INSTITUT DIDEROT

LES CARNETS DE L'INSTITUT DIDEROT

L'avenir du bitcoin et de la blockchain

Georges GONTHIER & Ivan ODONNAT

INSTITUT DIDEROT // www.institutdiderot.fr / @InstitutDiderot

LES CARNETS DE L'INSTITUT DIDEROT

L'avenir du bitcoin et de la blockchain

Georges GONTHIER & Ivan ODONNAT

2019

Sommaire

Préface

En novembre 2017, le cours du bitcoin évoluait joyeusement vers les 20 000 dollars ; les médias consacraient de nombreux articles à cette extraordinaire innovation financière et de respectables institutions annonçaient qu'elles étudiaient son utilisation éventuelle.

L'analyse de l'Institut Diderot était très différente. Une aimable confusion organisée par les bénéficiaires du système mêlait la sécurité des échanges sur la blockchain, l'idée de monnaie privée dans un environnement numérique, et le bitcoin qui participait des deux mais n'en était qu'une application. Les caractéristiques de celui-ci ne lui conféraient pas la qualité de monnaie et ne lui permettaient pas de tirer parti de la sécurité apportée par la blockchain qui n'en constitue qu'un élément.

C'est cette conviction qui a conduit l'Institut Diderot à organiser un débat entre Ivan Odonnat [1] et Georges Gonthier [2].

1. Adjoint au Directeur général de la Stabilité Financière et des opérations de la Banque de France.
2. Directeur de recherches à l'INRIA - Institut National de Recherche en Sciences du Numérique - Saclay Île-de-France.

Ce débat a largement confirmé les analyses de l'Institut Diderot présentées dans son blog [3] en avril 2018.

Depuis le bitcoin a vu son cours s'effondrer. C'était prévisible et probablement envisagé par les promoteurs qui tenteront sans doute de le faire renaître après de prétendues améliorations, pour exploiter à nouveau la naïveté du public.

Le bitcoin n'était qu'un jeu et, même en tant que tel, ne méritait pas la confiance qu'on peut accorder aux casinos du fait de l'absence d'un droit et d'autorités de contrôle qui en assurent la loyauté.

La blockchain, quant à elle, poursuit sa carrière. C'est un dispositif sécurisé d'échanges de données qui trouve de plus en plus d'applications ; son seul défaut est une consommation élevée d'énergie qui mérite attention.

Les monnaies privées établies sur le modèle du bitcoin ont été affectées par les mêmes déboires, mais, dans un monde où la confiance accordée à nombre d'États est très faible, l'idée même de monnaies émises par des institutions privées à vocation à renaître, sous réserve de respecter trois conditions :

- que l'émetteur soit connu et digne de confiance ;
- que l'émission se fasse dans un cadre juridique clair qui assure la loyauté de l'émetteur et ouvre des droits de recours aux usagers ;

3. https://www.institutdiderot.fr/tous-les-articles/

• que la monnaie ait un véritable pouvoir libératoire.

En avril 2018, l'article de l'Institut Diderot suggérait qu'une organisation de type Amazon pouvait réunir ces conditions ; ce n'est pas le cas pour l'instant, mais Facebook vient d'annoncer qu'il souhaitait, avec 28 grandes entreprises et ONG, lancer à la mi-2020 une cryptomonnaie baptisée *Libra*.

Cette évolution, avec d'autres, marquerait l'érosion du rôle des États, dont le contrôle de la monnaie est une prérogative régalienne, au profit d'autres entités dont la dimension politique a vocation à s'affirmer.

Jean-Claude Seys
Président de l'Institut Diderot

L'avenir du bitcoin et de la blockchain

INTRODUCTION

Ivan Odonnat

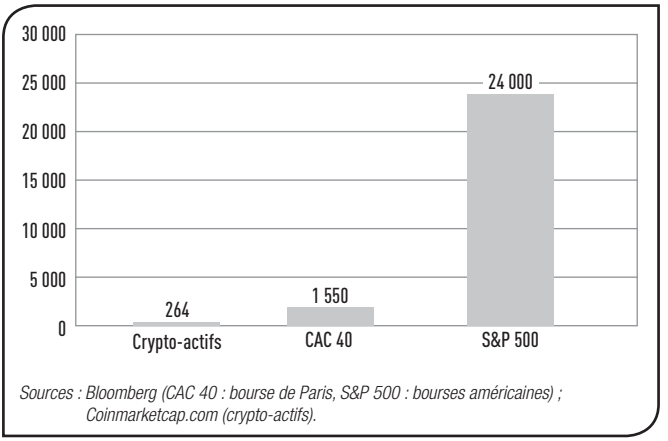
Il existe aujourd'hui plus de 1 600 crypto-actifs. C'est donc un ensemble très diversifié. Le bitcoin, le principal de ces actifs, représente 40 % de la capitalisation. Cet ensemble apparait pourtant assez petit, quand on compare la capitalisation des crypto-actifs à celle de marchés classiques : à peine 25 % de la capitalisation du CAC40, moins de la moitié de la capitalisation d'Apple (cf. graphique n°1).

Cette capitalisation relativement faible explique pourquoi pendant longtemps les banques centrales ne s'en sont pas préoccupées. Qu'y-a-t-il donc de changé ? Principalement la volatilité accrue du prix du bitcoin, passé en un an de 700 dollars à 19 000 dollars en décembre 2017 et qui avoisine aujourd'hui 7 000 dollars. Mais aussi l'émergence d'un véritable écosystème composé d'entrepreneurs, d'informaticiens, d'apporteurs de projets et de juristes, que la Banque de France, mais aussi l'Autorité de contrôle prudentiel et de résolution (ACPR) et l'Autorité des marchés financiers (AMF) cherchent à mieux comprendre.

GRAPHIQUE 1 :

Comparaison des capitalisations en juillet 2018

(en milliards de dollars)



Sources : Bloomberg (CAC 40 : bourse de Paris, S&P 500 : bourses américaines) ; Coinmarketcap.com (crypto-actifs).

Selon les propos de l'humoriste américain, John Oliver, les crypto-actifs combinent tout ce que nous ne comprenons pas de la monnaie avec tout ce que nous ne comprenons pas de l'informatique. Pour apporter quelques éclaircissements, Georges Gonthier et moi répondrons à quatre questions :

– comment fonctionnent les crypto-actifs ?
– qu'apportent-ils ?
– quels risques leur sont attachés ?
– si ces risques sont avérés, comment les autorités doivent-elles réagir ? Faut-il réglementer ?

Georges Gonthier abordera les deux premières questions, et je traiterai les deux suivantes.

Georges Gonthier

Il faut commencer par tirer au clair trois termes précis.

- un crypto-actif est, d'un point de vue technique, un actif. Il a une valeur reconnue, qui n'est pas garantie par une autorité régalienne, mais par un algorithme, par une opération logique.

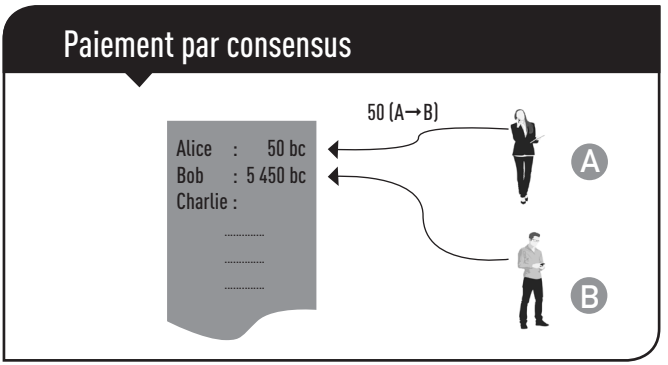
- la blockchain, chaîne de blocs pour ceux qui préfèrent le français, est un mécanisme pour représenter un registre de valeurs indispensable quand on fait une monnaie. Ce registre peut servir pour d'autres choses : des risques d'assurances, par exemple, ou des diplômes. Il s'agit donc du mécanisme sur lequel s'appuient les actifs.

- derrière tout ça, il y a le mot consensus ; il est le moteur qui fait marcher tous ces algorithmes. En quelque sorte, il assoit la valeur des monnaies, dans la mesure où pour vouloir affirmer quelque chose il faut établir un consensus, un accord entre des parties qui ne sont pas fiables. C'est un problème étudié depuis longtemps par les informaticiens, en particulier parce qu'il se pose soit dans les systèmes qui doivent avoir une très haute résistance aux pannes, par exemple dans l'aérospatiale, ou dans les systèmes qui sont naturellement sujets aux pannes, par exemple les grands systèmes de base de données répartis, où on ne peut pas garantir que tous les ordinateurs d'un réseau fonctionnent en même temps. Or c'est une réelle innovation concernant le problème du consensus qui a permis de lancer les crypto-monnaies.

