour compte propre sur les marchés des crypto-monnaies. Elles portent, en outre, une grande attention au respect des règles de lutte anti-blanchiment. Il faut encourager le statu quo, et, pour ce faire, suivant la suggestion de certains banquiers centraux, soumettre les opérations en crypto-monnaies pour comptes propres à une pondération de 100 % au titre des exigences en capital. Les banques pourraient également être soutenues et encouragées dans leur refus de financer les achats de crypto-monnaies par leurs clients.

S'agissant des gestionnaires d'actifs

Les ministres et régulateurs pourraient exprimer clairement, dès les prochaines réunions internationales, leur souhait de décourager l'exposition des gestionnaires d'actifs aux risques financiers liés aux crypto-monnaies, en particulier la création de nouveaux produits et marchés dérivés, d'indices et de fonds – ETF en particulier – dédiés aux crypto-monnaies et en prohibant l'inclusion des crypto-monnaies dans les véhicules de placement collectifs ouverts à l'épargne « grand public » (assurance-vie, fonds de pension, etc.).

Cette recommandation ne vaut toutefois pas pour les investisseurs informés et la gestion alternative. Elle pourrait être périodiquement réexaminée en fonction des évolutions de la technologie et des habitudes si celles-ci devaient conduire à une utilisation large des crypto monnaies leur conférant dès lors une valeur d'usage (comme instrument de paiement).

Intégrité de marché et protection des épargnants

Cette protection doit être pleinement et légitimement garantie en raison du caractère relativement répandu de la fraude.

Si aucune bonne pratique n'a encore vu le jour en dehors des seules alertes émises et des informations rendues publiques par les régulateurs, l'interdiction du démarchage en ligne sur les produits liés aux crypto-monnaies à l'attention du « grand public » (en particulier, sur les réseaux sociaux) pourrait être envisagée. La législation française offre, à cet égard, un précédent : le législateur a ainsi interdit la publicité électronique relative au *trading* en ligne[96].

Cette interdiction pourrait être limitée aux seuls acteurs de la crypto-finance ne s'étant pas conformés aux règles édictées par les régulateurs. Ainsi, les émetteurs d'ICO ayant reçu le visa optionnel de l'AMF, les plateformes opérant dans le cadre du statut expérimental d'agrément unique et tout intermédiaire de la chaîne de valeur des crypto-actifs se soumettant aux prescriptions internationales et européennes en matière de lutte contre le blanchiment et le financement du terrorisme ne seraient pas visés.

C. Une clarification des pratiques et du cadre règlementaires français et européens

1. Le cadre comptable et fiscal des activités sur crypto-monnaies

L'envolée des cours des crypto-monnaies à la fin de l'année 2017 et le développement rapide des ICO sur la même période sont intervenus en dehors de tout cadre comptable et fiscal bien défini. Cette absence laisse aujourd'hui une large place à l'interprétation des règles comptables et fiscales et crée une incertitude défavorable au développement de ces activités. Une clarification peut être recherchée dans les directions suivantes :

- pour les crypto-monnaies elles-mêmes, adopter un régime proche, voire identique, à celui qui s'applique aux opérations en devises ;
- pour les opérations d'ICO conduisant à l'émission de jetons d'utilité, aligner d'une part le rythme de constatation des revenus (et partant de leur imposition) sur celui de développement de l'entreprise et encourager d'autre part la détention durable des jetons émis.

Les gains liés à l'achat et à la vente de crypto-monnaies : le régime des devises

L'exonération de TVA des opérations de conversion des crypto-monnaies

En matière de TVA, le régime fiscal des monnaies virtuelles est aligné sur celui des monnaies ayant cours légal. Ainsi, assimilées à des opérations portant sur des devises, les opérations de conversion de crypto-monnaies contre d'autres crypto-monnaies ou des monnaies ayant cours légal sont exonérés de TVA, ainsi que l'a jugé la Cour de justice de l'Union européenne (CJUE), en 2013, dans un arrêt *Hedqvist*.

La fiscalité des particuliers

La question de la fiscalité des plus-values réalisées lors de la cession de crypto-monnaies a fait l'objet d'une position de l'administration fiscale en 2014[97], position sur laquelle le Conseil d'État est partiellement revenu le 26 avril 2018[98].

Par des commentaires administratifs du 11 juillet 2014, l'administration fiscale avait, en effet, considéré que les gains tirés par des particuliers – personnes physiques ou morales soumises à l'impôt sur le revenu – de la cession de crypto-monnaies étaient imposables dans la catégorie des bénéfices industriels et commerciaux (BIC) lorsqu'ils correspondaient à une activité habituelle et dans la catégorie des bénéfices non commerciaux (BNC) lorsqu'ils correspondaient à une activité occasionnelle. Dans les deux cas, le taux marginal à l'impôt sur le revenu, prélèvements sociaux compris, pouvait atteindre 62,2 %.

Dans sa décision précitée du 26 avril 2018, le Conseil d'Etat a jugé que :

- les crypto-monnaies ont le caractère de biens meubles incorporels et que les profits tirés de leur cession à titre occasionnel par des particuliers relèvent en principe du régime des plus-values de cession de biens meubles de l'article 150 UA du code général des impôts, soit un taux forfaitaire de 40,2 % ;
- les gains provenant de la cession à titre habituel de crypto-monnaies acquises en vue de leur revente, dans des conditions caractérisant l'exercice d'une profession commerciale, sont imposables dans la catégorie des BIC, soit un taux marginal pouvant aller jusqu'à 62,2 %.

Comme le met en exergue le tableau figurant en annexe n° 7, la jurisprudence du Conseil d'État présente l'avantage d'aligner la fiscalité applicable aux cessions de crypto-monnaies par des particuliers sur celle aujourd'hui applicable aux gains en devises.

La fiscalité des entreprises

Les gains que les personnes morales soumises à l'impôt sur les sociétés tirent de leur cession de crypto-monnaies sont imposés dans les conditions de droit commun et sont donc assujettis à un taux de 33 %. Ce régime fiscal est comparable à celui applicable aux gains de devises réalisés par des entreprises.

Le traitement comptable et fiscal des ICO

La fiscalité des ICO revêt deux enjeux, suivant que l'on se place du point de vue de l'émetteur de *tokens* ou du point de vue du souscripteur.

Du point de vue de l'émetteur

L'objectif est de parvenir à lisser comptablement les produits liés à l'émission de *tokens*, afin de pouvoir étaler fiscalement le paiement correspondant de l'impôt sur les sociétés sur toute la durée nécessaire au développement du bien ou du service, lesquels n'ont vocation à être effectivement produits et fournis que plusieurs années après l'émission des *tokens*. En effet, un assujettissement prématuré à l'impôt sur les sociétés risquerait d'entraver la production du bien ou du service considéré.

Pour y parvenir, cela suppose :

- **au plan comptable**, d'inscrire au passif de l'entité émettrice les sommes perçues en contrepartie de l'émission de tokens en produits constatés d'avance[99] (et ce, dans l'attente de la production et de la fourniture du bien et du service), afin d'éviter l'inscription au compte de résultat de la totalité des sommes perçus dès le stade de l'émission ;

[96] Voir l'article L. 533-12-7 du code monétaire et financier.

[97] Commentaires administratifs publiés le 11 juillet 2014 au bulletin officiel des finances publiques (BOFIP).

[98] http://www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/Conseil-d-Etat-26-avril-2018-M.-G-et-autres

[99] La méthode comptable de l'avancement consiste à comptabiliser les ventes et les coûts associés à un projet au fur et à mesure de son niveau d'avancement.

- **au plan fiscal**, d'étaler le paiement correspondant de l'impôt sur les sociétés en fonction de la constatation progressive au compte de résultat des produits perçus du niveau d'avancement des biens ou services, dont le *token* est la contrepartie.

Ces règles ne vaudraient que pour les jetons considérés comme des « *utility tokens* ». En effet, pour les jetons assimilés à des « *security tokens* », les règles de comptabilisation et de fiscalité des valeurs mobilières ont vocation à s'appliquer à droit constant[100].

En revanche, dès lors que, dans le cadre d'une ICO, l'entité émettrice est amenée à détenir des crypto-monnaies perçues en contrepartie des *tokens* vendus, il est recommandé d'inscrire ces monnaies virtuelles à l'actif du bilan des entités émettrices au sein d'une classe d'instruments de trésorerie divers, qui a elle-même vocation à être créée au sein du plan comptable général. Les éventuelles plus-values réalisées sur ce stock de monnaies virtuelles détenues à l'actif doivent être taxées à l'impôt sur les sociétés dans les conditions de droit commun.

Du point de vue de l'investisseur

L'enjeu est d'adapter la fiscalité des plus-values réalisées sur les *tokens* détenus par les souscripteurs suivant que (i) leur détention est durable et que (ii) ces crypto-actifs répondent effectivement à la production ou à la fourniture de biens ou de services de l'entité émettrice.

Si ces conditions sont remplies, les *tokens* effectivement détenus par les souscripteurs ont vocation à être inscrits à l'actif de leur bilan en tant qu'immobilisations incorporelles amortissables selon les règles de droit commun, et dépréciées le cas échéant selon les règles actuelles du plan comptable général. La valorisation de la détention durable de ces *tokens* par les investisseurs pourrait se traduire, au plan fiscal, par un régime d'exonération à l'impôt sur le revenu en fonction de la durée de détention, s'inspirant en cela des applicables actuellement aux fonds communs de placement à risque (FCPR).

En revanche, si les conditions précitées – détention durable et production ou fourniture d'un bien et service – ne sont pas réunies, les *tokens* détenus par les souscripteurs ont vocation à être inscrites à l'actif de leur bilan au sein d'une classe d'instruments de trésorerie divers qu'il convient de créer au sein du plan comptable général. Sur le plan fiscal, les plus-values réalisées sur les jetons détenus ont vocation à entrer dans le champ d'application du régime fiscal applicable à l'achat et à la vente de crypto-monnaies, à savoir l'assujettissement soit au taux forfaitaire de 40,2 % en cas de cession à titre occasionnel, soit au taux marginal pouvant aller jusqu'à 62,2 % au titre du régime des BIC en cas de cession à titre habituel.

2. Un statut expérimental pour les plateformes d'échange

Deux considérations imposent aujourd'hui de réguler les plateformes d'échange : elles sont les principaux points de contact entre le monde crypto le système financier ; elles sont particulièrement vulnérables aux risques de détournement, de blanchiment et d'intégrité de marché.

De nombreuses places de marché régulent d'ores et déjà les plateformes sur la base d'un agrément et d'un régime uniques. C'est notamment le cas de *Bitlicense* dans la juridiction de New York[101]. Le département des services financiers de l'Etat de New York (NY DFS) n'a accordé, à ce jour, que cinq Bitlicenses, dont deux ont été octroyées aux plateformes Ripple et Gemini. Celles-ci ont publiquement souligné les avantages d'une telle régulation reposant sur une licence d'exploitation, qui présente le double avantage de faciliter l'ouverture et le maintien d'une relation d'affaire avec les banques et d'offrir plus largement des garanties aux investisseurs institutionnels souhaitant réaliser des transactions en crypto-monnaies.

[100] Une levée de fonds classique est sans incidence fiscale, seules les plus-values étant taxées lors de leur cession ou transmission.

[101] https://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm et voir annexe n° XX du présent rapport.

Sur le même modèle que la Bitlicense, les autorités de régulation japonaises ont introduit en avril 2017 un système d'agrément unique des plateformes d'échange, ainsi assujetties aux règles de lutte contre le blanchiment de capitaux et le financement du terrorisme, aux obligations d'information loyale et transparente des clients sur les risques encourus, aux règles prudentielles relatives au capital minimum requis (près de 85 000 euros), aux règles de sécurité des systèmes informatiques et des données et à l'obligation d'une conservation distincte des dépôts en cash et de ceux en crypto-monnaies.

Ces règlementations tant new-yorkaise que japonaise, sur des places financières très actives et respectées, tendent de plus en plus à constituer des standards.

Au contraire, l'Union européenne appréhende actuellement chacun des différents métiers réalisés par les plateformes sous le prisme de réglementations et de procédures d'agrément distinctes, ce qui peut s'avérer pénalisant du point de l'attractivité de la place financière.

Ainsi, si une plateforme d'échange de crypto-monnaies détient et contrôle des fonds et si, dans le même temps, elle offre des services d'investissement, il lui faut solliciter deux agréments distincts : celui de prestataire de services de paiement au titre de la directive « DSP 2 » et celui de prestataires de services d'investissement au titre de la directive « MiFID 2 ». À ces deux agréments vient désormais s'appliquer, dans le cadre de la directive 2018/843 de lutte contre le blanchiment et le financement du terrorisme, une procédure d'immatriculation[102].

Ce cadre réglementaire impose donc un choix aux opérateurs de plateformes et aux régulateurs : soit créer pour une même plateforme autant entités juridiques qu'elles exercent de métiers ; soit appliquer indifféremment à toutes les plateformes un régime unique, qui serait la « somme » de tous les régimes existants indépendamment de la réalité des métiers exercés.

Cette dernière option serait très pénalisante. Par exemple, une plateforme ne détenant ni ne contrôlant des fonds n'a pas vocation à se voir imposer le statut de prestataire de services de paiement. En revanche, un socle minimal de règles relatives à l'information loyale et transparente des clients ainsi qu'à la lutte contre le blanchiment et le financement du terrorisme a vocation à s'appliquer dans tous les cas, sans possibilité pour les plateformes considérées de s'en exonérer.

