CRYPTOMONNAIES ET TECHNOLOGIE DE LA BLOCKCHAIN.

• Le qualificatif à utiliser pour évoquer ces « monnaies » très particulières comme le bitcoin dont on parle beaucoup et qui se créent depuis une vingtaine d'années en marge de la création des monnaies bancaires n'est pas simple. En tous les cas, il faut éviter le qualificatif d'électronique. En effet, toutes les monnaies, que ce soit celle de la Banque centrale ou celles des banques commerciales sont électroniques en ce sens qu'elles sont inscrites sur des supports d'enregistrement numérique. Rappelons ici que de même que les chèques, cartes de paiement, ordres de virement, … sont des instruments qui permettent de mobiliser les monnaies inscrites dans des comptes de passif des banques commerciales, les billets peuvent être considérés eux-mêmes comme les instruments qui permettent de mobiliser la monnaie légale inscrite dans les comptes de passif de la Banque centrale ; et que ces comptes bancaires ne sont plus tenus depuis longtemps dans des « grands-livres » mais sur des supports magnétiques. Rappelons aussi ici que toute monnaie, qu'elle soit de Banque centrale ou de banque commerciale, est à la fois fiduciaire quant à sa valeur (la confiance est le maître mot de la science monétaire et financière) et scripturale quant à sa production puisqu'elle est inscrite en compte et qu'elle circule par jeu d'écritures.
On pourrait qualifier aussi ces « cryptomonnaies » de monnaies « parallèles » ou complémentaires puisqu'elles côtoient les monnaies bancaires, officielles. Mais ce ne sont pas les seules monnaies « parallèles : en effet, les « monnaies locales », les Lets et autres SEL, en sont aussi. Mais, et c'est très important, ni les unes ni les autres ne sont des monnaies pleines et entières, pour au moins trois raisons. La première raison est que ces « monnaies » ne remplissent pas les 7 fonctions qu'une monnaie doit remplir (voir ici le document sur ce thème), y compris les 3 fonctions utilitaires traditionnelles (fonction de compte, fonction de paiement, fonction d'épargne) : les monnaies locales ne sont que des instruments de paiement et les cryptomonnaies sont de fait des actifs de spéculation (d'ailleurs, la Banque de France préfère les appeler « cryptoactifs » plutôt que cryptomonnaies). La deuxième raison est que ces monnaies ne sont légitimées par aucun pouvoir politique ; or, c'est un pouvoir régalien que de « frapper monnaie », surtout que la monnaie est un bien commun, un bien public. La troisième raison est que ces « monnaies » constituent uniquement du « cash » : elles cassent le lien entre monnaie et finance puisqu'elles ne permettent pas, comme le font les monnaies bancaires, de pré-financer l'activité économique par l'intermédiaire du crédit. Notons toutefois que les ICO (Initial Coin Offerings » constituent de nouveaux modes de financement qui utilisent les coins et la technologie des cryptomonnaies, la blockchain. Actuellement, les autorités de régulation financière sont partout très opposées au développement des ICO parce qu'elles y attachent beaucoup de risques. Mais, dès 2018, la France souhaite se démarquer des autres pays en accompagnant cette innovation technologique importante : le gouvernement désire jouer les précurseurs en légiférant vite sur ces nouveaux produits. L'AMF et le ministère de l'économie et des finances travaillent à la mise en place pour les ICO d'un cadre souple, adapté et incitatif.
• Lets, que l'on a traduit par « Local exchange tip system », alors que le sens originel était simplement « let's do it », est parti vers 1982 d'un Canadien, Michael Lynton, écossais d'origine qui vivait dans une vallée en crise près de Vancouver et qui a eu l'idée de créer un système de crédit mutuel, sans banque : pas de source extérieure, on se fait confiance. Chaque fois que j'achète quelque chose, c'est noté en moins et chaque fois que je vends quelque chose, c'est noté en plus. C'est l'échange qui crée spontanément la monnaie. Les Canadiens ont appelé leur monnaie parallèle « CC », pour « Community Currencies » et leur système fit des émules partout dans le monde. En France, sont nés les SEL, « système d'échange local ». Le 1er SEL est créé au Mans dans les années 1980 par Franck Fouqueray et son entreprise « Trader France » ; son système, appelé « Troc Temps », gérait les échanges de services entre les 500 adhérents par l'intermédiaire du Minitel. Un SEL est un système d'échange de biens ou de services qui se font au sein d'un groupe fermé, généralement associatif. La base de l'échange dans un SEL s'effectue à partir d'un accord de gré à gré, un accord mutuel entre les deux co-échangistes (P2P et C2C mais aussi, de plus en plus, B2C et B2B). Le SEL permet à toute individu d'échanger des

compétences, des savoir-faire et des produits avec les autres membres du groupe. Un SEL est un groupe de personnes vivant dans un même secteur géographique. Pour comptabiliser les échanges, le SEL crée sa propre monnaie, appelée unité d'échange, le plus souvent basée sur le temps. Ainsi, les Lets et SEL sont des formes intermédiaires entre le troc pur et l'échange entièrement monétaire.