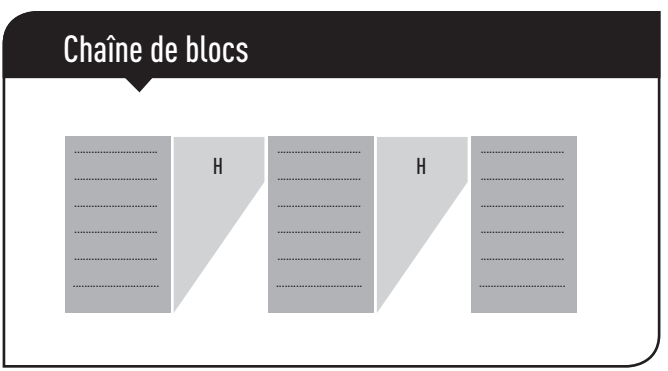
Il faut expliquer pourquoi il est possible, à partir du moment où on a un registre et un consensus, de faire une monnaie, en tout cas un moyen de paiement. Si vous disposez d'un registre où, d'un commun accord, tout le monde peut écrire, vous pouvez faire des paiements entre deux parties. Par exemple si Alice (les cryptographes appellent toujours leurs parties Alice et Bob) veut acheter un objet pour cinquante unités à Bob, Alice peut inscrire sur le registre, implémenté par la blockchain, qu'elle envoie cinquante unités à Bob. Une fois cette transaction enregistrée, dès que Bob peut voir qu'il a été crédité, il peut délivrer la marchandise à Alice. (graphique 2)

Pourquoi parle-t-on de chaîne de blocs ? Parce que le problème du consensus est un problème difficile à résoudre. On n'essayera pas de résoudre un consensus sur un registre complet, qui dans le cas des grandes monnaies atteint des téraoctets et plus. On va découper ce registre en petits blocs pour faire le consensus pièce par pièce, bloc par bloc. Mais si on fait le consensus bloc par bloc, on risque de ne s'accorder que sur une partie des choses. Pour s'assurer de l'ensemble, on fait comme la télé quand elle diffuse un feuilleton : pour chaque bloc on va rajouter un résumé de l'épisode précédent. Ainsi le dernier bloc, tout à droite, contient quelque part la totalité du registre, parce qu'il en contient le résumé. Tout repose sur la propriété indiquée avec un grand H sur la graphique 3 et que les informaticiens appellent une fonction de hachage.

GRAPHIQUE 2 :



GRAPHIQUE 3 :



Cette fonction a quelques propriétés miraculeuses qui résultent du fait que ce sont des calculs soigneusement agencés pour être imprévisibles. Ils sont imprévisibles essentiellement parce qu'on mélange deux types d'opérations, des opérations arithmétiques et des opérations sur des images. Les opérations sur les images ont une

logique et on peut prédire ce qu'elles font. Idem avec l'algèbre pour les opérations arithmétiques. Mais si on mélange les deux, le calcul devient imprévisible, ce qui veut dire qu'étant donné une valeur, un résumé donné, il est impossible de deviner quelle est l'histoire, l'épisode complet qui correspond à ce résumé. Il est même impossible de trouver deux épisodes qui auraient exactement le même résumé. Bref, cela revient à numéroter au hasard. Le résultat, c'est qu'on a essentiellement un mécanisme qui permet de compresser une quantité illimitée d'informations sur 256 bits, soit 32 octets – pour mémoire, votre téléphone portable a probablement une mémoire 1 milliard de fois plus grande. 32 octets représentent un nombre gigantesque, largement de quoi donner un numéro différent à chaque élément d'information qu'un humain pourrait créer dans toute l'histoire de l'humanité.

Le cœur du problème est alors le consensus, ce qu'on fait sur chaque bloc. Traditionnellement, l'informatique étudie les problèmes de consensus fermés, c'est-à-dire que les parties qui doivent s'entendre sont fixes ou connues. C'est un problème qui a été très étudié parce qu'il se pose pour des systèmes fiables, des bases de données, etc. Essentiellement, le mécanisme de résolution repose sur un scrutin à deux tours.

La grande innovation qui a permis les crypto-monnaies, c'est d'imaginer un nouvel algorithme qui permet d'avoir un algorithme de consensus ouvert capable de dégager un accord entre tous les participants, sans même avoir fixé leur nombre. Ceci est essentiel pour une monnaie

parce que chacun doit pouvoir l'utiliser comme moyen de paiement.

Cette contrainte impose qu'on ait un seul tour : pour faire revenir tous les votants pour un second tour, il faudrait les connaître. Comme en politique, le risque d'avoir un scrutin à un seul tour, c'est le ballottage, qu'on appelle ici une divergence de la chaîne.

Le second problème, c'est celui de l'identité : quand on vote, il faut identifier les électeurs, mais c'est beaucoup plus difficile d'identifier les machines, de façon purement algorithmique. Une identité informatique, c'est juste un nombre et quelqu'un de malveillant pourrait s'amuser à bourrer les urnes en inventant un nombre arbitraire d'électeurs. La solution qui a permis l'avènement des crypto-monnaies, largement utilisée maintenant dans les deux principales monnaies, bitcoin et ether, c'est la preuve de travail : l'identité doit être rattachée à une personne réelle et, puisqu'il s'agit d'un réel d'informaticiens, cette personne est un ordinateur. Or on reconnaît un ordinateur physique par le fait qu'il peut calculer. Ce n'est pas une idée nouvelle : elle avait été proposée pour résoudre le problème des pourriels, ou spams. En demandant à un ordinateur de calculer, on l'oblige à démontrer qu'il existe. Si on pousse ce mécanisme à la limite, on peut exiger un calcul suffisamment important pour qu'on ait en moyenne un seul votant à la fois. Il est alors facile de s'entendre puisqu'il y a une seule personne qui parle. Ainsi tout le monde peut se mettre d'accord sur ce qu'elle a dit, par exemple tout le monde peut vérifier qu'au moment

où une transaction est faite, il y a bien de l'argent sur le compte.

Toutefois, ce calcul, qui est important, doit être rémunéré, sinon personne ne voudrait le faire. C'est peut-être la grande innovation du bitcoin : une des manières de résoudre le consensus est d'y attacher une valeur monétaire. Là où cela a mal tourné, c'est que le bitcoin s'est mis à avoir beaucoup de valeur. Du coup des participants ont eu intérêt à investir lourdement dans le « minage » de blocs. Le bitcoin est une monnaie dont la réserve n'est pas l'or-étalon, mais la consommation électrique, qui est l'équivalent de celle du Danemark, et même peut-être plus maintenant. Cela a donné naissance à une spéculation, à une concentration débridée.

Un dernier problème de la preuve de travail est que si elle est un mécanisme pour s'accorder sur les blocs, il n'y en a pas pour s'accorder sur la façon dont cette monnaie va fonctionner globalement, à l'exception des règles fixées au départ. Toutes ces monnaies ont un problème de gouvernance. Elles ont beaucoup de mal à évoluer même pour des choses aussi simples que de déterminer la taille des blocs afin de les agrandir. Quand le nombre d'utilisateurs a augmenté pour le bitcoin, cela a conduit à une majorité de blocage des mineurs et à un schisme de la monnaie.

Il est important de comprendre comment on a résolu le problème de la divergence, celui du ballottage : le plus souvent il n'y a qu'une seule personne qui parle, mais il

est possible que deux personnes parlent en même temps. On peut alors se retrouver avec deux registres, ou deux additions au registre, une qui dit que A paie 75 à B et l'autre qui dit que A paie 75 à C. S'il n'y a que 100 dans le compte de A, on ne peut pas avoir les deux en même temps ; il faut choisir ! L'idée du bitcoin c'est que si deux blocs arrivent en même temps dans le réseau, on attend un troisième bloc pour les départager : quand un mineur voit une chaîne plus longue que celle qu'il connaît il abandonne cette dernière. Comme il y a peu de chances qu'un conflit se reproduise, on garantit ainsi le consensus à brève échéance : si on attend qu'une transaction soit enterrée derrière six blocs, il est presque certain que personne ne peut la modifier.

Cette preuve de travail a beaucoup de défauts et elle n'est pas écologique. Une seconde technique a été proposée et adoptée par les monnaies plus modernes, dont EOS, Algorand ou Tezos, une crypto-monnaie française lancée très récemment, c'est la preuve d'enjeu. L'idée est de dire qu'on a une autre notion naturelle d'identité : les avoirs. Vous existez si vous avez investi dans la monnaie. Si vous avez beaucoup d'avoirs, vous n'avez pas intérêt à ce que la monnaie fonctionne mal et perde sa valeur. Alors, pour la faire marcher, on regroupe les votes pour avoir une sorte de scrutin à deux étages, avec des grands électeurs. Toutefois, si on admet la divergence, il faut définitivement limiter la profondeur : la valeur des chaînes étant basée uniquement sur la tenue de registres et pas sur un actif physique, quelqu'un qui parvient à fausser le système peut en principe produire une chaîne arbitrairement

grande. On ne peut donc pas se baser uniquement sur la longueur de chaîne pour ajouter une limite. Le gros avantage de ce mécanisme, c'est qu'en tant que système de vote, il permet de faire de la gouvernance. Cette dernière innovation permet de prévoir un système à l'intérieur duquel la monnaie est à même de s'adapter à un monde fluctuant.