La régulation des plateformes d'échange pourrait donc passer, à court terme, par l'expérimentation à l'échelle nationale d'un statut spécifique portant agrément unique des prestataires de services de crypto-monnaies, les obligations afférentes étant modulées en fonction de la réalité des différents métiers exercés :

- les règles relatives aux établissements de paiement (directive « DSP 2 ») ne s'appliqueraient qu'en cas de détention ou de contrôle des fonds par la plateforme ;
- les règles relatives aux prestataires de services d'investissement (directive « MiFID 2 ») ne s'appliqueraient qu'en cas de transactions sur des instruments financiers à terme portant sur des crypto-actifs ;
- dans tous les cas de figure, les plateformes resteraient assujetties aux règles de lutte contre le blanchiment et le financement du terrorisme ainsi qu'à des règles d'accès, de négociation et de formation des prix transparentes, équitables et non-discriminatoires.

Ce statut expérimental n'a pas vocation à faire concurrence aux statuts et procédures d'agrément existants. Il vise simplement à apporter aux acteurs émergents de la sécurité juridique, sans pour autant graver dans le marbre des contraintes réglementaires trop fortes dans un domaine en perpétuelle évolution.

[102] La directive ne précise pas si cette immatriculation doit se faire sous la forme d'un simple enregistrement ou d'un agrément. En revanche, elle précise que la procédure doit comprendre a minima un examen de la compétence et à l'honorabilité des personnes qui exercent une fonction de direction au sein de ces entités.

De surcroît, ce statut expérimental pour une durée de deux à trois ans aurait vocation à s'effacer à terme devant un statut européen unique, de type « Euro Bitlicense » capable de concurrencer les Bitlicenses new-yorkaise et japonaise. Ainsi, l'expérimentation française doit permettre de préfigurer cette « *Euro Bitlicense* », dont l'ambition doit être de rétablir les conditions d'une concurrence équitable entre États membres et avec les autres grandes places financières. Cet agrément unique européen supposerait des plateformes d'échange le sollicitant qu'elles s'engagent à respecter, au cas par cas, les seules obligations correspondant à la réalité des métiers exercés.

Régime juridique d'une future *Euro Bitlicense*

Si les obligations réglementaires ont vocation à être modulées en fonction des métiers pris en charge par les plateformes, les dispositifs LCB-FT sont incontournables et ont vocation à s'appliquer à l'ensemble des plateformes sollicitant un agrément unique.

Cet agrément les obligerait également à respecter un socle minimal d'exigences en matière de KYC, d'audit et de contrôle interne (en particulier en matière IT face aux risques opérationnels[103]), de réserve de capitaux (ratio *hot/cold wallets*), d'assurance civile professionnelle[104] ainsi que de transparence sur la formation des prix et les frais de transaction.

En revanche, au-delà de ce socle de règles minimales, les autres obligations seraient adaptées, au cas par cas, à la réalité des métiers exercés : statut de prestataire de services de paiement en cas de détention et de contrôle des fonds, règles transparentes et non-discriminatoires en cas de seules activités de négociation.

3. Une approche innovante et pragmatique en matière d'*Initial Coin Offerings* (ICO)

Le potentiel de développement du marché primaire d'émission de *tokens* est encore incertain, en particulier sous l'effet de la place encore importante de la fraude, comme en attestent les récentes actions judiciaires entreprises par le département américain de la justice[105] et l'avertissement lancé par la *Monetary Authority of Singapore* le 24 mai 2018[106].

Alors même qu'il s'agit de produits risqués cumulant plusieurs niveaux d'aléas, le risque d'une classification normative distinguant les jetons financiers ou « *securities* » – conférant des droits aux revenus ou à la décision – des jetons d'utilité ou « *utilities* » - conférant un droit d'usage – est d'offrir *in fine* aux entreprises souhaitant lever des fonds un arbitrage réglementaire entre les normes applicables suivant la nature de l'actif considéré.

[103] Les plateformes doivent, au titre de la Bitlicense, réaliser au moins une fois par un an un test de pénétration de leur système informatique.

[104] Les plateformes pourraient être soumises soit à l'obligation de souscrire à une assurance de sécurité civile professionnelle, soit au respect un ratio minimal de capitaux de réserve (*cold wallet*), dont le volume devrait toujours être supérieur à celui des crypto-actifs détenus en *hot wallet*.

[105] La CFTC, l'autorité de régulation des marchés à terme et des produits dérivés, a demandé à quatre des principales plateformes de crypto-monnaies (Bitstamp, Coinbase, itBit et Kraken) de leur fournir des informations sur des paris concernant l'évolution des prix du bitcoin. Cette requête vise à aider les autorités dans leur enquête sur des manipulations potentielles des cours du bitcoin.

[106] L'autorité monétaire de Singapour a appelé les émetteurs d'ICO à mettre fin à la souscription de jetons numériques sur le territoire de la Cité-État.

La seule approche raisonnable pour le régulateur est pragmatique : il lui revient, en effet, d'analyser chacune des ICO au cas par cas, comme le fait d'ores et déjà la SEC américaine (sur la base du test Howey, 1946). C'est également l'approche que se propose d'adopter l'autorité des marchés financiers (AMF) avec l'instauration d'une procédure de visa optionnel garantissant aux souscripteurs l'intégrité de la démarche présidant à l'ICO ainsi qu'une appréciation au cas par cas de la nature des *tokens* sur la base, d'une part, de l'évaluation approfondie de l'information contenue dans chaque *White Paper* et, d'autre part, de l'identification des prestations restant à fournir ou des biens restant à livrer.

4. La bancarisation des acteurs de la chaîne de valeur de la crypto-finance

Les banques constituent un tiers de confiance important dans la chaîne de valeur de la crypto-finance. L'accès des acteurs de marché aux services de comptes de paiement, conditionne le développement de leur activité. Il est paradoxal que, pour les entrepreneurs français, cet accès soit relativement plus aisé quand ils s'adressent à des banques étrangères.

Les difficultés rencontrées par les acteurs de la crypto-finance sont de deux ordres :

- les acteurs dont l'activité les amène à détenir ou contrôler directement des crypto-monnaies (plateformes d'échanges, émetteurs d'ICO et fournisseurs de « *hot wallets* ») : la bancarisation de ces acteurs exige qu'un dialogue de place s'engage entre eux et l'industrie bancaire. Ce dialogue doit permettre aux banques de mieux discerner les acteurs et le niveau de risque de leur activité. Il a aussi vocation à s'inscrire dans un environnement réglementaire offrant davantage de garanties aux banques grâce à un assujettissement plus large des acteurs aux obligations de lutte contre le blanchiment. Les banques n'auront dès lors plus à assumer seules la responsabilité du respect des règles de connaissance client et de traçabilité des fonds ;
- les acteurs, dont l'activité est indirectement liée aux crypto-monnaies et ne les conduit pas à les détenir ou à les contrôler de manière directe (fournisseurs de « *cold wallets* », entreprises travaillant sur des projets de blockchain, sociétés de conseil dans les crypto-monnaies, par exemple) : le souci de conformité peut conduire certaines banques à refuser l'ouverture d'une relation d'affaire. Leur activité ne présentant pas de risques particuliers tant du point de vue de la sécurité que de la lutte anti-blanchiment, une simple recommandation professionnelle de la fédération bancaire française (FBF) publiée avant la fin de l'été 2018 devrait parvenir à lever tout obstacle.

CONCLUSION : PERSPECTIVES DE LA MONNAIE ET DES PAIEMENTS À L'ÈRE DIGITALE

Les crypto-monnaies visent simultanément : à changer les formes de la monnaie (en la détachant du système bancaire) ; à transformer sa nature (de publique à privée) ; et à révolutionner sa gestion (de centralisée à décentralisée). Cette ambition est grande et, sans doute, peu réaliste. Mais elle répond à une question fondamentale et légitime : comment le progrès technologique affecte-t-il la monnaie ? En particulier, à l'ère digitale, doit-on s'attendre à ce qu'émergent un jour des monnaies privées, peut-être différentes des crypto-monnaies actuelles, mais qui concurrenceront effectivement les monnaies officielles ?

À la lumière de l'histoire, la réponse est négative. Toutes les monnaies privées qui ont existé, parfois longuement depuis le début du XIX^{e} siècle, se sont finalement effondrées sous l'effet de crises de confiance et dans des épisodes de grave instabilité financière et bancaire. Ces crises récurrentes ont conduit à la création des banques centrales contemporaines, qui émettent et contrôlent la monnaie publique, laquelle sert de base au système et assure sa stabilité.

Mais l'histoire est un guide imparfait. La monnaie est une « technologie sociale[107] » : elle résulte d'interactions complexes et changeantes entre la technologie, les habitudes et les conventions. La digitalisation bouleverse ces interactions. Elle transforme nos modes de vie, de déplacement, nos façons de conduire, de travailler, de communiquer, de commercer, pourquoi pas la monnaie ? L'argument le plus puissant des promoteurs des crypto-monnaies est centré sur le *smartphone*. Si chacun peut envoyer instantanément un message dans toute partie du monde, pourquoi ne peut-on pas transférer de la monnaie par cette même voie, avec la même souplesse et la même rapidité ?

La monnaie change de forme : elle est de plus en plus immatérielle et digitale. Mais changera-t-elle de nature ? L'aspiration à des paiements plus rapides et plus souples peut être satisfaite par les systèmes existants, qui utilisent les monnaies officielles. Des progrès considérables ont été réalisés en termes de rapidité, d'efficacité et de coût des paiements de détail.

Mais d'autres scénarios sont possibles. Dans les périodes de changement rapide, un peu de futurologie est nécessaire et légitime. Trois forces se combinent aujourd'hui pour transformer le paysage monétaire et financier :

- la possibilité de stocker et de transférer de la valeur, sous forme digitale, immédiatement et en toute sécurité ;
- l'émergence de réseaux sociaux ou de e-commerce qui rassemblent des centaines de millions de personnes, à travers les frontières ;
- la faculté, pour chacun, de gérer directement et instantanément ses finances à partir d'applications dédiées sur terminal mobile, par exemple en convertissant de l'épargne financière (comptes et portefeuilles boursiers) en monnaie ou inversement.

Conjointement ou séparément, ces forces peuvent transformer l'architecture ou la nature des paiements comme de la monnaie. En particulier, les questions suivantes se posent : comment ces forces vont-elles affecter la détention d'espèces ? Comment vont-elles affecter le système financier ? Comment vont-elles affecter la monnaie ?

[107] Jon Cunliffe.

Quel avenir pour la monnaie fiduciaire ?

Une première question concerne l'avenir des paiements en espèces ou, pour parler familièrement, du cash :

- ces paiements en espèces sont directement affectés par la digitalisation de la monnaie et le développement accéléré, dans de nombreux pays avancés et émergents (en premier lieu, la Chine), des paiements par terminaux mobiles, y compris pour les plus petits montants ;
- l'élimination du cash est un objectif affiché des grands systèmes de paiements ;
- les autorités elles-mêmes considèrent la monnaie fiduciaire avec méfiance. La règlementation contraint de plus en plus les paiements en espèces pour lutter contre le blanchiment d'argent, la fraude, les activités criminelles et le financement du terrorisme ;
- néanmoins, l'utilisation du cash se maintient : si le stock de billets augmente, sa part dans le volume des paiements diminue. Les observations et enquêtes montrent, en effet, que le cash est principalement apprécié comme réserve de valeur, notamment dans les pays où subsiste le souvenir de la crise bancaire et financière de 2008-2009.

Si, en toute hypothèse, le cash venait à disparaître, tous les paiements s'effectueraient en monnaie digitale, et les citoyens perdraient tout accès à la monnaie publique de banque centrale[108]. Seule la monnaie émise par des institutions privées – les banques et, le cas échéant, les systèmes de paiements – leur seraient disponibles. Il est difficile de prévoir les conséquences d'une telle évolution sans précédent dans l'histoire contemporaine :

- d'un point de vue politique, la disparition du souverain en tant que signe monétaire visible ne serait probablement pas neutre (on se souvient des débats intenses qui ont marqué la création des billets en euros) ;
- la stabilité des systèmes monétaires repose sur la conviction, ancrée en chacun des déposants, que les avoirs bancaires (ou disponibles sur un terminal mobile) sont instantanément et inconditionnellement convertibles en monnaie publique. Même si cette option est de plus en plus rarement exercée, elle reste fondamentale. Avec la disparition des billets, il n'existerait aucun support pour effectuer cette conversion ;
- enfin, la dématérialisation totale de la monnaie exposerait l'ensemble de l'économie à un gigantesque « risque opérationnel », si des catastrophes humaines ou naturelles venaient à perturber ou détruire les systèmes qui supportent la circulation de la monnaie digitale.

Ces considérations pourraient justifier, de la part des banques centrales, la création d'une nouvelle monnaie digitale publique. Le débat sur cette question est ouvert depuis l'apparition des crypto-monnaies. Mais il est compliqué par des considérations multiples, qui portent sur l'efficacité de la politique monétaire et la structure du système financier. Spécifiquement :

- certains analystes et responsables y voient l'opportunité de renforcer les mécanismes de transmission de la politique monétaire en payant un intérêt (positif ou négatif) sur la nouvelle monnaie publique digitale. Mais alors, celle-ci entrerait directement en concurrence avec les dépôts bancaires, déstabilisant toute l'intermédiation financière et compromettant la distribution du crédit ;
- d'autres observateurs considèrent une telle « désintermédiation » des banques comme bénéfique. Ceux-là plaident depuis longtemps pour que soit retiré aux banques le pouvoir de création monétaire et que l'émission de monnaie soit réservée à la puissance publique. C'est l'esprit de l'initiative récente de « monnaie souveraine » en Suisse ou, dans le monde anglo-saxon, des propositions de « *narrow banking* ».