Le dernier sujet que je veux aborder est celui des smart contrats, les contrats intelligents. C'est une façon de désigner l'opération qui permet, quand on inscrit une transaction dans un registre, de vérifier qu'elle est correcte. L'idée des smart contrats est de rendre programmable la logique qui régit les sommes concernées par le crypto-actif. Le bitcoin permet de régir la logique de validation, ce qui permet de faire avec la monnaie ce que font les instruments financiers classiques, lettres de change, signatures multiples, versements d'arrhes et reversement d'arrhes sous contrôle. Des monnaies comme ether rajoutent la possibilité de stocker de l'information en utilisant le même mécanisme de hachage cryptographique. Cela s'appelle les arbres de Merkle, et leur application majeure est de créer à l'intérieur d'une monnaie des plateformes d'échanges pour des actifs plus spécifiques. Ce mécanisme permet de construire tous les ICO (*initial coin offering*).

Je termine en disant que l'intérêt pour la blockchain vient du fait qu'étant donné que ces programmes manipulent les valeurs, la vérification du bon fonctionnent de ces programmes est une valeur ajoutée importante. Les pertes importantes de crypto-monnaies ne sont pas dues à la

violation des ordinateurs des plateformes de change, mais à des erreurs de programmation sur ces contrats.

Ivan Odonnat

Dans le prolongement des commentaires de Georges Gonthier, je voudrais d'abord apporter deux précisions.

La première est que ni le bitcoin ni ses semblables ne sont des monnaies !

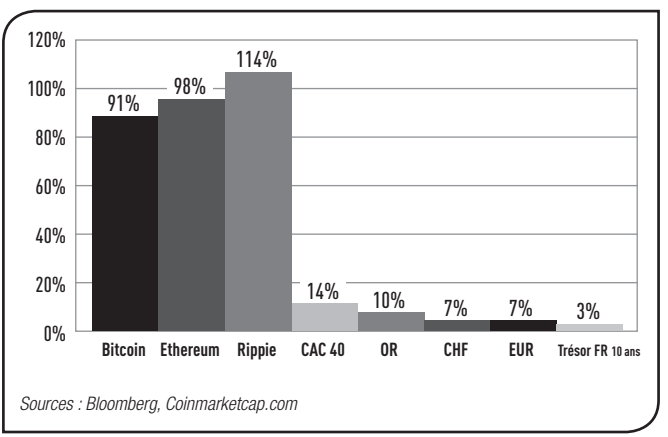
Il y a une trentaine d'années, l'économiste américain, Hyman Minsky, soulignait déjà que si tout le monde pouvait créer de la monnaie, c'était autre chose que de la faire accepter.

On peut examiner le problème sous l'angle des trois fonctions de la monnaie définies par Aristote : réserve de valeur, intermédiaire des échanges, unité de compte.

Pour être une réserve de valeur, la monnaie doit avoir une valeur stable qui serve de référence. Le graphique 4 représente la volatilité historique de différents prix d'actifs : cours des trois principaux crypto-actifs (bitcoin, ether et ripple) d'une part ; prix d'un certain nombre d'instruments financiers traditionnels (cours de l'or, taux de change du franc suisse, taux de change de l'euro, taux d'intérêt à dix ans de la dette souveraine française) d'autre part. De toute évidence, nous avons affaire à deux mondes différents. La volatilité du prix des crypto-actifs est très élevée par rapport aux standards

auxquels nous sommes habitués. Difficile, donc, d'en faire une référence de valeur. Et puis, quelle serait la valeur intrinsèque du bitcoin ? Je mets au défi quiconque de l'indiquer avec certitude. Il n'existe pas pour le moment de modèle de prix à même d'expliquer le prix du bitcoin.

GRAPHIQUE 4 :
Volatilité historique sur un an du prix de différents actifs



Sources : Bloomberg, Coinmarketcap.com

Concernant la fonction d'intermédiaire des échanges, il n'y a pas à ma connaissance de grande enseigne commerciale qui permette à ses clients de régler leurs achats à l'aide de bitcoins, que ce soit en ligne ou en magasin. Ce mode d'utilisation des crypto-actifs se heurte en effet à des limites physiques. Alors que les systèmes de paiement par carte bancaire permettent d'effectuer

plusieurs dizaines de milliers de transactions à la seconde, un paiement au guichet d'un commerçant avec le bitcoin par exemple nécessiterait probablement plusieurs heures avant que la transaction soit complètement validée. Cette deuxième fonction assignée à la monnaie ne me paraît donc pas remplie par les crypto-actifs.

Ce n'est pas davantage le cas pour la fonction d'unité de compte. Pourquoi faire une unité de compte d'un objet dont le prix est volatil, dont on ne connaît pas la valeur intrinsèque et qui ne peut pas servir d'intermédiaire des échanges ? Ma conclusion est formelle : les crypto-actifs ne remplissent pas aujourd'hui les fonctions de la monnaie.

Deuxième précision : on parle des crypto-actifs et Georges Gonthier en a excellemment décrit les principes de création et de fonctionnement ; on parle aussi des Initial Coin Offerings ou ICO pour qualifier des jetons numériques permettant des opérations d'échange ou le financement de projets. La différence entre ICO et crypto-actifs est technique. Elle porte sur le processus d'émission : à la source des bitcoins émis, vous trouvez des mineurs ; les ICO reposent sur un processus d'émission de jetons qui peut s'apparenter à un financement par actions d'un projet classique, les jetons étant même porteurs de droits d'usage. Ils peuvent être ensuite acquis par des investisseurs ou des souscripteurs en échange soit de monnaie ayant cours légal, soit de crypto-actifs. Cependant, sous l'angle des enjeux pour le système financier, il n'y a absolument aucune différence entre ces

deux formes d'instruments. En fait, quand on évoque les crypto-actifs et les ICO, on parle d'objets qui se ressemblent, qui diffèrent par leur processus d'émission sous-jacent, mais qui sur le marché secondaire forment un ensemble assez fongible.

Ces deux précisions apportées, quels sont les risques attachés aux crypto-actifs et autres ICO ? Je l'ai souligné d'entrée, pendant longtemps les banques centrales ont été relativement indifférentes à ces innovations et leurs conséquences. Cela se comprend : ces marchés n'occupent pas une place prédominante dans l'espace financier ; les corrélations entre les prix de ces actifs et ceux des actifs financiers traditionnels sont assez faibles, de sorte que le risque de propagation d'un choc négatif affectant le bitcoin ou d'autres crypto-actifs à d'autres segments de marché est quasi inexistant ; de même, il y a très peu d'interactions entre crypto-actifs et sphère réelle, dans la mesure où ces instruments sont utilisés par une communauté encore assez restreinte. Pour autant, peut-on se contenter de ce constat rassurant ?

En réalité, il y a deux sujets de préoccupation.

Le premier concerne l'anonymat des transactions effectuées à l'aide de crypto-actifs. Si aujourd'hui un certain nombre de pays européens limitent l'utilisation des espèces, c'est parce que l'anonymat comporte le risque qu'à l'origine de ces opérations, il y ait des comportements de type criminel ou des opérations de blanchiment de capitaux et de financement du terrorisme. Ce raisonnement

doit s'appliquer aux crypto-actifs également. L'illustration la plus récente est le scandale financier qui frappe la banque danoise Danske Bank dont la filiale estonienne est impliquée dans un certain nombre de transactions non conformes réalisées au moyen de crypto-actifs.

Le deuxième sujet concerne la fraude en général. Le graphique 5 représente la répartition des avoirs en bitcoins par détenteur et montre une extrême concentration. Un très petit pourcentage d'investisseurs détient aujourd'hui l'essentiel de la capitalisation. Sans prétendre à une exactitude absolue, ce graphique, établi par la Banque de France d'après les informations dont nous disposions, illustre un phénomène bien connu : un petit nombre de détenteurs de bitcoins a la capacité de faire bouger le marché et de manipuler les cours d'une façon qui serait inacceptable sur n'importe quel autre marché financier. C'est une anomalie qui exige une action des autorités du secteur financier (régulateurs, banques centrales, superviseurs). Le paradoxe, est que celles-ci sont assez prudentes sur la façon de procéder. Le graphique 6 représente les pertes enregistrées dans les cas de fraudes détectées sur des opérations liées au bitcoin, notamment en relation avec le fonctionnement des plateformes d'échanges. Ces cas ne renvoient pas nécessairement à des problèmes intrinsèques au fonctionnement de la chaîne de blocs. Toutefois, même si celle-ci comporte un certain nombre de dispositifs assez sécurisés, des points de fragilité existent. Comme dans n'importe quel domaine d'activité, il peut y avoir des gens malveillants qui proposent de participer à des opérations qui n'existent

pas, ou qui effectuent des vols. Le bilan de ces fraudes est assez significatif : la courbe en gris représente le cumul des pertes évaluées à la valeur du crypto-actif au moment où l'incident a été détecté ; la courbe en noir représente le montant de la perte cumulée si on la convertissait au cours actuel. Le cumul des pertes se situe entre 1 et 9 milliards de dollars selon le mode d'évaluation, ce qui n'est pas négligeable. Ces deux préoccupations renvoient à l'une des missions fondamentales de la Banque de France, qui veille quotidiennement à la sécurité des instruments de paiement utilisés en France, depuis le chèque jusqu'à la carte. Si on veut permettre une utilisation sécurisée de ce type d'actifs, il faut un dispositif de suivi et de contrôle adapté, à même de limiter les risques identifiés. Pour le moment, il n'existe pas.

Face à ces deux difficultés, quelle doit être la réponse des autorités ? Comment les autorités pourraient-elles accompagner ce mouvement d'innovation en essayant de faire la part entre ce qui mérite d'être encouragé et ce qu'il faut contenir ou interdire ?

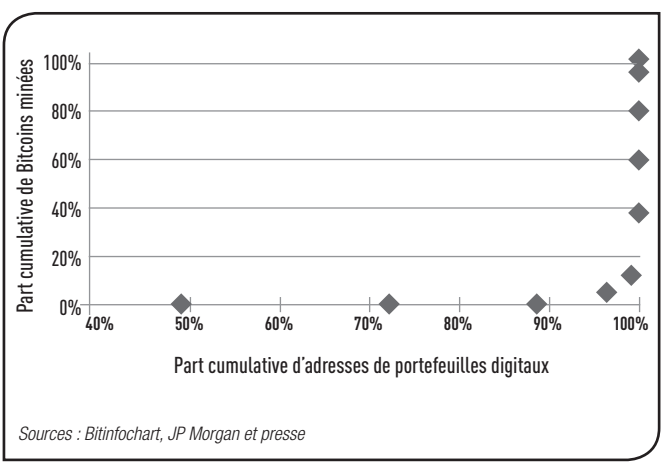
Interrogeons-nous d'abord sur la sécurité de la block-chain. Celle-ci s'appuie largement sur des techniques anciennes, certes améliorées grâce aux programmes de cryptographie et à la puissance de calcul. Les progrès en la matière continuent et il n'y a pas de raison de s'y opposer. Il faut cependant veiller à prévenir ou contenir un certain nombre de problèmes : performance insuffisante, consensus qui pourrait s'établir d'une façon non conforme aux attentes, prise de contrôle par certains

utilisateurs à des fins personnelles ou à des fins frauduleuses, erreurs de codage des informaticiens.

Pour ce qui est du risque de blanchiment des capitaux et de financement du terrorisme, différents aspects sont à considérer. Est-ce que cela doit être une préoccupation nationale ou une préoccupation internationale ? Comment coordonner les efforts ? En réalité, la lutte contre le blanchiment des capitaux et le financement du terrorisme n'est pas une préoccupation nouvelle. Il existe un dispositif qui prend appui sur les recommandations du GAFI (Groupe d'action financière).

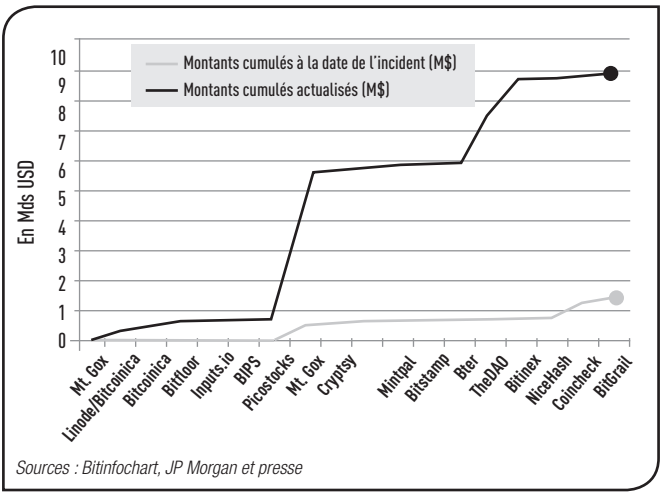
GRAPHIQUE 5 :

Concentration de la détention de bitcoins dans les portefeuilles digitaux



Sources : Bitinfochart, JP Morgan et presse

GRAPHIQUE 6 :
Détournement de crypto-actifs



Sources : Bitinfochart, JP Morgan et presse

Une quatrième directive de lutte contre le blanchiment des capitaux et le financement du terrorisme est en cours d'adoption dans l'Union européenne. Elle couvre notamment les problématiques liées aux plateformes de conversion de crypto-actifs contre monnaie légale en leur imposant des obligations de connaissance de la clientèle. Au plan international, les autorités françaises et allemandes, ministres et banquiers centraux, ont écrit à leurs pairs du G20 en avril 2018 pour appeler à une action concertée et collective en la matière.

S'agissant du risque de fraude, c'est la protection des consommateurs qu'il met en jeu directement. L'action dans ce domaine est principalement de portée nationale.

Les autorités sont intervenues en France mais aussi ailleurs dans le monde, à différents niveaux, allant de la simple mise en garde à des interdictions. Les ICO sont ainsi interdites en Chine. Le Japon est plus accommodant : il a donné un statut légal au bitcoin. En France, les régulateurs ont averti les épargnants sur les précautions à observer dans l'utilisation des plateformes d'échange. Une régulation coordonnée au niveau du G20, telle que promue par les autorités françaises et allemandes, serait bienvenue. En pratique, ce serait au régulateur international des marchés financiers, l'IOSCO (*International Organisation of Securities Commissions*), d'agir. Cependant, la coopération internationale étant difficile et lente, les autorités françaises ont pris le parti d'intervenir, à travers le projet de loi PACTE qui est en cours de discussion au Parlement et comporte notamment un article visant les conditions d'émission des jetons émis dans le cadre des ICO.

Au plan mondial, sur les cinq ou six premiers mois de l'année 2018, il y a eu vingt fois plus d'ICO que d'émissions d'actions. Les ICO concernent des entreprises du secteur de l'Internet, on en voit donc bien l'enjeu. Il faut offrir un dispositif qui protège et favorise le développement ou la mise en œuvre de ces ICO de façon sécurisée.

Les entrepreneurs qui veulent financer des projets par l'émission de jetons numériques expriment eux-mêmes le besoin d'un dispositif qui permette de faire la part entre les arnaques et les projets sérieux. Le dispositif décrit

dans PACTE prévoit l'obtention optionnelle auprès de l'AMF d'un label offrant notamment des garanties sur l'identité des participants et les modalités de conservation des actifs.

Au-delà du bon fonctionnement du marché primaire, des règles portant sur la sécurité des opérations et la protection de la clientèle sur le marché secondaire sont également nécessaires : que se passe-t-il une fois les jetons émis et acquis ? Dans quelles conditions s'opèrent les échanges et comment les utilise-t-on ? La Banque de France et l'ACPR préconisent la création d'un statut de prestataire de services en crypto-actifs de toute nature : échanges entre crypto-actifs et monnaies ayant cours légal, échanges entre crypto-actifs, conservation, conseil.

Le débat n'est pas tranché. Ce statut doit-il être obligatoire, comme c'est le cas aujourd'hui lorsqu'on veut offrir des services de paiement ? Est-ce qu'il faut faire de même pour ce type d'actifs, dont j'ai expliqué que ce n'est pas de la monnaie, et dont l'enjeu est différent ? Le projet PACTE veut encadrer les marchés primaire et secondaire sans tuer l'initiative. Il y a derrière ces efforts une ambition politique : permettre le développement de l'écosystème des actifs numériques en France aussi.

Plus largement, au plan de la stabilité financière, l'enjeu est assez limité à ce stade. Notre action consiste à suivre ce qu'il se passe, à l'aide d'indicateurs mesurant le phénomène des crypto-actifs. Toutefois, il y a beaucoup de lacunes dans la couverture statistique des activités liées

aux crypto-actifs. Un vrai effort reste à faire au plan international afin de mettre à la disposition des autorités une batterie d'indicateurs et de méthodes communes couvrant aussi bien l'Asie et les États-Unis que l'Europe.