[108] Celle-ci étant dorénavant constituée uniquement des réserves des banques.

Ces débats sont importants, mais relativement indépendants. Il est possible, si on le souhaite, de les contourner en créant une monnaie digitale de banque centrale qui reproduise exactement les caractéristiques des billets, c'est-à-dire (1) ne portant pas intérêt et (2) ne nécessitant pas l'ouverture d'un compte. Les ménages auraient ainsi accès, comme aujourd'hui, à la monnaie publique, dans des formes adaptées à leurs aspirations et au progrès de la technologie.

Les autorités devraient toutefois opérer un choix important : cette monnaie publique digitale serait-elle, comme les billets actuels, anonyme ou, au contraire, traçable à l'instar des actuels virements bancaires ou paiements électroniques ? Les deux sont techniquement possibles, mais correspondent à des visions opposées sur les rapports entre monnaie et protection de la vie privée. C'est un mérite des crypto-monnaies que de conduire à débattre et expliciter de tels choix.

Les systèmes de paiements et la monnaie

Une autre évolution se dessine : la transformation des grands systèmes de paiement en conglomérats rassemblant, dans un même écosystème, les fonctions de banque, de e-commerce et de gestion d'actifs.

Cette transformation répond à une demande : il peut être attractif, pour les ménages et les entreprises, de détenir la monnaie sur un terminal électronique, sans rattachement nécessaire à un compte bancaire – particulièrement si chacun peut, à partir d'une application disponible vingt-quatre heures sur vingt-quatre, transformer en permanence son épargne en monnaie et réciproquement.

Dans ce schéma, les utilisateurs finaux voient seulement des unités de valeur digitales stockées sur leurs terminaux mobiles[109]. Les systèmes de paiement se situent en intermédiaires entre ces utilisateurs et les banques, où ils détiendraient des comptes globaux. Même si les paiements et avoirs restent libellés en monnaie officielle, cette transformation emporterait des conséquences extrêmement fortes sur l'intermédiation financière, les coûts de financement des banques, leurs relations avec les systèmes de paiement, la supervision de ceux-ci et la distribution du crédit.

Elle soulèverait en particulier trois enjeux pour les politiques publiques :

- comment superviser et réguler de tels conglomérats ? Outre la surveillance des systèmes de paiements, des licences bancaires devront être imposées. Les politiques de la concurrence devront être adaptées pour assurer l'interopérabilité des réseaux et éviter l'apparition de monopoles naturels ;
- comment protéger les données privées ?
- comment assurer l'efficacité de la politique monétaire ?

Celle-ci repose aujourd'hui sur le monopole des banques centrales dans l'émission de la monnaie publique. C'est en fixant le taux d'intérêt auquel cette monnaie est prêtée ou rémunérée que les banques centrales conduisent la politique monétaire. Mais, dès lors que les paiements s'effectueront majoritairement à l'intérieur de grands réseaux connectés, le besoin d'une telle monnaie diminuera, ce qui peut affaiblir leur pouvoir.

Les mêmes inquiétudes s'étaient manifestées, il y a vingt ans, lors de l'introduction des monnaies électroniques. Elles ne se sont pas concrétisées. En effet, la monnaie de banque centrale remplit deux fonctions essentielles : c'est d'abord l'instrument ultime de paiement ; mais c'est aussi la réserve ultime de valeur. La première fonction est peut-être menacée, mais pas la seconde. Au contraire, la demande d'actifs « sûrs » est en forte croissance dans les économies modernes. En fixant comme elles le font actuellement, le taux d'intérêt sans risque attaché à la monnaie qu'elles émettent, les banques centrales sont assurées de continuer à influencer puissamment les conditions monétaires et financières dans l'ensemble de l'économie.

[109] C'est le système opéré aujourd'hui par M-Pesa.

Des monnaies privées centralisées ?

Des paiements à la monnaie, il n'y a souvent qu'un pas. Une étape supplémentaire dans la transformation technologique et monétaire peut être franchie, si un grand réseau organise ses opérations autour d'une nouvelle unité de compte interne, une véritable monnaie privée, dont il contrôlera l'émission. Cela s'avère, dans un avenir proche, techniquement et économiquement possible.

D'un point de vue technique, rien ne s'oppose à la création de nouvelles monnaies à des fins de paiement à l'intérieur d'un réseau. Des expériences ont d'ores et déjà été tentées avec des monnaies spécialisées, au sein d'espaces géographiques plus ou moins restreints : jeux vidéo, systèmes de crédit (Facebook), attributions de bonus sous forme digitale. Dès lors que la gestion est centralisée (contrairement aux crypto-monnaies), il est possible de bénéficier de tous les avantages de la digitalisation en termes de souplesse, de réactivité et d'indépendance vis-à-vis des banques.

D'un point de vue économique, les réseaux et la monnaie ont une proximité naturelle. La monnaie est un phénomène de réseau, car elle existe pour faciliter les transactions entre les individus. Plus le réseau est large, plus l'adoption de la monnaie en son sein lui confère stabilité et valeur. La différence est grande avec les monnaies privées du XIX^{e} siècle qui voyaient leur influence limitée par les distances et les obstacles physiques. Aujourd'hui, une monnaie privée pourrait instantanément accéder à plusieurs centaines de millions d'individus qui, si leurs échanges sont suffisamment intenses, forment *de facto* une quasi-zone monétaire. Dès lors que les participants auraient pris l'habitude, pour une partie de leurs opérations, d'utiliser l'unité de compte interne, celle-ci gagnerait progressivement une acception élargie, voire universelle. Dans cette phase extrême d'évolution, l'économie digitale peut créer une concurrence nouvelle entre monnaies privées et publiques, réalisant ainsi le rêve de Hayek d'une « dénationalisation » des monnaies.

Néanmoins, le facteur technologique ne peut à lui seul suffire à bouleverser les régimes monétaires. L'instabilité naturelle des monnaies privées ne disparaîtra pas nécessairement sur des réseaux larges. Des monnaies privées seront confrontées à trois difficultés incontournables :

- comment organiser une « offre élastique », ce qui est l'objectif (et, dans certains pays, le mandat) des monnaies officielles ? La régulation par algorithme, aussi sophistiquée soit-elle, est à cet égard trop rigide et le recours au seul jugement humain peut, pour une monnaie privée, ne pas suffire à établir la confiance ;
- comment organiser le crédit ? C'est une composante essentielle de tout système monétaire. Une monnaie privée sans crédit est possible, mais ramenée à sa seule fonction de paiement verra son développement limité. Elle obligerait les agents économiques à supporter un risque en s'endettant dans une monnaie différente de celle de leurs paiements. Une monnaie privée avec crédit est, pour sa part, exposée au risque de transformation de maturité et d'illiquidité des intermédiaires, auquel il est impossible de faire face sans un prêteur en dernier ressort ;
- Comment gérer le taux de change ? Un régime de flottement pur laisserait les participants très exposés au risque de change, si leurs revenus sont libellés en monnaie officielle. Un régime de fixité devrait être assis sur des « réserves » et exposerait le système privé à des attaques.

Ces trois problèmes ont en commun qu'ils sont aujourd'hui résolus (parfois très difficilement) par la mobilisation d'une monnaie publique, elle-même assise sur des ressources publiques et le pouvoir du souverain. Un opérateur privé, qui tenterait d'y faire face avec ses propres ressources, si importantes soient-elles, mettrait sérieusement en risque sa propre solvabilité.

Pour ces raisons, les banques centrales resteront probablement indispensables et pourront défendre ou imposer leur monnaie comme unité de compte (sans parler de la force légale que mobilise le souverain).

Néanmoins, la digitalisation et les réseaux favorisent une déconnection des espaces géographique et monétaire. On ne peut exclure que des monnaies privées s'imposent en dehors de leur juridiction d'origine ou que les grands systèmes de paiement servent indirectement à l'internationalisation des principales monnaies officielles, dont la diffusion et l'utilisation se répandraient au-delà de leurs frontières.

RÉFÉRENCES

Abadi J and M Brunnermeier, (2018), « Blockchain Economics », https ://www.bis.org/events/confresearchnetwork1803/Brunnermeier_pres.pdf

Abraham, M, (2017), « Publication de l'ordonnance « blockchain »« , bitcoin.fr

All, R, J Barrdear and R Clews, (2014), « Innovations in payment technologies and the emergence of digital currencies », Quaterly Bulletin 2014 Q3

Allouch, N., (2015), « On the private provision of pubilc goods on networks », Journal of Economic Theory 157 527-552

Al-Naji N, and J Chen, (2018), « Basecoin Whitepaper », https ://basis.io/basis_whitepaper_en.pdf

Andolfatto, D., (2018), « Blockchain : What It Is, What It Does, and Why You Probably Don't Need One », https ://files.stlouisfed.org/files/htdocs/publications/review/2018/04/16/blockchain-what-it-is-what-it-does-and-why-you-probably-dont-need-one.pdf

Azouvi, S, M Maller and S Meiklejohn, (2015), « Egalitarian Society or Benevolent Dictatorship : The State of Cryptocurrency Governance », University College London

Bacon, J, J David Michels, C Millard and J Singh, (2017), « Blockchain Demystified », Queen Mary University of London, School of Law

Barrdear, J and M Kumhof, (2016), « The macroeconomics of central bank issued digital currencies », Bank of England, Staff Working Paper No. 605

Barthelemy J, and E Mengus, (2018), « Nominal Anchoring, Disanchoring and Re-Anchoring : The Role of Credibility »

Bech, M and R Garratt, (2017), « Central bank cryptocurrencies », BIS Quarterly Review, BIS, Annual Report, September, 2017.

Bech, M, Y Shimizu and P Wong, (2017), « The quest for speed in payments », BIS Quaterly Review, BIS, Annual Report, December 2017

Berentsen, A, (2006), « On the private provision of fiat currency », European Economic Review 50

Berentsen, A and F Schär, (2018), « A Short Introduction to the World of Cryptocurrencies », Federal Reserve Bank of St. Louis Review, First Quarter 2018, 100(1), pp. 1-16

Berentsen, A., (2018), « The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies », St Louis Federal Reserve

Bergstrom T, L Blume and H Varian, (1984), « On the private provision of public goods », Department of Economics, University of Michigan

Blummont, D., (2016), « Blocking the future ? The regulation of distributed ledgers », Faculty of Law, Victoria University of Wellington

Böhme R, N Christin, B Edelman and T Moore, (2015), « Bitcoin : Economics, Technology and Governance », Journal of Economic Perspectives - Volume 29, Number 2

Bolt, W and M R.C. van Oordt, (2016), « On the Value of Virtual Currency », Bank of Canada Working Paper 2016-42

Bonneau J, A Miller, J Clark, A Naranayan, J A. Kroll and A W. Felten, (2015), « SoK : Research Perspectives and Challenges for Bitcoin and Cryptocurrencies », https ://www.ieee-security.org/TC/SP2015/papers-archived/6949a104.pdf

Bordo, M and A Levin, (2017), « Central Bank Digital Currency and the Future of Monetary Policy », National Bureau of Economic Research, Working Paper No. 23711

Brennan C, B Zelnick and M Yates, (2018), « Cryptocurrencies are only the beginning », Credit Suisse

Brown, A., (2017), « CME's Bitcoin Foray Has Three Plausible Outcomes », CME Group

Buiter, W, (2014), « Gold : a six thousand year-old bubble revisited », Citi Research, Global Economic View

Buterin V., (2014), « Toward a 12-second Block Time »

Buterin V., (2016), « Ethereum Whitepaper »

Carney, M., (2018), « The Future of Money », BIS central bankers' speeches

Carstens, A, (2018), « Money in the digital age : what role for central banks ? », House of Finance, Goethe University, Lecture

Casey, M, Crane, J, Gensler, G, Johnson, S, Narula, N, (forthcoming), « The Potential Impact of Blockchain Technology on Finance : Small, Significant, or Completely Transformative ? », ICMB, Geneva Report

Chepurnoy, A., (2016), « Interactive Proof of Stake »

Chiu, J and T Wong, (2014), « E-Money : Efficiency, Stability and Optimal Policy », Bank of Canada Working Paper 2014-16

Clayton, J, (2017), « Statement on Cryptocurrencies and Initial Coin Offerings », Public Statement

Cochrane, J, (2014), « Toward a run-free financial system »

Commodity Futures Trading Commission, (2017), « A CFTC Primer on Virtual Currencies », LabCFTC

Consensy, (2018), « Blockchain vs. Distributed Ledger Technologies »

CPMI, (2005), « New developments in large-value payment systems », Bank for International Settlements

CPMI, (2014), « Non-banks in retail payments », Bank for International Settlements

CPMI, (2015), « Digital currencies », Bank for International Settlements

CPMI, (2017), « Distributed ledger technology in payment, clearing and settlement », Bank for International Settlements

CPMI, (2018), « Central bank digital currencies », Bank for International Settlements

CPMI, (1996), « Implications for Central Banks of the Development of Electronic Money », Bank for International Settlements