Je souhaiterais conclure en évoquant les défis liés à la technologie qui sous-tend le bitcoin, c'est-à-dire la blockchain. Compte tenu des risques et des insuffisances de ces instruments financiers dont on ne souhaite pas cependant entraver le développement, il s'agit pour les autorités de trouver le bon équilibre entre innovation et sécurité et de réglementer en articulant ces deux impératifs. On sait faire aujourd'hui la part entre les aspects à surveiller dans l'utilisation du bitcoin et les apports possibles de la blockchain, si elle était appliquée à d'autres domaines. C'est le sens de certaines expérimentations menées actuellement. Nous avons mis en production à la Banque de France, après l'avoir évaluée, une blockchain pour gérer les identifiants des créanciers SEPA, à laquelle participent plusieurs établissements bancaires de la place de Paris, et qui est ouverte *de facto* à l'ensemble des établissements bancaires. Plus précisément, un des métiers de la Banque de France consiste à gérer pour le compte de la communauté bancaire et financière de gros fichiers, comme celui qui contient les identifiants des entreprises qui se font payer sous forme de prélèvements SEPA. Ce fichier, qui existe depuis quelques années, était géré assez largement de façon manuelle. La blockchain apporte plus de sécurité dans la gestion du fichier, ainsi que plus de rapidité dans les mises à jour et les consultations. Là où il fallait plusieurs

jours pour que telle ou telle partie obtienne les informations nécessaires sur son créancier afin de le payer, cela se fait aujourd'hui de façon quasi-instantanée. Donc, la blockchain appliquée à ce cas d'usage, cela fonctionne et c'est utile. Notre démarche est modeste, nous avons fait ce qui nous paraissait le plus facile. On peut envisager d'autres cas d'application dans le secteur financier. En particulier, certaines opérations de post marché demeurent lentes et chères. Des projets qui visent à les rendre plus efficaces grâce à la blockchain sont en cours sur la place de Paris, dont certains vont devenir des réalités concrètes d'ici la fin de l'année pour le règlement-livraison de titres de créances négociables, également dénommés NEU-CP ou papier commercial à la française. Il y a d'autres initiatives aussi, en cours sur d'autres segments du marché, tels les titres émis par les PME. Au plan européen, il convient de noter la coopération entre la BCE et la Banque du Japon, pour réfléchir à l'intérêt et la faisabilité d'un système de paiement adossé à une blockchain. Cependant, dans ce domaine, l'apport de la blockchain n'est pas immédiat. En effet, les grands systèmes de paiement actuels permettent de faire du paiement en temps réel et de réaliser des dizaines de milliers de transactions à la seconde. Utiliser une blockchain dans ce contexte serait revenir cinquante ans en arrière. Autrement dit, il faut savoir évacuer l'écume et examiner concrètement les avantages et inconvénients de la blockchain par rapport à l'existant. En matière de paiement, la blockchain n'a guère de sens, pour le moment. Il y a d'autres domaines d'application. J'en ai présenté un concernant la Banque de France, mais ce qu'il faut

retenir, c'est qu'on en est encore largement au stade de l'expérimentation. La blockchain à grande échelle dans le secteur financier, ce ne sera pas avant quelques années.

Ceci dit, pour ne pas finir sur une note négative, je me tourne vers un sujet qui est déjà sur le métier : l'émission de monnaie digitale par les banques centrales. Que se passerait-il si ceux qui créent des instruments de transaction numériques au sein de communautés données n'étaient plus des acteurs privés mais les banques centrales elles-mêmes, dans le but de rendre leur processus d'émission monétaire plus efficace ?

La Banque de Suède a ainsi lancé un projet en ce sens, alors qu'elle fait le constat que les consommateurs utilisent de moins en moins d'espèces pour régler leurs achats. Elle envisage en particulier un scénario de crise dans lequel les consommateurs ne pourraient plus se fournir en espèces. Une monnaie digitale pourrait alors servir de dispositif de secours pour permettre la continuité des transactions et répondre aux besoins de l'économie. Dans la zone euro où les espèces servent encore à payer environ 80 % des achats en volume et 50 % des achats en valeur, il n'y a pas à ce jour de travaux précis en cours sur ce sujet. En outre dans ce contexte, caractérisé par le poids largement prédominant des banques dans le financement de l'économie, l'introduction éventuelle d'une monnaie digitale de banque centrale nécessiterait d'en examiner au préalable les conséquences sur le rôle de l'intermédiation bancaire, ainsi qu'en matière d'inclusion financière. On parle des crypto-actifs et des activités qui

en dépendent comme d'une sorte de nouvel Eldorado. Mais il faut garder en tête qu'un certain nombre de nos concitoyens butent encore sur l'utilisation de la carte, ce qui appelle naturellement à la prudence sur ce qui se passerait si demain on leur offrait d'utiliser des billets de banque digitaux.

Débat

Jean-Claude Seys : *Vous avez mentionné les ICO. Je ne suis pas certain que tout le monde sache de quoi il s'agit. Pourriez-vous en donner une explication plus synthétique, une définition ?*

Georges Gonthier : Si on veut comprendre le bitcoin, il faut l'utiliser, et si on veut comprendre l'ICO, il faut rencontrer ceux qui montent des ICO. Prenons l'exemple d'un projet à financer pour optimiser l'accès aux structures sportives, type gymnase, etc. Vous avez déjà des systèmes d'abonnement et de carte. Ce que des entrepreneurs que j'ai rencontrés essayent de mettre en place, c'est la possibilité de réutiliser les avoirs sur tel gymnase de façon à disposer d'un système plus fluide, à même de permettre d'utiliser les avoirs ou les droits d'usage acquis dans tel gymnase ou centre sportif dans un autre.

Cela suppose une interconnexion qui pourrait se faire par une blockchain. Le client se rend sur un site Internet qui offre ce service et derrière vous avez cette blockchain qui vous permet d'organiser cet échange entre les droits d'usage que vous avez, sur tel ou tel centre sportif.

L'idée est de faire financer ce projet par ceux qui y souscrivent. C'est comme une entreprise qui entre en Bourse afin de lever des capitaux pour financer son activité. Elle va demander à un certain nombre d'investisseurs particuliers ou institutionnels de lui apporter ce financement sous forme d'actions en contrepartie d'une partie de la propriété de l'entreprise. Là, dans ce cas d'espèce, le jeton ne rend pas nécessairement celui qui le possède propriétaire d'une partie de l'entreprise, mais offre des avantages, comme, par exemple, l'acquisition d'autres jetons ou d'autres services offerts par cette plateforme ou par d'autres. Ces ICO se font souvent dans l'écosystème Ethereum. Lorsque vous entrez dans le monde d'Ethereum, vous avez accès à toute une gamme de services qui vous permettent de financer ou de payer ces jetons. L'acquisition de jetons se fait en contrepartie soit d'espèce ayant cours légal, euros ou dollars, soit de crypto-actifs, bitcoin, par exemple.

Il y a aujourd'hui un enjeu juridique pour les autorités des marchés financiers : ces jetons, sont-ils des instruments financiers classiques ? S'ils le sont, il y a déjà pour eux des dispositions légales. Mais si leur nature est différente, comment procède-t-on pour assurer la sécurisation de ces opérations ? C'est l'enjeu du projet PACTE.

Arnaud Bazin [4] ***:*** *Il y a un aspect que vous n'avez pas abordé : la fraude à l'impôt. Si on a des échanges entre particuliers, entre particuliers et entreprises et entre*

4. Sénateur, membre de la commission des finances du Sénat.

entreprises, qui se font sous la forme de trocs à travers des blockchains, on pourrait échapper à l'impôt. Pouvez-vous me dire quelques mots sur cette question, qui aurait dû intéresser les autorités nationales. Deuxième question, plus pratique : pourquoi est-il impossible de faire avec les crypto-actifs des paiements instantanés, comme avec la carte ? Enfin, quelle différence faites-vous entre les services de paiement en blockchain par monnaie digitale, dont vous dites qu'ils se font dans un cadre légal, et le paiement par carte bancaire qui ressemble fort à de la monnaie numérique ?

Ivan Odonnat : Résoudre la question fiscale est essentielle pour savoir comment encadrer l'utilisation des crypto-actifs. En fait, il y a plusieurs dimensions. En particulier une dimension comptable : comment enregistrer les opérations en crypto-actifs dans les comptes des entreprises ? Et une dimension fiscale : comment taxer ces opérations en fonction de leur nature ? L'enjeu est la nature juridique de l'actif et de l'opération. Pour le moment, il n'y a pas de convention claire pour définir ces actifs. Cette question n'est pas encore tranchée. Une discussion est en cours et l'ambition du ministre est qu'avant la fin de l'année on ait une vision claire de ce sujet. Mais il est difficile d'avancer sans être sûr que le traitement de ce problème sera cohérent avec les solutions apportées dans les autres pays.

Concernant la fraude elle-même, des progrès sont encore à faire pour couvrir la fraude fiscale et le blanchiment de fraude fiscale. Deux aspects sont à considérer : ce

qu'il faut taxer et comment le taxer. Ces questions font actuellement l'objet d'une discussion en cours entre le service de la législation fiscale à Bercy et l'autorité des normes comptables.

S'agissant du peu d'intérêt que vous prêtez des autorités françaises pour le risque de fraude fiscale lié aux crypto-actifs, gardez en tête qu'il n'y a aujourd'hui en France que trois ou quatre plateformes d'échange, alors qu'on en compte environ 400 dans le monde, et qu'elles sont parmi les plus petites en montants de transactions. En effet, les transactions s'effectuent surtout au Royaume-Uni, aux Pays-Bas, à Luxembourg, à Malte, aux États-Unis et en Asie.

Georges Gonthier : Il est simple de comprendre pourquoi ces transactions sont si lentes : VISA prend le risque de la transaction et quelque part, historiquement, le bitcoin et ether ont été des monnaies conçues pour que le consensus reflète ce que seraient les opérations d'arbitrage interbancaire, qui ne sont pas instantanées. Ripple, la troisième crypto-monnaie importante, a été conçue essentiellement pour remplir cette fonction. Mais il y a des solutions algorithmiques, le sac de tours des informaticiens est très profond ! Il y a des expérimentations qui permettent de faire du paiement très rapide, même des micro-paiements, payer instantanément des fractions de centimes. Il s'agit juste d'avoir une méthode un peu différente. En fait, le bitcoin est une expérience qui a trop bien réussi, victime de son succès.

Une remarque concernant la confidentialité et la fraude. Les chaînes qui existent aujourd'hui sont des chaînes publiques, la seule source d'anonymat sont les pseudonymes utilisés pour les transactions. Ces pseudonymes ne sont pas difficiles à lever. C'est le même principe que pour l'accès aux sites Internet. Ce n'est pas gênant d'avoir des gens qui font leurs transactions sur des blockchains tant que ça laisse des traces. Cela dit, les informaticiens ont aussi des solutions pour rendre certaines chaînes totalement anonymes. Ils peuvent s'assurer que les transactions sont correctes sans savoir qui a fait quoi, ce qui peut être intéressant lorsqu'on souhaite révéler aux intéressés seulement le nom d'un payeur ou d'une fraction de la liste des payeurs sans donner accès à toute la liste des payeurs.

Ivan Odonnat : La carte est aujourd'hui un moyen de paiement extrêmement sécurisé, qui permet d'offrir des services d'une grande efficacité. Mais la société évolue et il y a une demande pour la numérisation. La question est de savoir si demain le billet de banque peut être numérisé, de telle sorte qu'au lieu d'avoir dans votre poche des billets en papier, vous disposiez d'un portefeuille électronique à la Banque centrale ou dans une banque commerciale. Ce sont des questions qu'on se pose aujourd'hui parce que le monde change et évolue.

Georges Gonthier : J'ajouterais que la carte est un service qui fonctionne de manière complètement centralisée. Vos capacités de paiement dépendent du bon fonctionnement du réseau VISA ou Mastercard. Complè-

tement décentralisé, le fonctionnement d'une monnaie électronique est beaucoup plus fiable. En dépit des moyens énormes mis en place pour que la carte fonctionne correctement, le système tombe quand même assez régulièrement en panne. Le souci des Suédois est de se demander ce qu'on fait si on ne dispose pas de liquidités, pour que la société continue à fonctionner même dans le cas d'une panne prolongée du réseau de paiement bancaire.

Michel Aglietta [5] ***:*** *Les gens qui travaillent sur la blockchain, etc. ne savent pas ce que c'est que la monnaie, c'est ça le problème. Fonder une monnaie exclusivement sur un protocole technologique présuppose que la société se réduit à l'ensemble de ses membres et de leurs relations. Or c'est complètement faux : la société, c'est une puissance collective distincte de ses membres et c'est pour cette raison que ce qui fait fonctionner la société, ce sont les institutions. Étant elle-même une institution, la monnaie ne peut absolument pas être le produit d'un processus purement privé. Cela ne remet pas en cause la blockchain. Il faut néanmoins distinguer entre ce que les anglo-saxons appellent permissionless blockchain, qui ne mènera pas à grand-chose, et permissioned blockchain. Parmi toutes les difficultés évoquées à propos de la blockchain, on n'en a pas cité une qui est sans doute la plus importante : la consommation de carbone. Les*

5. Professeur émérite de sciences économiques à l'université Paris X, conseiller scientifique au CEPII, membre de l'Institut universitaire de France et professeur de macroéconomie au sein de la majeure Sustainability and Social Innovation de l'HEC Paris.

sociétés humaines sont aujourd'hui devant ce problème qui peut mener à une catastrophe fondamentale et on est en train de nous dire que la blockchain peut remplacer les milliards de transactions qui se font par les monnaies existantes. C'est absurde. Peut-être que dans les décennies à venir il y aura des ordinateurs quantiques qui permettront d'éviter ça, mais c'est absurde de travailler là-dessus aujourd'hui. C'est une des raisons pour lesquelles le gouvernement chinois a déjà fermé une plateforme essentielle, étant donné que sa politique bas carbone devient prépondérante. D'autre part, au fur et à mesure que se développe ce processus de vérification par les mineurs, les Chinois se sont aperçus que le processus de minage devient extraordinairement concentré. Un pouvoir privé remplace l'autorité publique. Vous avez des fermes de minage gigantesques, ce qui soulève un problème fondamental : pour définir une monnaie et pour faire que celle-ci soit effectivement l'actif sûr en permanence et assurer la stabilité de l'unité de compte il est impossible de se passer de la centralisation. Avec le bitcoin, ce n'est pas possible de le faire parce que cela suppose une autorité légitime qui la maintient, et un actif sûr en permanence. C'est là qu'on retrouve la notion de liquidité et je veux qu'on m'explique comment cela peut se faire avec, simplement, un protocole technique, sans l'aval d'une autorité centrale.

Georges Gonthier : J'ai traduit *permissioned* et *permissionless* par fermé et ouvert. J'ai essayé d'expliquer que le problème de la consommation électrique est un accident historique. La situation d'aujourd'hui sera dé-

passée dans quelques années en changeant d'algorithme. Une des monnaies émergentes, EOS, essaie de le faire. Il faut faire la part des choses entre l'héritage technique du passé et ce qui est vraiment intrinsèque au problème. On n'a pas besoin d'une puissance de calcul phénoménale pour faire toutes les transactions financières de la planète. Le choix technique de la preuve de travail et les choix techniques du bitcoin ont été particulièrement mauvais, mais il était difficile pour l'inventeur du système de prévoir toutes les conséquences de son invention.

Ivan Odonnat : Je partage les critiques de Michel Aglietta mais je lui renvoie la question : pourquoi ne pas interdire le bitcoin ? Les Chinois ont interdit les ICO et, confrontés à un engouement excessif dans l'utilisation dans ces crypto-monnaies, les Coréens ont pris des mesures coercitives, qu'ils ont abandonnées depuis.

Faut-il interdire le bitcoin compte tenu des critiques que vous faites et que je partage ? Je n'ai pas de réponse absolue à cette question. J'observe simplement que la technologie progresse. La blockchain et les registres distribués, ce n'est pas nouveau. L'innovation progresse continuellement. Notre préoccupation aujourd'hui à la Banque de France est de ne pas être à rebours de la société, de la demande pour le digital, y compris en matière d'émission et de gestion d'actifs. Alors faut-il interdire le bitcoin ou faire autre chose ?

Michel Aglietta : *Je pense qu'il faut intégrer les monnaies particulières à l'intérieur d'un système monétaire*

organisé, avec une entité légitime qui permet d'assurer l'intégrité de l'unité de compte. On peut concevoir des monnaies partielles convertibles dans la monnaie supérieure, des monnaies dont le mode de formation pourrait être digital. Dans ce domaine on peut faire des progrès considérables, mais ce sont des monnaies complémentaires, qui ne remplacent pas le système monétaire. Il peut y avoir des développements tout à fait intéressants. C'est sans doute ce qu'avait en tête Tirole : le retour des communs dans des collectivités qui assument leur souveraineté sur ces problèmes qui sont les leurs, en particulier concernant la biodiversité sur des territoires particuliers, etc. Cela demande des investissements considérables et un système d'échanges qui permet ces réalisations, reconnu comme quelque chose de collectif. Là, ce type de technologie peut s'avérer utile. Mais cela ne peut pas remplacer la souveraineté de la monnaie, c'est complètement absurde.

Jacques Galvani [6] ***:*** *Quand je vous écoutais, je me disais que le directeur des grands systèmes d'IBM des années 1950 aurait probablement dit la même chose sur l'apparition de ces petits trucs qui à l'époque s'appelaient les microordinateurs, et qui étaient une très petite part du marché. On se disait que cela ne concernait que quelques personnes et ne remplacerait jamais les grands systèmes centralisés, absolument indispensables au fonctionnement économique. Ma question est simple : qu'est-ce que ça implique pour nous en tant que régula-*

6. Directeur associé de Schoolab, laboratoire d'innovations.

teurs, en matière de transformation de nos modes de fonctionnement, de notre culture, et même du type d'employés censés faire cette régulation ? Est-ce que vous intégrez ces questions en vous disant que dans trente, quarante ou cinquante ans les crypto-monnaies représenteront 70 %, 80 % ou 90 % des monnaies ?

Philippe Pajot [7] ***:*** *J'ai une question plus technique, pour Georges Gonthier. En ce moment on est en train de réfléchir en cryptographie à l'ère des ordinateurs quantiques. Est-ce que ces ordinateurs quantiques ne risquent pas de rendre obsolète la blockchain ?*

Georges Gonthier : La réponse est mixte. Pour tout ce qui est cryptologie et vérification d'identité, les algorithmes utilisés maintenant sont attaquables par les ordinateurs quantiques. Le mécanisme de la blockchain et le hachage cryptographique, eux, ne le sont pas. Les ordinateurs quantiques n'auront pas beaucoup plus de chances que les ordinateurs classiques de trouver des collisions de hachage. La blockchain elle-même est sûre : le mécanisme qui permet de s'appuyer sur le passé de manière efficace, en ayant un résumé compact d'un historique complet va continuer à bien fonctionner. En revanche, tout ce qui est preuve d'identité devra s'adapter, mais alors ce sera le cas de l'ensemble de la société parce que ce sont les mêmes algorithmes qui sont utilisés pour les échanges interbancaires.