CPMI, (2018), « Cross-border retail payments », Bank for International Settlements

Cyprys, M, Z N Feierstein, B L. Graseck and J E Faucette, (2017), « Will Bitcoin Futures on CME & CBOE Open the Door for Discount Brokers ? », Morgan Stanley Research

De Vauplane, H., (2018), « Crypto-assets, Token, Blockchain, ICO : un nouveau monde ? », Medium

Dowd, K, (2014), « New Private Monies : A Bit-Part Player ? », The Institute of Economic Affairs

Dr. Hacker, P, and Dr. C Thomale, (2017), « Crypto-Securities Regulation : ICOs, Token Sales and Cryptocurrencies under EU Financial Law », Yale University

Dwyer, G, (2014), « The economics of Bitcoin and similar private digital currencies », Journal of Financial Stability 17 (2015) 81 - 91

ESMA, (2016), « The Distributed Ledger Technology Applied to Securities Markets"

European Banking Authority, (2014), « EBA Opinion on « virtual currencies »« , Op/2014/08

European Central Bank, (2012), « Virtual Currency Schemes »

European Central Bank, (2015), « Virtual currency schemes – a further analysis »

European Central Bank, (2017), « Impact of digital innovation on the processing of electronic payments and contracting : an overview of legal risks », Legal Working Paper Series

Eyal I and E Gün Sirer, (2013), « Majority is not enough : Bitcoin Mining is Vulnerable », Department of Computer Science, Cornell University

Eyal, I, and E Gün Sirer., (2014), « Bitcoin : Concepts, Practice, and Research Directions », Department of Computer Science, Cornell University

Fanusie, Y and T Robinson, (2018), « Bitcoin Laundering : An Analysis of Illicit Flows into Digital Currency Services », Elliptic, Center on Sanctions & Illicit Finance

Faucette, J, B L. Graseck, V Govil and D Hussain, (2017), « Bitcoin, Ethereum, XRP : Decrypted ! Takeaways », Morgan Stanley Research

Fernandez-Villaverde, J and D Sanches, (2017), « Can Currency Competition Work ? », National Bureau of Economic Research, Working Paper No. 22157

Financial Action Task Force, (2014), « Virtual Currencies : Key Definitions and Potential AML/CFT Risks »

Financial Conduct Authority, (2017), « Discussion Paper on distributed ledger technology », DP17/3

Fischer, M, Lynch, N, and Paterson, M, (1985), « Impossibility of distributed consensus with one faulty process »,, Journal of the Association for Computing Machinery

Fischer, S, (1986), « Friedman versus Hayek on Private Money », Journal of Monetary Economics 17 (1986) 433-439. North-Holland

Fung, B, M Molico and G Stuber, (2014), « Electronic Money and Payments : Recent Developments and Issues », Bank of Canada Working Paper 2014-2

Fung, B, S Hendry and W E. Weber, (2017), « Canadian Bank Notes and Dominion Notes : Lessons for Digital Currencies », Bank of Canada Working Paper 2017-5

Gans, J and H Halaburda, (2013), « Some Economics of Private Digital Currency », Bank of Canada Working Paper 2013-38

Gazi, P, A Kiayias, and A Russell, (2018), « Stake-Bleeding Attacks on Proof-of-Stake Blockchains »

Glazer, P., (2018), « The Bitcoin Scaling Debate : Context, Proposed Solutions, and the Future », Berkeley

Glazer, P., (2018), « An Explanation of Cryptocurrency Forks », Berkeley

Greenspan, G, (2016), « Blockchains vs centralized databases », Multichain blog

Greenspan, G, (2017), « The Blockchain Immutability Myth »

Grym, A, P Heikkinen, K Kauko and K Takala, (2017), « Central bank digital currency », Bank of Finland, Economic Review

Hayek, F.A., (1990), « Denationalization of Money : The Argument Refined », The Institute of Economic Affairs

He, D, K Habermeier, R Leckow, V Haksar, Y Almeida, M Kashima, N Kyriakos-Saad, H Oura, T Saadi Sedik, N Stetsenko and C Verdugo-Yepes, (2016), « Virtual Currencies and Beyond : Initial Considerations », IMF Staff Discussion Note

He, D, R Leckow, V Haksar, T Mancini-Griffoli, N Jenkinson, M Kashima, T Khiaonarong, C Rochon and H Tourpe, (2017), « Fintech and Financial Services : Initial Considerations », IMF Staff Discussion Note

Hendrickson J, T L. Hogan and W J. Luther, (2016), « The Political Economy of Bitcoin » Economic Enquiry Vol. 54, No. 2, 925-939

Hilleman, G and M Rauchs, (2017), « Global cryptocurrency benchmarking study », Cambridge Centre for Alternative Finance

IMF, (2018), Global Financial Stability Report, chapter 1.

Issing, O, (1999), « Hayek – currency competition and European monetary union », Text of the Annual Hayek memorial lecture

Jack, W and T Suri, (2011), « Mobile Money : the Economics of M-Pesa », National Bureau of Economic Research, Working Paper No. 16721

Kasireddy, P., (2017), « How does Ethereum work, anyway ? », Medium

Koenig, JP, (2018), « Critiquing the Carney critique on central bank digital currency »

Krugman, P, and M Obstfeld, (1987), « International Economics : Theory and Policy », Chapter 14 : Money, Interest Rates and Exchange Rates

Kumar A, and C Smith, (2017), « Crypto-currencies - An introduction to not-so-funny moneys », Reserve Bank of New Zealand Analytical Notes

Lamport, L, R Shostak and M Pease, (1982), « The Byzantine Generals Problem », SRI International

Lewis, A., (2018), « What is Ripple ? », Medium

Loeys, J and al, (2018), « Decrypting Cryptocurrencies : Technology, Applications and Challenges », JP Morgan Research

Lowe, P, (2017), « An eAUD ? », BIS central bankers' speeches

Ludwigs, A and C Brenig, (2016), « Transparency through Decentralized Consensus : The Bitcoin Blockchain and Beyond », Freiburgh University

Luther, W and J Olson, (2014), « Bitcoin is Memory », George Mason University, Institute of Human Studies

Luther W, and L H. White, (2014), « Can Bitcoin Become a Major Currency ? », George Mason University, Department of Economics, Working Paper No. 14-17

Ma J, J S. Gans and R Tourky, (2018), « Market Structure in Bitcoin Mining », National Bureau of Economic Research, Working Paper No. 24242

Macdonald T, D Allen and J Potts, (2016), « Blockchain and the Boundaries of Self-Organized Economics : Predictions for Future Banking », School of Economics, Finance & Marketing, RMIT University, Melbourne, Australia

Marimon, R, J Pablo Nicolini and P Teles, (2012), « Money is an experience good : Competition and trust in the private provision of money », Journal of Monetary Economics 59 (2012) 815 - 825

McAndrews, J, (2017), « The Case for Cash », ADBI Working Paper Series, No. 679

McLean, S and S Deane-Johns, (2016), « Demystifying Blockchain and Ditributed Ledger Technology – Hype or Hero ? » , Morrison &Foerster, client alert

Menon, R, (2018), « Crypto-tokens - the good, the bad, and the ugly », Speech, Singapore Monetary Auhtority

Mersch, Y, (2017), « Digital Base Money – an assessment from the European Central Bank's perspective », BIS central bankers' speeches

Mersch, Y, (2018), « Virtual currencies ante portas », BIS central bankers' speeches

Multichain blog, (2017), « A rational take on cryptocurrencies »

Nakaso, H, (2014), « Toward innovative payment and settlement systems », BIS central bankers' speeches

Naranayan A and J Clark, (2017), « Bitcoin's Academic Pedigree : the concept of cryptocurrencies is built from forgotten ideas in research literature »

Naranayan A and M Möser, (2017), « Obfuscation in Bitcoin : Techniques and Politics », Princeton University

Narula, N., (2017), « Cryptographic vulnerabilities in IOTA », Medium

Nash, J, (2002), « Ideal Money », Southern Economic Journal, published by Southern Economic Association

Nicolaisen, J, (2017), « Challenges for the payment system », BIS central bankers' speeches

Nicolaisen, J, (2017), « What should the future form of our money be ? », BIS central bankers' speeches

Perlaky, A, JC Artigas, A Hewitt, and J Reade, (2018), « Investment Update : Cryptocurrencies are no subsitute for gold », World Gold Council

Pfeffer, J, (2017), « An (Institutional) Investor's Take on Cryptoassets », Medium

Pfeffer, J, (2018), « Doubts about the Long-Term Viability of Utility Cryptoassets », Medium

Pfister, C, (2017), « Monetary Policy and Digital Currencies : Much Ado about Nothing ? », Banque de France working paper #642

Poelstra, A, (2015), « On Stake and Consensus »

Poelstra, A, (2014), « Distributed Consensus from Proof of Stake is Impossible »

Poloz, S, (2017), « Three things keeping me awake at night », BIS central bankers' speeches

Popov, S, (2017), « The Tangle - IOTA Whitepaper »

Potter, S, (2018), « The supply of money-like assets », BIS central bankers' speeches

Prasad, E, (2018), « Central Banking in a Digital Age : Stock-Taking and Preliminary Thoughts »

Pruneet, Er. Deepika and Er. R Kaur, (2017), « Cryptocurrency : Trends, Perspectives and Challenges », Computer Science and Engineering Department, Chandigargh University, India

Raskin, M and D Yermack, (2016), « Digital Currencies, Decentralized Ledgers, and the Future of Central Banking », National Bureau of Economic Research, Working Paper No. 22238

Rogaway, P,(2015), « The Moral Character of Cryptographic Work »,Department of Computer Science, University of California

Rogoff, K, (2014), « Costs and benefits to phasing out paper currency », NBER Macroeconomics Annual Conference

Rosic, A , (2017), « Proof of Work vs Proof of Stake : Basic Mining Guide », Blockgeeks blog

Samuelson, P, (1958), « An Exact Consumption-Loan Model of Interest with or without the Social Contrivance of Money », The Journal of Political Economy, Vol. 66, No. 6. (Dec., 1958), pp. 467-482

Schilling, L, and H Uhlig, (2018), « Some Simple Bitcoin Economics », National Bureau of Economic Research, Working Paper No. 24483

Schnabel, I and H Song Shin, (2018), « Money and trust : lessons from the 1620s for money in the digital age », BIS Working Papers, No. 698

Schwartz, D, N Youngs and A Britto, (2014), « The Ripple Protocol Consensus Algorithm », Ripple Labs, Inc

Sebastian, J, (2017), « Central banks-issued digital currencies : a challenge to the financial system », Dinario Expansion (Spain) press article

Selgi, G, (2014), « Synthetic commodity money », Journal of Financial Stability 17 (2015) 92 - 99

Sompolinsky Y, A Zohar, (2013), « Accelerating Bitcoin's Transaction Processing - Fast Money Grows on Trees, Not Chains »

Sompolinsky Y, A Zohar, (2015), « Secure High-Rate Transaction Processing in Bitcoin »

Stevens, A, (2017), « Digital currencies : threats and opportunities for monetary policy », National Bank of Belgium, Economic Review

Stinchcombe, K, (2017), « Ten years in, nobody has come up with a use for blockchain », Hackernoon

Sveridges Riksbank, (2017), « The Riksbank's e-krona project »

Swissborg, (2018), « Terms of CHSB Token Sale »

Tirole, J, (1985), « Asset Bubbles and Overlapping Generations », Econometrica, Vol. 53, No. 6. 5nov., 1985), pp. 1499-1528

Tullock, G, (2018), « Competing Monies », Ohio State University Press

Tulpule, A, (2017), « Enforcement and Compliance in a Blockchain(ed) World », CPI Antitrust Chronicle

Velde, F, (2013), « Bitcoin : A primer », Chicago Fed Letter

Velde, F, (2017), « Technological Change and the Future of Cash », SUERF Policy Note n° 15

Volkswirtschaftliche Gesellschaft, Z., (2018), « How money is created by the central bank and the banking system », Swiss National Bank, Speeches

Walport, M, (2015), « Distributed Ledger Technology : beyond block chain », UK Government Office for Science

Weber, W, (2015), « Government and Private E-Money-Like Systems : Federal Reserve Notes and National Bank Notes », Bank of Canada Working Paper 2015-18

Weidmann, J, (2018), « Opening remarks - Fourth cash symposium of the Deutsche Bundesbank », Opening remarks at the Fourth Cash symposium of the Deutsche Bundesbank, Frankfurt

Whiterspoon, Z, (2013), « A Hitchhiker's Guide to Consensus Algorithms »

Williamson, S, (2002), « Private Money and Counterfeiting », Federal Reserve Bank of Richmond Economic Quaterly Volume 88/3

Woodford, M, (2000), « Monetary Policy in a World without Money », working paper n° 7853

Woodford, M, (2001), « Monetary Policy in the Information Economy »

Yermack, D, (2013), « Is Bitcoin a Real Currency ? An Economic Appraisal », National Bureau of Economic Research, Working Paper No. 19747

(2018), « WTF is $XRP ? », Medium

(2016), « Fast payments – Enhancing the speed and availability of retail payments », Bank for International Settlements (CPMI)

(2018), « CoinPoker Whitepaper »

(2018), « Telegram Whitepaper »

(2017), « We Power Whitepaper »

ANNEXES

ANNEXE N°1 : PERSONNES RENCONTRÉES

1. Administrations publiques

Ministère de l'Économie et des Finances

M. Emmanuel Monnet, conseiller financement de l'économie au cabinet du Ministre,

M. Sébastien Raspiller, chef du service du financement de l'économie, direction générale du Trésor,

M. Guillaume Chabert, chef du service des affaires multilatérales et du financement, direction générale du Trésor,

M. Didier Gautier, chef du service national des enquêtes, direction générale de la consommation et de la répression des fraudes,

M^{me} Nadine Mouy, Sous-Directrice des services et des réseaux, direction générale de la consommation et de la répression des fraudes,

M. Nicolas Dupas, inspecteur des finances.

Cour des comptes

M. Mohammed Adnène Trojette, conseiller référendaire, secrétaire général adjoint,

M. Yorick de Mombynes, conseiller référendaire.

Caisse des dépôts et consignations (CDC)

M. Olivier Sichel, directeur général adjoint,

M^{me} Nadia Filali, Head of Blockchain Programmes & LaBChain.

Agence nationale des normes comptables (ANC)

M. Patrick de Cambourg, président,

M. Jean-Gil Saby, Deputy Chief Financial Officer, BNP Paribas,

M. Hervé Thiery, chef de projet.

Tracfin

M. Bruno Dalles, directeur,

M. Jocelyn Lelong, analyste, cellule d'analyse stratégique.

Cyberdouane

M. Nicolas Milhou, chef de la division veille et analyse stratégique.

US Treasury

M. Daniel Greenland, International Economist – Office of International Financial Market.

2. Autorités nationales de régulation et de supervision

Banque de France

M. François Villeroy de Galhau, gouverneur,

M^me^ Emmanuelle Assouan, directrice des systèmes de paiement et des infrastructures de marché.

Autorité de contrôle prudentiel et de résolution (ACPR)

M. Jean-Claude Huyssen, directeur des agréments, des autorisations et de la réglementation,

M^me^ Nathalie Beaudemoulin, directrice du pôle FinTech.

Autorité des marchés financiers (AMF)

M. Robert Ophèle président,

M. Franck Guiader, Head FinTech, Innovation and Competitiveness,

M. Domitille Dessertine, Deputy Head FinTech, Innovation and Competitiveness.

3. Autorités étrangères et internationales de régulation et de supervision

Federal Reserve Bank of New York (FED)

M. Antoine Martin, Senior Vice President,

M. Morgan Macdonald, Senior Counsel Office of International Affairs.

Commodity Futures Trading Commission

M. Jason A. Mahoney, Esq., Special Counsel,

M. Jorge Herrada, Senior Technical Data Specialist,

M. Brian S. Trackman, Counsel on FinTech and Innovation.

Board of Governors of the Federal Reserve System

M. David Mills, Deputy Associate Director – Division of Reserve Bank Operations and Payment Systems,

M^me^ Julia J. Philipp, Senior Supervisory Financial Analyst – Division of Banking Supervision and Regulation.

International Monetary Fund (IMF)

M. Ross Leckow, Deputy General Counsel – Legal Department,

M. Tanai Khiaonarong, Senior Financial Sector Expert – Central Bank,

M. Christophe Waerzeggers, Senior Counsel – Financial and Fiscal Law Unit – Legal Department,

M^me^ Jess Cheng, Counsel – Financial and Fiscal Law Unit – Legal Department.

Bank of International Settlements (BIS)

M. Raphael Auer, Senior Economist – Monetary and Economics Department,

M. Egemen Eren, Economist – Monetary and Economic Department,

M. Takeshi Shirakami, Deputy Head of the CPMI Secretariat.

European Securities and Markets Authority **(ESMA)**

M^{me} Anne Choné, senior risk analysis officer – innovation and product team.

4. Personnalités qualifiées et représentants d'intérêts

Fédération Bancaire Française (FBF)

M. Benoît de la Chapelle Bizot, directeur général délégué,

M^{me} Pauline Guérin, Senior Advisor Investment and Merchant Banking.

Cabinet Kramer Levin

M. Hubert de Vauplane, avocat associé.

5. Entreprises

Neurochain

M. Frédéric Goujon, co-fondateur et CEO,

M. Renaud Roquebert, avocat à la Cour, associé gérant.

ACinq

M. Pierre-Marie Padiou, co-fondateur et CEO.

Mazars

M^{me} Stéphanie Latombe, associée Capital Markets.

PwC

M. Marc Ripault, directeur.

Solid

Pierre Paperon, Co-fondateur et CEO.

SGH Capital

M. Alexandre Azoulay, associé-gérant.

Blockchain.io

M. Pierre Noizat, co-fondateur et CEO.

Le Cercle du Coin

M. Jacques Favier, membre fondateur et secrétaire.

Avolta Partners

M. Philippe Rodriguez, managing partner,

M^{me} Éléonor Lasou, consultante.

Ledger

M. Éric Larchevêque, fondateur et CEO,

M. Jean Michel Pailhon, vice-président, corporate development & strategy,

M^{me} Nathalie de Gaulle, directrice, affaires gouvernementales et banques centrales.

Association française de gestion des crypto monnaies (AFGC)

M. Charlie Méraud, président.

Blockchain Partners

M. Alexandre Stachtchenko, co-fondateur, directeur général,

M. Antoine Yeretzian, co-fondateur, directeur partenariats et développement,

M. Clément Jeanneau, cofondateur, directeur contenu et communication,

M. William O'Rorke, conseiller juridique.

Coinhouse

M. Nicolas Louvet, CEO,

M. Manuel Valente, directeur,

M^{me} Sandrine Lebeau, compliance officer.

Booking Token Unit Protocol

M. Hervé Hababou, président,

M. Vidal Chriqui, ERC-808 inventor.

iEx.ec

M. Gilles Fedak, président,

M. Jean-Charles Cabelguen, chief innovation & adoption.

Consensys

M. Ken Timsit, Managing Director,

M. Jérôme de Tychey, Blockchain Tech Lead & Key Account Manager.

Tobam

Yves Choueifaty, président.

Ark Ecosystem

M. François Xavier Thoorens, Co-fondateur et CEO.

JP Morgan

M^{me} Joyce Chang, Managing Director,

M. Alexander Roever, CFA, Managing Director.

Gemini

M^{me} Sarah Olsen, Head of Business Development,

M. Michael Breu, Chief Compliance Officer.

Davis Polk

M. Joseph A. Hall, partner, Corporate Department and head of the firm's corporate governance practice.

Legolas Exchange

M. Frédéric Montagnon, co-fondateur & CEO.

Ripple

M. Ryan Zagone, Director of Regulatory Relations.

ANNEXE N° 2 : GLOSSAIRE

Algorithme de consensus : protocole par lequel les nœuds d'un réseau blockchain arrivent à un consensus pour valider les transactions ou d'autres engagements sur la chaîne de blocs. Les algorithmes de consensus les plus souvent employés par les blockchains sont les systèmes de preuve de travail ou « *Proof of Work* » (PoW) et de preuve d'enjeu ou « *Proof of Stake* » (PoS).

Bloc : composant principal de la blockchain, un bloc est un regroupement de plusieurs transactions effectuées par les utilisateurs du réseau. Dans le cas de Bitcoin, la création d'un nouveau bloc est faite par les mineurs qui résolvent des calculs compliqués et vérifient les transactions du bloc. Sur la blockchain Bitcoin, un nouveau bloc est créé toutes les dix minutes. La blockchain Ethereum a un temps de validation plus court.

Blockchain : technologie permettant à un réseau de stocker et d'échanger de l'information, ainsi que de la valeur dans la mesure où les tokens émis y sont toujours adossés, sur un registre partagé. Elle est transparente, horodatée, sécurisée, immuable et fonctionne sans organe central de contrôle. Elle peut s'appréhender comme une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Chaque transaction est validée par un protocole de consensus, de manière irréversible.

Blockchain publique : blockchain ouverte à tous. Chacun peut lire une blockchain publique et y accéder librement sans restriction. Chaque transaction apparaît sur le registre public, dès lors que l'utilisateur respecte le protocole. Une blockchain publique supprime tout intermédiaire de confiance, puisque les utilisateurs participent au processus d'approbation des transactions (grâce à une récompense, de nature financière dans la plupart des cas).

Blockchain privée : blockchain appartenant à un seul acteur, son propriétaire étant le seul à pouvoir écrire dans le registre. Cela signifie que le droit d'ordonner des transactions sur cette blockchain est restreint. Le propriétaire définit les caractéristiques de cette blockchain selon son gré, notamment le droit de lecture, qui peut être public ou restreint.

Blockchain de consortium : forme hybride de blockchain, entre publique et privée. Le processus d'approbation est contrôlé par certains nœuds déterminés au préalable. Le droit de lecture peut être public ou restreint selon les règles fixées *ex ante* par les membres du consortium habilités à en déterminer les règles.

Ethereum : protocole d'échanges décentralisés permettant la création par les utilisateurs de « *smart contrats* ». Ces « contrats intelligents » sont basés sur un protocole informatique permettant de vérifier le respect de conditions préalablement fixées et d'en exécuter automatiquement les clauses, dès lors que les conditions sont réunies. Ils sont déployés et consultables publiquement dans la blockchain. Ethereum utilise une unité de compte dénommée Ether comme moyen de paiement de ces contrats.

Initial Coin Offering **(ICO)** : mécanisme par lequel des sociétés ou des individus lèvent des fonds en émettant des jetons pour financer leur projet, ou ses phases les plus amont, en échange de monnaies digitales privées comme le bitcoin, ou légales (monnaies fiat). C'est une procédure de levée de fonds sur internet en contrepartie de jetons numériques, appelés « tokens ». Cette procédure s'inscrit dans le cadre du marché primaire des crypto-monnaies, dans la mesure où elle relève de la première émission des jetons numériques.

Lightning **:** protocole de paiement fonctionnant comme une seconde couche par-dessus la blockchain, dans lequel s'effectueraient les transactions de petits montants. À cette fin, les participants ouvriraient entre eux des « canaux » temporaires sécurisés, bilatéraux ou multilatéraux, contribuant à la réduction de la congestion de la chaîne principale.

Minage en blocs : processus au cours duquel une transaction effectuée sur la blockchain est vérifiée et validée par un des nœuds du réseau avant d'apparaître sur la blockchain. Elle est ensuite incluse dans un bloc. Les transactions ayant lieu dans un certain laps de temps sont regroupées en blocs par des mineurs et enregistrée dans un langage binaire (comme tout donnée numérique). Chaque transaction passe par un hash cryptographique, le SHA-256.

Hash cryptographique : fonction mathématique à sens unique qui transforme une suite binaire très longue en une suite de chiffres et de lettres bien plus courte. Cette fonction permet d'identifier plus rapidement une transaction. La particularité du hash SHA-256 est que pour un infime changement de dans la suite binaire de départ, le résultat final sera complétement différent.

Mineurs : individus ou rassemblements de ressources techniques (« pools » de minage), ils sont en compétition perpétuelle pour réunir les transactions venant d'avoir lieu, leur permettant ensuite de créer des blocs, et tenter de résoudre un problème informatique. Toutes les dix minutes en moyenne, les mineurs effectuent des quadrillions (10^{24}) d'opérations mathématiques de hachage : le mineur doit prouver qu'il a fourni suffisamment de puissance de calcul pour trouver la solution (« *Proof of Work* »), ce qui lui permet de gagner la compétition, et lui donne donc le droit de créer un bloc. Il le publie sur la blockchain, et empoche la récompense prévue en crypto-monnaie (selon le protocole). Cette récompense permet de pérenniser le système, en incitant les mineurs à continuer de mettre à disposition du réseau leur puissance de calcul pour créer de nouveaux blocs de transaction. Plus le nombre de transactions augmente, plus le problème à résoudre est difficile, car la difficulté s'ajuste progressivement, pour que le temps de résolution du problème soit toujours égal à 10 minutes.

Nœuds : ensemble des machines détenues par des individus appartenant à un réseau, qui stockent une copie de la blockchain et la mettent progressivement à jour. Ils jouent un rôle comparable à celui des serveurs sur Internet. Les nœuds ont pour objectif de contrôler l'intégralité des transactions ayant lieu sur le réseau. Ils conservent une copie totale ou partielle de la blockchain. Ils ne se font pas confiance entre eux, ce qui implique qu'à chaque transaction reçue par un de ses pairs, le nœud vérifie la transaction indépendamment de sa propre copie enregistrée sur la blockchain.

Toute transaction jugée incorrecte par un nœud est rejetée et suspendue pendant un délai fonction de la gravité de la fraude constatée. Les nœuds essayant de propager des transactions frauduleuses sont donc en théorie très rapidement isolés car tous les autres nœuds du réseau s'en déconnectent progressivement.

Contrairement aux mineurs, les nœuds ne sont pas rémunérés, mais ils permettent à leurs détenteurs de contrôler leur argent, sans avoir à faire confiance aux autres nœuds. Ils leurs fournissent donc un niveau de sécurité supplémentaire.

Plateforme d'échange de crypto-monnaies : plateforme d'échange où des crypto-monnaies peuvent être achetés ou cédés, quel que soit leur statut légal. Ces plateformes permettent de faire fonctionner le marché secondaire des crypto-monnaies, dans lequel ces dernières sont échangées.

Sharding : procédure de traitement « en parallèle » qui aboutirait à découper la blockchain en plusieurs parties, dont chacune serait conservée et mise à jour dans des groupes différents de serveurs. Actuellement, tous les nœuds du réseau conservent – et mettent à jour constamment – des copies identiques de la blockchain. Cette duplication est une garantie de sécurité –puisque tous les nœuds valident chaque transaction – mais c'est une source d'allongement des délais. La « spécialisation » du réseau en différentes parties, introduite par le *sharding*, accroîtrait son efficacité.