7. Rédacteur en chef de La Recherche.

Philippe Lagayette [8] ***:*** *C'est très intéressant de voir qu'on s'efforce de séparer les innovations possibles dans le monde de la blockchain et les crypto-monnaies dans leur aspect monétaire. Cela prouve qu'il y avait toutes les raisons d'interdire le bitcoin, comme Michel Aglietta l'a bien illustré. Les autorités passent leur temps à lutter contre l'anonymat et l'instabilité or le bitcoin est un facteur d'anonymat et d'instabilité. Si on n'a pas interdit le Bitcoin, au-delà des raisons invoquées, c'est pour une autre raison, plus profonde : il y a des choses qui se développent dans le côté obscur de la Force et qu'il nous est difficile de contrôler. Les gens qui font ces innovations ignorent totalement les notions de frontière et d'État, là où des gens ayant la responsabilité de la société agissent dans le cadre d'un monde institutionnel, réglementé, bureaucratique.*

Marie-Françoise Aufrère [9] ***:*** *Vous avez dit qu'il y a peu de risques que le bitcoin mette en danger le système financier parce qu'il y a peu de plateformes. Ce qui signifie qu'il s'agit d'un rapport de force. Mais celui-ci peut être inversé. Dans ce cas, le bitcoin pourrait contribuer à l'effondrement du système bancaire ?*

Ivan Odonnat : Nous n'avons pas, à la Banque de France, de vision particulière du monde de demain. En revanche, nous essayons de faire notre métier d'une façon aussi efficace que possible au service de la croissance,

8. Ancien banquier central.
9. Philosophe.

en France et en Europe, pour avoir une meilleure orientation de l'épargne et financer les entreprises, les projets. Il y a aujourd'hui au sein de la zone euro un excédent d'épargne de l'ordre de 400 milliards d'euros. Cette épargne pourrait être mieux utilisée au service de l'innovation et du développement. L'innovation est un processus complexe. Pourquoi le VHS a supplanté le Bétamax qui était un procédé technologiquement plus avancé dans le monde des magnétoscopes ? Ce n'est pas à la Banque de France et aux autorités de dire dans quel sens doit se développer l'innovation. Notre préoccupation est de savoir dans quelle mesure l'innovation crée de l'instabilité pour le système financier et menace le bon financement et le développement de l'économie. Notre action consiste simplement à intervenir à travers la politique monétaire et à maintenir la stabilité financière et dans le cas d'espèce, trouver un équilibre entre innovation et stabilité. L'innovation nous inquiète seulement si elle met en cause la stabilité du système financier. Il s'agit d'assurer une action cohérente dans le temps et dans l'espace, et reposant sur quelques principes. Nous évitons de créer des situations d'arbitrage réglementaire. Nous ne sommes pas favorables à une approche du type bac à sable, où l'expérimentation porte sur un domaine limité, et mobilise un nombre restreint d'acteurs bénéficiant d'un encadrement réglementaire plus souple que celui appliqué aux autres acteurs du système financier ou économique. Nous assurons une proportionnalité entre le risque et le niveau de réglementation, pour permettre l'émergence de petits acteurs, plus ou moins bien organisés, plus ou

moins bien protégés contre le risque de cyber-attaque ou d'autres formes de risque. Nous mesurons les risques auxquels ces entrants sont exposés sans nécessairement chercher à imposer des règles aussi drastiques que celles appliquées aux institutions établies. Nous tenons compte de leur taille et de leur empreinte sur le système financier. Vis-à-vis de l'innovation, nous sommes neutres, évitant de favoriser telle innovation plutôt que telle autre. Ce n'est pas notre rôle de décider comment la société doit évoluer. Plus généralement la préoccupation des autorités est de protéger les consommateurs, de sécuriser leurs données individuelles, de défendre les grands principes de fonctionnement de l'Union européenne, de veiller à la protection contre les cyber-attaques. Je ne sais pas ce que deviendront les crypto-actifs demain, mais il est clair qu'aujourd'hui ce n'est pas de la monnaie.

Cela étant dit, il est probable que nous n'ayons pas encore trouvé la bonne réponse à la frénésie relative au bitcoin. Toutes les autorités financières ont signalé les défauts et alerté sur les dangers du bitcoin, sans effet significatif sur l'évolution du cours. Mais je n'y vois pas une incapacité de notre part à maîtriser les évolutions financières et les risques liés à l'action des différents acteurs. Le fonctionnement du système financier est quelque chose d'extrêmement complexe. Dix ans après une crise financière d'une gravité inusitée, c'est l'heure du bilan. On a effectué énormément de progrès, mais le monde continue d'évoluer. On parle beaucoup des crypto-actifs, mais il faut surtout noter les changements importants induits par le développement des paiements instantanés.

C'est cela la réalité du consommateur, pas le bitcoin. Je crois que nous avons su nous adapter. La Banque de France en particulier a changé dans sa façon de fonctionner. Elle dialogue davantage avec les entrepreneurs, y compris dans le monde des crypto-actifs. Nous écoutons, nous essayons de comprendre, et nous jugeons sur pièce. Je ne dis pas qu'il n'y aura plus de crise financière. L'économie fonctionne par cycles et on ne sait pas identifier ex ante certains risques. On demande aux banques et aux établissements financiers de se projeter au mieux, d'augmenter leur charge en capital, ce qui est une façon d'accroître les absorbeurs de choc. En France, en dix ans, le capital des banques a doublé, donc ce qu'elles peuvent faire pour gérer leurs risques, aujourd'hui, est deux fois mieux que ce qu'elles pouvaient faire à l'époque, qui n'était déjà pas si mal. Personnellement, s'il y a une chose que je retiens de ces trente années passées à la Banque de France, c'est que l'innovation financière est permanente. Vous ne savez jamais d'où elle vient, ni comment elle va évoluer. Quand elle survient, vous ne l'avez pas forcément anticipée. Il faut simplement être capable de réagir vite, de comprendre, d'orienter, d'identifier les risques et les contenir. À cet effet, on suit les évolutions en cours aussi étroitement que possible. C'est un exercice difficile dans le cas des crypto-actifs, mais on commence à avoir de l'information. Pour cela, il faut obliger les acteurs à s'identifier, à déclarer leurs activités. A titre d'illustration, nous expliquons aux banques pourquoi il faut accepter les fintech qui offrent des services de paiement dans le cadre d'un statut défini au plan européen, sans être des

banques, sans posséder les comptes des consommateurs dans leurs livres. Ce statut permet de connaître et suivre ces nouveaux acteurs. Je pense que c'est une situation infiniment meilleure en termes de gestion des risques qu'une situation où ces nouvelles activités de paiement se développeraient de façon anarchique, et qu'une démarche similaire devrait être appliquée aux opérations sur crypto-actifs.

Philippe Lagayette : *Notre société déploie son activité dans le développement durable, notamment dans l'électromobilité. Nous avons créé un business model qui permet de déployer les 100 000 bornes de recharge électrique en France sans faire appel à l'argent des collectivités. Dans ce modèle économique, nous nous appuyons en partie sur la blockchain pour faire la gestion intelligente des charges des véhicules électriques. Nous nous intéressons à des start-ups qui peuvent implémenter ces blockchains au niveau de notre réseau de bornes, et là on est confrontés à trois questions : la sécurité, la latence, car nous voulons que la décharge des transactions se fasse en quelques secondes, et la consommation puisqu'on est dans le développement durable. Si on parle de blockchain avec du minage dans le développement durable, ce n'est pas terrible. Il existe des start-ups en France qui ont des solutions, que nous essayons aujourd'hui, sur différents matériels, mais c'est vrai qu'on est assez limités dans le fait de pouvoir qualifier ces blockchains. Comment qualifier les blockchains en France, sous quelle forme ?*

Ivan Odonnat : C'est un des points traités dans le projet de loi PACTE actuellement en discussion au parlement, plus précisément par les dispositions relatives aux ICO qui visent à offrir sous la forme d'un label optionnel suffisamment de garanties sur le projet concerné et la blockchain sous-jacente ? La garantie devrait notamment impliquer un avis de sécurité rendu par l'ANSSI (Agence nationale de la sécurité des systèmes d'information).

Georges Gonthier : Je pense que ce problème n'est pas propre aux blockchains, mais concerne plutôt la qualité des logiciels. Le plus sûr serait de s'appuyer sur les normes qui existent en matière de certification de logiciels. Certains acteurs de la blockchain essaient d'ailleurs d'aller vers le niveau le plus élevé, où l'on a une preuve mathématique de correction, une vérification mécanique du bon fonctionnement. La blockchain pose un problème sérieux parce que beaucoup de plateformes des blockchains souffrent d'un défaut assez flagrant de qualité de logiciel. Les solutions sont en fait à chercher du côté de la sûreté du logiciel.