Smart contrat : programmes informatiques autonomes qui exécutent automatiquement les conditions et les termes d'un contrat, en dehors de toute intervention humaine.

Portefeuille *(wallet)* : application qui stocke les Bitcoins (ou autre crypto-monnaie) détenus et qui est accessible uniquement à l'aide de la clé privée de l'utilisateur. Il existe des portefeuilles virtuels en ligne *(hot wallet)* mais également physiques (*cold wallet*).

Preuve d'enjeu ou preuve d'intérêt (« *Proof of Stake* ») : procédé alternatif à la preuve de travail (*proof of work*) selon lequel les mineurs devront prouver qu'ils possèdent une certaine quantité de crypto-monnaie pour pouvoir valider des nouveaux blocs dans la blockchain et prétendre à la récompense. Si on possède 1 million de bitcoin sur les 10 millions existants, on a 10 % de chances de valider la transaction. Si on valide une transaction, on ne peut pas participer aux prochaines validations pendant un certain temps pour éviter la concentration du pouvoir au sein du réseau.

Preuve de travail (« *Proof of Work* ») : méthode de validation des blocs, basée sur la puissance de calcul. Les utilisateurs doivent, en effet, exécuter et résoudre des calculs, des algorithmes et des équations mathématiques pour valider les transactions électroniques dans la blockchain. La difficulté de ce travail varie pour garder un temps de validation constant (10 minutes sur la blockchain Bitcoin).

Token (ou jeton numérique) : représentation digitale de valeur, émise et échangeable sur un registre distribué, comme la blockchain. Ces actifs numériques peuvent être transférés sans être dupliqués entre deux acteurs sur Internet et sans nécessiter l'accord d'un tiers – l'équivalent digital de billets. Ils sont fongibles et divisibles si nécessaire : par exemple, tandis qu'actuellement un individu possédant 100 euros ne peut pas détenir une action individuelle d'une entreprise s'échangeant à 200 euros, un *token* permettrait de détenir 0.5 part de l'entreprise, sous forme de part digitalisée. L'acquisition de cette fraction de part serait ensuite instantanément réalisée sur la blockchain en question.

Security token : représentations virtuelles de bénéfices économiques similaires à ceux présents dans des instruments de capitaux propres (ou de dette) et donnant droit à des revenus futurs, voire de vote, dans le cadre de différents projets.

Utility token : représentations virtuelles d'un droit d'accès ou d'usage, comme l'utilisation d'une application au sein d'un blockchain, d'un algorithme de trading, etc. Ces *tokens* octroient ainsi un droit d'usage à leurs utilisateurs en leur permettant d'utiliser ou de bénéficier de la technologie ou des services distribués par l'émetteur de l'ICO. Ils peuvent aussi contenir des droits de vote.

Currency token : représentations virtuelles d'un moyen de paiement, permettant d'effectuer des transactions au sein de réseaux et plateformes créés dans le cadre du projet d'ICO.

Coin/Token « burn » : les émetteurs d'une ICO cherchent à détruire une certaine quantité de jetons de manière permanente. Également appelé « brûlage de pièces », le processus est généralement observé à la fin d'une procédure d'ICO, lorsque les jetons invendus sont détruits afin de limiter quantitativement l'offre.

Whales (ou « baleines ») : souscripteurs détenant une quantité importante d'une crypto-monnaie donnée, au point d'être en capacité théorique d'en manipuler le cours.

Whitelist (ou liste blanche) : liste des souscripteurs ayant eu l'accord de participer à une ICO.

White paper : document de présentation d'un projet de type blockchain ou crypto-monnaie. Ce document vise à la bonne information des souscripteurs potentiels. Ce document contient généralement les grandes catégories suivantes : le concept, le *business model*, les modalités d'émission du *token* et les informations sur l'équipe.

ANNEXE N° 3 : LISTES DES PRINCIPALES *INITIAL COIN OFFERINGS* (ICO) RÉALISÉES EN FRANCE ET DANS LE RESTE DU MONDE DEPUIS 2017

1. Présentation des ICO en France

16 ICO domiciliées en France, et possédant une équipe française, ont été réalisées à début juin 2018. Le total des fonds levés s'élève à environ **130 millions de dollars**, pour un peu moins de 340 millions de dollars de valeur réellement émise sur le marché[110].

1.1. Montant initial des principales ICO françaises (en millions de dollars) au 4 mai 2018

Émetteur	Nom du token	Valorisation initiale[111]	Montants effectivement levés
Ark	ARK	1,25	0,998
iEx.ec	RLC	15,00	12,160
Telcoin	TEL	25,00	25,000
Legolas	LGO	36,19	34,920
Nexium	NXC	0,90	0,400
DomRaider	DRT	17,24	65,890
NapoleonX	NPX	29,80	12,300
Dether	DTH	2,89	13,258
Origami network	ORI	5,39	1,144
BCDiploma	BCDT	1,79	1,889
Kryll	KRL	8,06	3,500

Source : Mission.

1.2. Valeur en cotation des principales ICO françaises (en millions de dollars) au 4 mai 2018

Émetteur	Nom du token	Valorisation actuelle du token[112]	Nombre de tokens en circulation	Réserve totale de tokens
Ark	ARK	379,61	102 320 208	133 570 208
iEx.ec	RLC	132,92	80 070 793	86 999 785
Telcoin	TEL	63,35	29 259 751 257	100 000 000 000
Legolas	LGO	35,90	119 635 679	217 698 062
Nexium	NXC	14,16	66 520 799	100 000 000
DomRaider	DRT	14,16	591 500 000	1 300 000 000
NapoleonX	NPX	9,92	25 330 000	50 000 000
Dether	DTH	7,04	72 500 000	100 000 000
Origami network	ORI	3,52	4 225 879	5 527 379
BCDiploma	BCDT	1,67	n.a.	100 000 000
Kryll	KRL	n.a.	n.a.	72 000 000

Source : Mission.

[110] Source : Avolta Partners, juin 2018
[111] Cours du token au lancement*total des tokens en circulation au lancement.
[112] Cours du token au 4 mai 2018*montant total en circulation au 4/5/18

1.3. Exemples de jetons émis en France, par type :

1.3.1. Exemples de jetons servant à de futurs paiements :

- **ARK Ecosystem** est un réseau dans lequel interagissent plusieurs blockchains différentes et déjà existantes (Bitcoin, Ethereum, IOTA, etc.), ainsi que des forks du token ARK[113]. Le token ARK permet de passer d'une blockchain à l'autre grâce au système de « *smartbridges* » pour effectuer des paiements. La « *smartbridge* » permet de convertir des crypto-monnaies en monnaies fiat, ou en d'autres crypto-monnaies, en passant par les blockchains du réseau ARK. Par exemple, dans une boutique où seul le bitcoin est accepté, mais où le client ne détient que de l'Ether, s'il possède une carte de débit ARK, il pourra via le « *smartbridge* » convertir directement ses Ethers en bitcoin sur place.
- **iEx.ec** est un projet visant à construire un cloud distribué pour des applications utilisant la technologie blockchain. Le token RLC permet d'exécuter des transactions qui auront lieu dans le futur au sein de ce cloud. Le cloud est aujourd'hui principalement utilisé pour effectuer des calculs informatiques complexes. L'objectif est de construire un cloud décentralisé sur la blockchain.
- **Legolas Exchange** est une plateforme d'échange de crypto-monnaies, sur laquelle il est possible d'effectuer des transactions en fiat et en *altcoin*. Le token LGO sert à payer les frais de transactions sur la plateforme. A chaque transaction effectuée, 25 % des frais payé en LGO sont détruits, ce qui permet de réduire progressivement l'offre de LGO en circulation. La plateforme a pour objectif d'être un environnement de trading équitable et sécurisé.
- **Nexium** est une boutique de jeux vidéo en ligne. Le token NXC sert à acheter des éléments de cette boutique.
- **DomRaider** offre un service de réservation de noms de domaine abandonnés, pour « interconnecter » tous les acteurs du monde des enchères : acheteurs, commissaires-priseurs, etc. Le token DRT permet d'acquérir les noms de domaine rachetés par DomRaider.
- **Kryll** est une plateforme qui permet de définir une stratégie de trading. Le token KRL permet de payer des stratégies de trading en direct sur la plateforme, dont la complexité est fonction croissante du prix. Ces tokens peuvent être achetés avec d'autres crypto-monnaies.
- **BCDiploma** (BCDT) permet de garantir l'authenticité des diplômes grâce à la transparence que fournit la technologie Ethereum. Le token BCDT est utilisé pour payer les données, qui sont certifiées par la technologie.

1.3.2. Tokens conférant des droits, notamment d'accès :

- **Neurochain** est une plateforme technologique conçue pour accueillir des applications d'intelligence artificielle et collective. L'objectif est d'optimiser l'efficience de systèmes distribués, en construisant une plateforme technologique hébergeant des applications d'IA collective de pointes. Le token NCC (NeuroChain Clausius), est un token d'usage, permettant d'utiliser les fonctionnalités de la plateforme.
- **NapoleonX** développe des softwares sur une blockchain décentralisée. C'est un gestionnaire d'actifs 100 % crypto algorithmique[114]. Le token donne un statut de propriétaire du software en question, ce qui permet de posséder une licence. Cette licence donne accès à de l'information sur le réseau NPX, comme des signaux de trading par exemple.

[113] Le whitepaper précise que la communauté ARK peut se déployer à l'infini, ce qui signifie qu'elle peut mettre en place ses propres forks.
[114] Etude Avolta, juin 2018

- **Origami Network** cherche à faciliter le lancement de places de marché en fournissant des outils adaptés. La technologie blockchain est utilisée pour renforcer la sécurité des places de marché proposées. Le token ORI servira aux trois éléments suivants : i) moyen de paiement sur la plateforme via « *Origami Payment* », ii) système de récompense « *Origami Review* » en tokens ORI et iii) donne des droits de vote aux parties prenantes du projet.

2. Analyse des ICO à l'international

Les premières ICO sont apparues en 2016 mais sont en développement rapide. Le total des fonds levés par ICO avoisinait les 4Mds USD en 2017[115], et s'élèvent aujourd'hui à près de 9.5Mds USD[116] au niveau mondial.

2.1. Classement des principaux pays en fonction des montants levés par ICO

Pays	Montants levés (en m USD)	Part des montants totaux levés
Etats-Unis	1 031	31.1 %
Russie	310	9.3 %
Singapour	260	7.8 %
RPC	256	7.7 %
Hong Kong	196	5.9 %
Israël	192	5.8 %
Allemagne	187	5.6 %
Canada	175	5.3 %
Royaume-Uni	145	4.4 %
Suisse	64	1.9 %
Estonie	63	1.9 %
Argentine	62	1.9 %
Lituanie	51	1.5 %
Thaïlande	47	1.4 %
Australie	34	1.0 %
Ukraine	32	1.0 %
Espagne	25	0.8 %
Costa Rica	23	0.7 %
Liechtenstein	23	0.7 %
Slovénie	20	0.6 %
Corée du Sud	18	0.5 %
Suisse	15	0.5 %
Bulgarie	12	0.4 %
France	12	0.4 %
Autres	65	2.0 %
Total	**3 318**	**100 %**

Source : Mission, d'après étude d'EY (décembre 2017).

[115] Etude EY, décembre 2017
[116] Baromètre Chaintech, juin 2018

2.2. Présentation des montants levés au 4 mai 2018 :

Émetteur	Nom du *token*	Montants effectivement levés	Valorisation actuelle du *token*[117]	Nombre de tokens en circulation au 4 mai 2018	Réserve totale de tokens
Pétro	PTR	5 000,0	n.a.	n.a.	100 000 000
Telegram	GRAM	850,0	n.a.	n.a.	5 000 000 000
Dragon	DRG	320,0	240,2	360 000 000	500 000 000
Huobi	HT	300,0	154,9	50 200 000	500 000 000
Hdao	DAC	258,0	n.a.	n.a.	n.a.
Filecoin	FIL	257,0	n.a.	n.a.	n.a.
Tezos	XTZ	232,0	n.a.	n.a.	10 000 000 000
Eos	EOS	185,0	15 181,3	844 848 555	900 000 000
Paragon	PRG	183,0	12,2	65 936 605	164 936 595
Sirin Labs (Finney)	SRN	158,0	143,2	229 258 029	573 145 073
Bancor	BNT	153,0	253,9	51 550 340	75 842 294
Bankera	BNK	150,0	n.a.	n.a.	n.a.
Status	SNT	102,0	535,3	3 470 483 788	6 804 870 174
Envion	EVN	100,0	37,7	108 830 970	127 425 494
Kin	KIN	98,0	157,9	756 097 560 976	10 000 000 000
Elastos	ELA	94,0	284,7	5 129 266	33 497 702
TenX	PAY	80,0	147,5	109 004 761	205 218 256
Aragon	ANT	73,0	115,8	26 369 502	39 609 524
Neuromation	NTK	71,0	38,7	81 027 236	100 000 000
Tron	TRX	70,0	6 009,4	65 748 111 645	100 000 000 000

Source : Mission.

2.3. Exemples de jetons émis à l'international, par type :

2.3.1. Exemples de tokens servant à de futurs paiements :

- **Le Pétro** a été lancé par le gouvernement vénézuélien afin de contourner les sanctions économiques des Etats-Unis, le gouvernement a mis en place le Petro, sa propre crypto-monnaie adossée aux réserves pétrolières du pays et indexée sur le montant des réserves pétrolières du Venezuela.
- **Le token Gram** permet aux utilisateurs de l'application Telegram de se faire des paiements entre eux, au niveau international. Telegram est adossé à la blockchain TON, qui fonctionne sur le protocole du « *sharding* ». La validation se fait par le mode de consensus du *Proof of Stake*.
- **Huobi** était une plateforme d'échange initialement sans son propre token mais l'a récemment lancé. Le token HT permet d'acheter d'autres crypto-monnaies sur la plateforme. Le fait de l'utiliser permet de payer moins de frais de transaction sur la plateforme (dimension utilitaire). A noter que l'ICO ne semble pas avoir été faite en HT mais en Tether.
- **Le token DAC** a été lancé avec le support de Hyundai. L'objectif est de mettre en place une blockchain publique avec une multitude de blockchains privées, pour effectuer des micro-paiements sur la plateforme. Ces paiements sont faits avec le token DAC.

[117] Cours du token au 4/5/18 multiplié par le montant total en circulation au 4/5/18.

- **Filecoin** a pour objectif de créer un service de stockage décentralisé : le token FIL permet de payer de l'espace de stockage sur la plateforme.
- **Eos** fournit une plateforme hébergeant des applications décentralisées. Le token permet d'effectuer des transactions sur cette plateforme. Le projet se positionne comme disruptif car il ambitionne de créer une plateforme aussi rapide qu'Ethereum, mais aussi sécurisée que Bitcoin.
- **Sirin Labs** travaille avec Foxconn pour créer un téléphone portable basé sur de la blockchain : le « Finney ». Ce téléphone peut être précommandé avec des token SRN. Les applications pouvant être téléchargées sur ce téléphone seront décentralisées et fournies par la plateforme directement. Un logiciel permettra également de convertir des tokens ERC20 en Finney.

2.3.2. Tokens conférant des droits, notamment d'accès :

- **Le token DRG**, du projet Dragon, pourra être utilisé dans un casino devant être construit à Macao dans un futur proche, car il confère un statut de membre. Il permettra de contourner la réglementation chinoise très stricte sur les flux de capitaux en circulation en dehors de la RPC. 20 % des fonds seront utilisés pour la construction du casino et les 80 % restants nécessaire à la construction du casino seront financés par le gouvernement norvégien.

ANNEXE N° 4 : LISTE DES INCIDENTS INTERVENUS SUR LES PLATEFORMES D'ÉCHANGE DE CRYPTO-MONNAIES

649 millions de dollars de pertes de crypto-monnaies ont été enregistrées depuis 2011 au 31 décembre 2017[118], 73 % de ces pertes étant intervenues sur les plateformes d'échange. Les piratages successifs de Coincheck, Coingrail et Bithumb ont porté ce montant à 1,2 milliards de dollars au 30 juin 2018.

Cela atteste de la vulnérabilité et du risque inhérent au marché secondaire des crypto-monnaies. Les causes identifiées par les experts sont multiples. Le cas le plus courant d'incidents est aujourd'hui lié à la falsification des clés privées des utilisateurs. Vient ensuite l'introduction de logiciels malveillants (comme le hameçonnage dont a été victime Bitstamp en 2015), illustrant la vulnérabilité du code de la blockchain lui-même. En outre, le piratage récent de la plateforme Coincheck au Japon illustre le manque criant de protection des *hot wallet* par des clés multi-signatures.

Tableau : liste des incidents intervenus sur les plateformes d'échange au 13 juin 2018

Nom de la plateforme	Date	Montants perdus (en millions de dollars)
Mt Gox	2011 puis 2014	487
Bitcoinica	Mars 2012 Mai 2012	6 2,4
Bitfloor	Septembre 2012	0,25
Poloniex	4 mars 2014	12,3 % des réserves en bitcoin de la plateforme
Bitstamp	4 janvier 2015	4,3
Bitfinex	Août 2016	72
The DAO	Juin 2016	53
Steemit.com	Juillet 2016	0,085
Parity	Juillet 2017	32
Bithumb	Juillet 2017	1
Veritaseum	Juillet 2017	8,5
Tether	Novembre 2017	30,9
Youbit	Décembre 2017	2,125
Coincheck	Janvier 2018	530
Bitgrail	Février 2018	170
Coinrail	Juin 2018	Entre 0,530 et 0,795
Bithumb	Juin 2018	30

Source : Mission.

Tableau 3 : Présentation des incidents intervenus sur les plateformes d'échange au 13 juin 2018

Plateforme concernée	Nature de l'incident
Mt Gox	**Date** : 2011 puis 2014 **Montants perdus** : 487 millions de dollars (750 000 Bitcoins). **Cause du piratage** : faille de sécurité des *hot wallets*.

[118] Source : rapport Coingecko, décembre 2017.

Plateforme concernée	Nature de l'incident
Bitcoinica	**Date** : mars 2012 et mai 2012 **Montants perdus** : 8,4 millions de dollars ▪ 46 703 Bitcoins lors du premier piratage ; ▪ 18 000 Bitcoins lors du deuxième piratage. **Cause du piratage** : faille de sécurité du serveur Linode (*cloud* hébergeant la plateforme en mars) et du serveur Rackspace (*cloud* hébergeant la plateforme en mai), permettant le vol des clés privées des utilisateurs.
Bitfloor	**Date** : septembre 2012 **Montants perdus** : 250 000 dollars (24 000 Bitcoins). **Causes du piratage** : failles de sécurité de l'encryptage des données et des *hot wallets*.
Poloniex	**Date** : 4 mars 2014 **Montants perdus** : perte de 12,3 % de ses réserves en bitcoin[119]. **Cause du piratage** : mutabilité des signatures ou « malléabilité des transactions ».
Bitstamp	**Date** : 4 janvier 2015 **Montants perdus** : 4,3 millions de dollars (18 866 Bitcoins). **Cause du piratage** : hameçonnage de six salariés de la plateforme.
Bitfinex	**Date** : août 2016 **Montants perdus** : 72 millions de dollars (119 756 Bitcoins). **Cause du piratage** : faille de sécurité dans le portefeuille multi-signatures de Bitfinex et de Bitgo.
The DAO[120]	**Date** : juin 2016 **Montants perdus** : 53 millions de dollars (3,5 millions d'Ethers). **Cause du piratage** : faille de sécurité dans la programmation des *smart contracts*.
Steemit.com	**Date** : juillet 2016 **Montants perdus** : 85 000 dollars. **Cause du piratage** : indéterminé, mais plaintes des utilisateurs relatives à la fiabilité des systèmes d'authentification.
Parity	**Date** : juillet 2017 **Montants perdus** : 32 millions de dollars (150 000 Ethers). **Cause du piratage** : ▪ faille de sécurité dans les portefeuilles numériques multi-signatures ; ▪ faille de sécurité des *hot wallets*.
Bithumb	**Date** : juillet 2017 **Montants perdus** : 1 million de dollars. **Cause du piratage** : hameçonnage d'un employé de la plateforme.
Veritaseum	**Date** : juillet 2017 **Montants perdus** : 8,5 millions de dollars (153 037 Ethers). **Cause du piratage** : indéterminée.
Tether	**Date** : novembre 2017 **Montants perdus** : 30,9 millions de dollars. **Cause du piratage** : faille de sécurité du logiciel Omni Core, utilisé par Tether pour prendre en charge les transactions.
Youbit	**Date** : décembre 2017 **Montants perdus** : 2,125 millions de dollars. **Cause du piratage** : ▪ faille de sécurité permettant aux pirates d'infiltrer le système de retrait de la plateforme ; ▪ hameçonnage donnant accès aux clés privées.

[119] La plateforme n'a pas communiqué le nombre exact de Bitcoins ayant été piratés.
[120] *Decentralized Autonomous Organization*

Plateforme concernée	Nature de l'incident
Coincheck	**Date** : janvier 2018 **Montants perdus** : 530 millions de dollars. **Cause du piratage** : ▪ faille de sécurité des *hot wallets* ; ▪ dispositif de sécurité multi-signatures insuffisamment robuste.
Bitgrail	**Date** : février 2018 **Montants perdus** : 170 millions de dollars (17 millions de Nano – XRB). **Déroulé du piratage** : toutes les transactions ont été momentanément suspendues suite à l'annonce des pertes. **Cause du piratage** : indéterminée.
Coinrail	**Date** : juin 2018 **Montants perdus** : entre 530 000 et 795 000 dollars. **Cause du piratage** : faille de sécurité des *hot wallets*.
Bithumb	**Date** : juin 2018 **Montants perdus** : équivalent de 30 millions de dollars. **Cause du piratage** : faille de sécurité des *hot wallets*.

ANNEXE N° 5 : NATURE ET PORTÉE DES MESURES PRISES OU AYANT VOCATION À ÊTRE PRISES PAR LES ÉTATS MEMBRES DU *FINANCIAL STABILITY BOARD* (FSB)

Nature des mesures réglementaires	Nombre de pays ayant pris des mesures	Nombre de pays envisageant de prendre des mesures	Nombre total de pays ayant pris ou envisageant de prendre des mesures	Nombre total de pays n'ayant pas pris ou n'envisageant pas de prendre des mesures	Part des pays ayant pris ou envisageant de prendre des mesures (en %)
Lignes directrices publiées par le régulateur concernant une ou plusieurs crypto-monnaies	17	4	21	4	84 %
Législation autorisant certaines activités réglementées en lien avec les crypto-monnaies ou clarifiant leur statut juridique	7	10	17	8	68 %
Sandbox ou tout autre environnement réglementaire destiné à faciliter l'activité relative aux crypto-monnaies	9	6	15	10	60 %
Législation visant à limiter les risques liés aux crypto-monnaies	2	13	15	10	60 %
Sanctions administratives prononcées par le régulateur à l'encontre d'un ou plusieurs émetteurs de crypto-monnaies	6	5	11	14	44 %
Rejet d'une ou plusieurs demandes de création d'ETF portant sur des crypto-monnaies	5	4	9	16	36 %
Interdiction d'une ou plusieurs ICO	3	5	8	17	32 %
Interdiction faite à une ou plusieurs institutions financières réglementées de fournir des services de paiement à des plateformes d'échanges de crypto-monnaies	4	3	7	18	28 %
Fermeture d'une ou plusieurs plateformes d'échange de crypto-monnaies	3	3	6	19	24 %
Interdiction faite à une institution financière réglementée d'accorder un prêt en garantie d'un ou plusieurs crypto-actifs	3	3	6	19	24 %

Nature des mesures réglementaires	Nombre de pays ayant pris des mesures	Nombre de pays envisageant de prendre des mesures	Nombre total de pays ayant pris ou envisageant de prendre des mesures	Nombre total de pays n'ayant pas pris ou n'envisageant pas de prendre des mesures	Part des pays ayant pris ou envisageant de prendre des mesures (en %)
Interdiction de réaliser des opérations en comptes propres sur un ou plusieurs crypto-actifs	1	4	5	20	20 %
Action en justice engagées contre les promoteurs ou les émetteurs d'une ou de plusieurs crypto-monnaies	2	2	4	21	16 %
Rejet d'une ou de plusieurs demandes d'agrément de plateformes d'échange de produits dérivés portant sur des crypto-monnaies	1	3	4	21	16 %
Sanctions administratives prononcées par le régulateur à l'encontre d'institutions financières pour exposition au risque lié aux crypto-monnaies	1	3	4	21	16 %

Source : Financial Stability Board *(février 2018).*

ANNEXE N° 6 : COMPTABILITÉ ET FISCALITÉ SUR LE MARCHÉ PRIMAIRE DES ICO

Contribuable	Régime comptable	Régime fiscal
Émetteur	▪ **Au passif** : comptabilisation des *tokens* émis en tant que produits constatés d'avance (sous réserve des dispositions du *white paper* appréciées au cas par cas) ▪ **À l'actif** : comptabilisation du produit de l'émission en monnaies virtuelles en tant qu'instruments de trésorerie divers (voir *infra*).	**Fiscalité des *tokens* émis au passif** : ▪ Produits constatés d'avance dans l'attente de la production et de la fourniture du bien et du service (pas d'assujettissement à l'IS – **0 %**)[121] ; ▪ Produits exceptionnels au moment de la production et de la fourniture du bien et du service (assujettissement à l'IS – **33 %**) ; **Fiscalité des monnaies virtuelles détenues à l'actif** : ▪ IS (**33 %**).
Investisseur	Dissociation selon l'intention de gestion : ▪ conservation durable des *tokens* souscrits à des fins de production ou de fourniture de service de l'entité émettrice : classement en **immobilisation incorporelle** amortissable selon les règles classiques, et dépréciée le cas échéant selon les règles actuelles du PCG ; ▪ à défaut, création dans le PCG d'une classe d'**instruments de trésorerie divers**, intégrant l'ensemble des ICO non détenues à des fins de conservation durable (cotées ou non), et plus généralement les monnaies virtuelles ou les *tokens* détenus à des fins de placement.	Dissociation selon l'intention de gestion : ▪ **conservation durable** : (i) régime des fonds communs de placement à risque (FCPR) – exonération d'IR (**0 %**) si détention pendant au moins 5 ans en cas de détention inférieure à 5 ans – ou (ii) fiscalité applicable à l'achat et à la vente de crypto-monnaies (*cf. infra*) ; ▪ **à défaut** : fiscalité applicable à l'achat et à la vente de crypto-monnaies (*cf. infra*).