Les publications de l'Institut Diderot

Dans la même collection

- **L'avenir de l'automobile** - Louis Schweitzer
- **Les nanotechnologies & l'avenir de l'homme** - Etienne Klein
- **L'avenir de la croissance** - Bernard Stiegler
- **L'avenir de la régénération cérébrale** - Alain Prochiantz
- **L'avenir de l'Europe** - Franck Debié
- **L'avenir de la cybersécurité** - Nicolas Arpagian
- **L'avenir de la population française** - François Héran
- **L'avenir de la cancérologie** - François Goldwasser
- **L'avenir de la prédiction** - Henri Atlan
- **L'avenir de l'aménagement des territoires** - Jérôme Monod
- **L'avenir de la démocratie** - Dominique Schnapper
- **L'avenir du capitalisme** - Bernard Maris
- **L'avenir de la dépendance** - Florence Lustman
- **L'avenir de l'alimentation** - Marion Guillou
- **L'avenir des humanités** - Jean-François Pradeau
- **L'avenir des villes** - Thierry Paquot
- **L'avenir du droit international** - Monique Chemillier-Gendreau
- **L'avenir de la famille** - Boris Cyrulnik
- **L'avenir du populisme** - Dominique Reynié
- **L'avenir de la puissance chinoise** - Jean-Luc Domenach
- **L'avenir de l'économie sociale** - Jean-Claude Seys
- **L'avenir de la vie privée dans la société numérique** - Alex Türk
- **L'avenir de l'hôpital public** - Bernard Granger
- **L'avenir de la guerre** - Henri Bentegeat & Rony Brauman
- **L'avenir de la politique industrielle française** - Louis Gallois
- **L'avenir de la politique énergétique française** - Pierre Papon
- **L'avenir du pétrole** - Claude Mandil
- **L'avenir de l'euro et de la BCE** - Henri Guaino & Denis Kessler
- **L'avenir de la propriété intellectuelle** - Denis Olivennes
- **L'avenir du travail** - Dominique Méda
- **L'avenir de l'anti-science** - Alexandre Moatti
- **L'avenir du logement** - Olivier Mitterand

- L'avenir de la mondialisation - Jean-Pierre Chevènement
- L'avenir de la lutte contre la pauvreté - François Chérèque
- L'avenir du climat - Jean Jouzel
- L'avenir de la nouvelle Russie - Alexandre Adler
- L'avenir de la politique - Alain Juppé
- L'avenir des Big-Data - Kenneth Cukier & Dominique Leglu
- L'avenir de l'organisation des Entreprises - Guillaume Poitrinal
- L'avenir de l'enseignement du fait religieux dans l'École laïque - Régis Debray
- L'avenir des inégalités - Hervé Le Bras
- L'avenir de la diplomatie - Pierre Grosser
- L'avenir des relations Franco-Russes - S.E Alexandre Orlov
- L'avenir du Parlement - François Cornut-Gentille
- L'avenir du terrorisme - Alain Bauer
- L'avenir du politiquement correct - André Comte-Sponville & Dominique Lecourt
- L'avenir de la zone euro - Michel Aglietta & Jacques Sapir
- L'avenir du conflit entre chiite et sunnites - Anne-Clémentine Larroque
- L'Iran et son avenir - S.E Ali Ahani
- L'avenir de l'enseignement - François-Xavier Bellamy
- L'avenir du travail à l'âge du numérique - Bruno Mettling
- L'avenir de la géopolitique - Hubert Védrine
- L'avenir des armées françaises - Vincent Desportes
- L'avenir de la paix - Dominique de Villepin
- L'avenir des relations franco-chinoises - S.E. Zhai Jun
- Le défi de l'islam de France - Jean-Pierre Chevènement
- L'avenir de l'humanitaire - Olivier Berthe - Rony Brauman - Xavier Emmanuelli
- L'avenir de la crise du Golfe entre le Quatar et ses voisins
  Georges Malbrunot
- L'avenir du Grand Paris - Philippe Yvin
- Entre autonomie et Interdit : comment lutter contre l'obésité ?
  Nicolas Bouzou & Alain Coulomb
- L'avenir de la Corée du Nord - Juliette Morillot & Antoine Bondaz
- L'avenir de la justice sociale - Laurent Berger
- Quelles menaces numériques dans un monde hyperconnecté ?
  Nicolas Arpagian
- L'avenir de la Bioéthique - Jean Leonetti
- Données personnelles : pour un droit de propriété ?
  Pierre Bellanger et Gaspard Koenig
- Quels défis pour l'Algérie d'aujourd'hui ? - Pierre Vermeren
- Turquie : perspectives européennes et régionales - S.E Ismail Hakki Musa

Les Notes de l'Institut Diderot

- L'euthanasie, à travers le cas de Vincent Humbert - Emmanuel Halais
- Le futur de la procréation - Pascal Nouvel
- La République à l'épreuve du communautarisme - Eric Keslassy
- Proposition pour la Chine - Pierre-Louis Ménard

- L'habitat en utopie - Thierry Paquot
- Une Assemblée nationale plus représentative - Eric Keslassy
- Où va l'Égypte ? - Ismaïl Serageldin
- Sur le service civique - Jean-Pierre Gualezzi
- La recherche en France et en Allemagne - Michèle Vallenthini
- Le fanatisme - Texte d'Alexandre Deleyre présenté par Dominique Lecourt
- De l'antisémitisme en France - Eric Keslassy
- Je suis Charlie. Un an après... - Patrick Autréaux
- Attachement, trauma et résilience - Boris Cyrulnik
- La droite est-elle prête pour 2017 ? - Alexis Feertchak
- Réinventer le travail sans l'emploi - Ariel Kyrou
- Crise de l'École française - Jean-Hugues Barthélémy
- À propos du revenu universel - Alexis Feertchak & Gaspard Koenig
- Une Assemblée nationale plus représentative - *Mandature 2017-2022* - Eric Keslassy
- L'avenir de notre modèle social français - Jacky Bontems & Aude de Castet
- Handicap et République - Pierre Gallix
- Réflexions sur la recherche française... - Raymond Piccoli
- Le système de santé privé en Espagne : quels enseignements pour la France ? Didier Bazzocchi & Arnaud Chneiweiss
- Le maquis des aides sociales - Jean-Pierre Gualezzi
- Réformer les retraites c'est transformer la société Jacky Bontems & Aude de Castet
- Vers un droit du travail 3.0 - Nicolas Dulac
- Burn-out : le mal du siècle ? - Philippe Fossati & François Marchand
- L'avenir de la loi de 1905 sur la séparation des Églises et de l'État Jean-Philippe Hubsch

Les Dîners de l'Institut Diderot

- La Prospective, de demain à aujourd'hui - Nathalie Kosciusko-Morizet
- Politique de santé : répondre aux défis de demain - Claude Evin
- La réforme de la santé aux États-Unis : quels enseignements pour l'assurance maladie française ? - Victor Rodwin
- La question du médicament - Philippe Even
- La décision en droit de santé - Didier Truchet
- Le corps ce grand oublié de la parité - Claudine Junien
- Des guerres à venir ? - Philippe Fabry
- Les traitements de la maladie de Parkinson - Alim-Louis Benabib

Les Entretiens de l'Institut Diderot

- L'avenir du progrès (actes des Entretiens 2011)
- Les 18-24 ans et l'avenir de la politique

L'avenir du bitcoin et de la blockchain

Monnaie virtuelle lancée en 2009, le bitcoin est l'application la plus connue de ce qu'on appelle la blockchain. Il s'agit d'une technologie qui permet de créer des systèmes qui ne sont contrôlés par aucune autorité unique.

Le bitcoin promettait des plus-values mirobolantes. En novembre 2017, son cours évoluait vers les 20 000 $; les médias consacraient de nombreux articles à cette cryptomonnaie et de respectables institutions financières annonçaient qu'elles étudiaient son utilisation éventuelle.

Aujourd'hui, la blockchain poursuit sa carrière en rendant la falsification des données difficile. Cette technologie révolutionne la manière dont les individus et les organisations échangent et stockent de la valeur, mais son défaut capital consiste en une consommation élevée d'énergie et, de son côté, le bitcoin ne vaut plus qu'un quart de sa valeur de la fin 2017.

Le débat entre nos invités, Ivan Odonnat et Georges Gonthier permet d'apporter les éléments de réflexion indispensables pour saisir le phénomène dans sa globalité.

Georges GONTHIER,

Directeur de recherches à l'INRIA - Institut de Recherche en Sciences du Numérique - Saclay Île-de-France

Ivan ODONNAT,

Adjoint au Directeur général de la Stabilité Financière et des opérations de la Banque de France

INSTITUT DIDEROT

ISBN 979-10-93704-56-2

ISSN 2496-4948 (en ligne)
ISSN-2608-1334 (imprimé)

Réalisation www.idcomm.fr - Imprimé sur papier issu de forêts gérées durablement.