Source : Mission.

[121] Le report d'IS serait, en outre, conditionné à la publication du rapport annuel d'audit et de certification, réalisé par un commissaire aux comptes, afin de garantir aux épargnants et investisseurs que le projet est mis en œuvre conformément aux engagements pris par l'émetteur dans le *White Paper*.

ANNEXE N° 7 : COMPARAISON DES RÉGIMES FISCAUX APPLICABLES AUX DEVISES ET INSTRUMENTS FINANCIERS

Régime fiscal	Crypto-monnaies	Devises	Métaux précieux, bijoux, objets d'arts et de collection	Crowdlending	Instruments financiers à terme	Revenus de capitaux mobilier et de plus-values mobilières
Personne physique ou morales soumises à l'IR	▪ **A titre occasionnel** : régime des plus-values de cession sur biens meubles incorporels, soit un taux forfaitaire de 40,2 % ; ▪ **A titre habituel** : barème IR (BIC), soit un taux marginal à 62,2 %.	▪ **A titre occasionnel** : régime des plus-values de cession sur biens meubles incorporels, soit un taux forfaitaire de 40,2 % ; ▪ **A titre habituel** : barème IR (BIC), soit un taux marginal à 62,2 %.	▪ **Métaux précieux** : taux forfaitaire de 11,5 %, dont 0,5 % de CRDS ; ▪ **Bijoux, objets d'art, de collection ou d'antiquité** : taux forfaitaire de 6,5 %, dont 0,5 % de CRDS.	▪ **Régime du PFU**, soit un taux forfaitaire de 30 %.	▪ **A titre occasionnel** : régime du PFU, soit un taux forfaitaire de 30 % ; ▪ **A titre habituel** : barème IR (BNC), soit un taux marginal de 62.2 % ; ▪ **A titre professionnel** : barème IR (BIC) soit un taux marginal de 62.2 %.	▪ **Régime du PFU**, soit un taux forfaitaire de 30 %.
Personne morale soumise à l'IR	**IS** (33 %)	**IS** (33 %)	▪ **IS** (33 %) en cas d'inscription du bien à l'actif de l'entreprise ; ▪ **Par défaut taux forfaitaire** (11,5 % ou 6,5 %) en cas de non-assujettissement à l'IR ou l'IS.	**IS** (33 %)	**IS** (33 %)	**IS** (33 %)

Source : Mission.

ANNEXE N° 8 : PRÉSENTATION DE LA BITLICENSE NEW-YORKAISE

Depuis 2015, le département des services financiers de l'Etat de New York (NY DFS) impose la détention d'une BitLicense aux entreprises souhaitant avoir des activités commerciales sur le segment des crypto-monnaies. La règle, qui a suscité un vif intérêt du public, impose aux détenteurs de cette licence (« *BitLicensees* ») des obligations autour de trois axes :

- **la protection de la clientèle** : chaque entité agréée doit être en capacité de pouvoir restituer les fonds et disposer, à cette fin, d'un compte libellé en dollars. Les entités seront également tenues de ne pas vendre, transférer, assigner, prêter, gager ou rendre d'une quelconque manière indisponible les actifs de la clientèle qu'elles détiennent (monnaie virtuelle incluse). Afin de garantir la protection effective des avoirs de la clientèle, les « BitLicensees » sont également tenues d'enregistrer et de conserver les transactions réalisées pour le compte de leur clientèle. En amont de toute transaction, les entités licenciées sont par ailleurs tenues à des obligations de transparence impliquant d'informer de manière claire et concise les clients des risques éventuels associés aux transactions qui impliquent des monnaies virtuelles, et de présenter dès l'ouverture d'un compte les modalités et les conditions qui encadreront la relation contractuelle. il appartient en tout état de cause aux « BitLicensees » de s'assurer que le client a bien pris connaissance de ces différents éléments d'information ;
- **la lutte anti-blanchiment** : il revient aux entités agréées de conserver au titre du programme anti-blanchiment un certain nombre d'informations pour toutes les opérations qui impliquent le paiement, la réception, l'échange ou la conversion, le rachat, la vente, le transfert ou la transmission de monnaie virtuelle. Il incombe également aux entités assujetties de procéder à certaines vérifications concernant les titulaires de compte. Ainsi, les entités doivent au minimum, lors de l'ouverture d'un compte, s'assurer, dans la mesure du raisonnable, de l'identité du client et maintenir un enregistrement des données ayant permis cette identification. une obligation de déclaration de soupçon est également mise à la charge des « BitLicensees » pour toute activité laissant suspecter une fraude ou une activité illicite qu'ils seraient amenés à constater ;
- **un ensemble de dispositifs prudentiels** : les « BitLicensees » doivent, sous la responsabilité d'un *Chief Information Security Officer* (CISO), mettre en place un programme de cyber-sécurité permettant d'identifier les risques externes et internes auxquels l'entité est exposée, de protéger les systèmes de tout accès non-autorisé ou de tout acte malveillant, de détecter les intrusions et toute atteinte aux données et, le cas échéant, d'y répondre de manière adaptée. Parmi les dispositifs de sauvegarde attendus, les entités agréées doivent également à conduire des tests de pénétration de leurs systèmes d'information, visant à mettre à l'épreuve les mécanismes destinés à prévenir toute intrusion et ce, au moins une fois par an. Plus généralement, les « BitLicensees » doivent établir un plan de continuité d'activité destiné à garantir la pérennité des fonctions essentielles à la poursuite de l'activité dans l'hypothèse ou surviendrait une situation d'urgence ou tout autre évènement de nature à affecter le fonctionnement normal du service feront l'objet d'inspections diligentées par le NYSDFS, au moins une fois tous les deux ans. Au rang des obligations prudentielles, figurent enfin les exigences de fonds propres, exigences déterminées sur la base de plusieurs facteurs tels que la composition du bilan (actif et passif), l'effet de levier dont dispose l'entité agréée, le niveau de ses liquidités et tout autre facteur liés à la protection de la clientèle.

ANNEXE N° 9 : LE « *PROOF OF WORK* » ET SES ALTERNATIVES

Dans le « *proof of work* », la compétition entre les mineurs est régulée par trois paramètres : (1) la taille des blocs, (2) le délai entre deux blocs et (3) la « difficulté », élément central et variable de l'algorithme régulateur.

Les deux premiers paramètres –taille des blocs et délai entre les blocs – ont évidemment une influence sur la rapidité avec laquelle les transactions sont effectuées dans le système. Plus les blocs sont larges, plus les délais sont brefs, plus les transactions sont rapidement traitées.

Bitcoin a opté pour des blogs de faible taille (1MB), jugés plus accessibles pour des mineurs disposant de moyens modestes. Mais, évidemment, la performance s'en ressent. L'insatisfaction créée par la lenteur des transactions alimente un débat permanent et contentieux sur l'augmentation de la taille des blocs. L'impossibilité des acteurs du réseau à trouver un accord est à l'origine, en août 2017, du seul « *fork* » permanent intervenu sur le Bitcoin, avec la création de Bitcoin Cash, dont la taille des blocs est de 8MB.

Le choix essentiel concerne toutefois le délai entre les blocs. Un long délai laisse le temps au réseau de s'organiser et de se rassembler pour valider les blocs trouvés. Il y aura donc relativement peu de blocs orphelins, mais la vitesse du réseau est réduite. Inversement, un délai très bref entre les blocs génère une multitude d'orphelins (ou d'oncles), ce qui peut en retour frustrer les mineurs et perturber les communications. Bitcoin et Ether ont opté, sur ce point, pour deux solutions opposées. Les blocs sont séparés en moyenne de 10 minutes sur Bitcoin et de quelques secondes sur Ether. Cette différence explique à elle seule une grande part de l'écart de rapidité et de performance entre les deux monnaies.

Enfin, le troisième paramètre, la « difficulté « joue un rôle central. Il répond à la nécessité de respecter les délais entre blocs fixés par le protocole, et donc d'assurer un fonctionnement régulier et prévisible du réseau pour les mineurs. Sans cette régulation, l'augmentation de la puissance de calcul (ou sa réduction) entraînerait une diminution (ou une augmentation) du délai entre blocs, qui deviendrait imprévisible et nuirait à la sécurité des transactions. Le paramètre « difficulté « est donc automatiquement et périodiquement ajusté par l'algorithme du protocole pour neutraliser la variation de la puissance totale de calcul. Si la puissance (appelée en termes techniques le « hash power ») augmente, la difficulté augmente également (et inversement).

Au total, la « difficulté » neutralise toute augmentation de rapidité et d'efficacité provenant de la puissance de calcul. La concurrence entre mineurs au titre du « *proof of work* » peut conduire à la mobilisation de puissances de calcul additionnelles grâce aux ressources informatiques et électriques qui y sont attachées. Cependant, ces ressources sont dissipées et leur effet neutralisé par la variation de la difficulté. En définitive, et en simplifiant, le système produit la même performance, mais en mobilisant des ressources accrues. Le protocole fait en sorte que la concurrence entre mineurs produise les effets nécessaires sur la sécurité du réseau, mais annule simultanément tout impact positif sur son efficacité.

Les opérateurs, promoteurs, utilisateurs et défenseurs des crypto-monnaies sont conscients du problème de montée en puissance de la technologie. Des recherches intenses se développent pour y remédier. Plusieurs évolutions sont actuellement envisagées s'inspirant d'approches diverses :

- **Le « sharding »** est une procédure de traitement « en parallèle » qui aboutirait à découper la blockchain en plusieurs parties, dont chacune serait conservée et mise à jour dans des groupes différents de serveurs. Actuellement, tous les nœuds du réseau conservent – et mettent constamment à jour – des copies identiques de la blockchain. Cette duplication est une garantie de sécurité – puisque tous les nœuds valident chaque transaction – mais c'est aussi une source d'allongement des délais. La « spécialisation » du réseau en différentes parties, introduite par le « *sharding* », accroîtrait son efficacité.

- **Le « lightning »** est un protocole de paiement fonctionnant comme une seconde couche par-dessus la blockchain, dans lequel s'effectueraient les transactions de petits montants. À cette fin, les participants ouvriraient entre eux des « canaux » temporaires sécurisés, bilatéraux ou multilatéraux, contribuant à la réduction de la congestion de la chaîne principale.

  Ces canaux seraient mis en place au sein d'un même portefeuille multi-signatures permettant de détenir des crypto-monnaies. Ce portefeuille serait couplé à une adresse de portefeuille de réserve dans la blockchain, permettant aux parties prenantes de réaliser un nombre illimité de transactions non rendues publiques sur la blockchain. Le système fonctionnerait avec prépaiement et virements traditionnels entre les différents participants, chacun d'eux immobilisant dans une adresse dédiée sur la blockchain une provision sur laquelle s'imputeraient les transactions. Les soldes seraient reversés sur la blockchain lors de la fermeture des canaux dédiés. En effet, une fois que toutes les transactions initialement prévues seraient réalisées, le solde restant serait enregistré sur la blockchain et les parties prenantes pourraient récupérer leurs parts respectives sur leur portefeuille.

  L'architecture du système marque une évolution vers un système à deux niveaux (à l'image des systèmes bancaires et de paiements existants) avec, de la même manière, des relations bilatérales ou multilatérales plutôt que totalement décentralisées. Le « *lightning* » n'est pas aussi sécurisé que la blockchain elle-même, mais il pourrait être massivement adopté pour les transactions de plus petite taille et réduirait le trafic sur la blockchain publique, afin de la rendre davantage modulable (« *scalable* »). L'obligation du prépaiement (nécessaire pour éviter le risque de contrepartie dans des transactions répétées entre mêmes participants) peut néanmoins se révéler coûteuse en liquidités.
- L'évolution la plus radicale vise à changer le consensus lui-même en abandonnant le « *proof of work* » pour lui substituer **le « *proof of stake*** ». L'idée fondamentale est simple : la validation des transactions serait déléguée à ceux qui accepteraient de mettre en gage de leur honnêteté (dans une adresse dédiée) les avoirs qu'ils possèdent en crypto-monnaie. Chacun de ces validateurs volontaires posséderait un pouvoir de vote proportionnel à ses avoirs. Le protocole s'assurerait que les comportements malhonnêtes soient financièrement sanctionnés par une pénalité. Il y a donc un basculement dans la logique des incitations. La récompense est toujours assurée par l'attribution de monnaie (et les frais de transactions), mais la pénalité est différente, puisqu'elle intervient sous la forme d'amende *a posteriori*. On évite le déploiement – et la perte – de ressources capitalistiques et électriques qui pénalisent aujourd'hui le « *proof of work* ».

  Le « *proof of stake* » doit être mis en œuvre sur Ether et est développé dans le cadre du projet Casper. Ce projet a connu plusieurs délais. Si la logique économique du « *proof of stake* » paraît simple, la mise en œuvre recèle de nombreuses difficultés. Le processus est vulnérable à une prise de contrôle du réseau par la majorité des détenteurs de monnaie (possible en « *proof of work* », mais beaucoup plus difficile). Les mêmes validateurs peuvent « investir » simultanément dans plusieurs chaînes en parallèle, ce qui rend plus complexe la protection du réseau contre les abus de pouvoir potentiels des plus gros détenteurs de monnaie.