Les créateurs d'un SEL cherchent à satisfaire des besoins qui ne sont pas satisfaits pour certaines personnes, et à recréer du lien entre les membres du groupe. Comme il s'agit le plus généralement d'échanger du temps, la valeur est simplifiée à l'extrême, de façon à favoriser la solidarité et le lien social. Une heure d'échange vaut une heure, que l'on ait fait une tâche qualifiée ou non ; on gagne 60 unités que l'on ait fait du nettoyage ou donner un cours de physique appliquée. Ainsi, le SEL supprime les hiérarchies dans les compétences. La monnaie des SEL est souvent limitée à sa fonction d'échange et d'unité de compte pour la sphère d'échanges considérée ; elle ne remplit pas la fonction d'épargne et par conséquent ne peut pas faire a priori l'objet de spéculation. L'intérêt fondamental du SEL est de favoriser le développement d'une économie solidaire et locale. Il peut aussi permettre la réinsertion de publics marginalisés. Chaque membre peut profiter de biens et de services en échange de son temps, en offrant bien sûr à son tour biens et services. Faire partie d'un SEL permet ainsi de sortir de l'isolement, de bénéficier d'un réseau d'entraide et de prendre conscience de ce que l'on a à offrir à d'autres personnes. Contrairement au troc, on n'est pas tenu de rendre à celui dont on reçoit : cette disposition élargit les possibilités d'échanges.
Pour que les échanges puissent avoir lieu, il est nécessaire que les membres du SEL soient tenus régulièrement au courant des offres et des demandes. Pour cela, il existe de nombreuses façons de faire : tours de table lors de réunions régulières, panneau d'affichage, liste papier, actualisation régulière des offres et des demandes dans le bulletin du SEL, et bien sûr un site Internet. Les sites Internet présentent l'avantage de permettre une circulation très rapide de l'information.
Les débits et les crédits sont enregistrés sur les comptes des adhérents. Le fournisseur du produit ou du service voit son solde augmenter pendant que celui du receveur diminue. Lorsque la comptabilité est centralisée, ce qui est a priori la solution la meilleure, il y a l'envoi des différentes feuilles d'échange à l'association gestionnaire. Mais pour que le système ne soit pas trop lourd, il faut qu'il soit automatisé, notamment par l'emploi d'un tableur sur ordinateur. Mais, s'il n'est pas automatisé, mieux vaut que la comptabilité soit décentralisée : elle est alors tenue à l'aide soit d'un bon d'échange en 3 parties qui est rempli lors de chaque échange (chaque coéchangiste a un volet et le 3ème est envoyé au service gestionnaire), soit une feuille d'échange – ou feuille d'échange partagée - où chaque coéchangiste remplit et signe la feuille de son partenaire, cette feuille étant envoyée tous les mois au service, soit avec un carnet d'échanges. Mais de plus en plus de SEL gèrent les échanges par l'intermédiaire de sites Internet, ce qui facilite la mise en commun des informations ainsi que les tâches comptables. Une transaction est par exemple enregistrée directement en ligne par deux membres ayant réalisé un échange, et les soldes sont calculés automatiquement.
• Depuis le milieu des années 2000, grâce aux NTIC, se sont développés des sites de troc en ligne, dont le pionnier aux EU est « peerfilix » et en Europe « digitroc ». Ces sites sont les descendants des SEL. Ces sites sont de vraies bourses de troc et vont donc plus loin que les simples sites d'annonces. Avec ces sites, de nouvelles fonctions apparaissent, voire de nouvelles philosophies de consommation : on veut éviter les gaspillages en donnant une deuxième vie aux objets, favoriser les circuits courts, avoir un style de vie plus écologique, plus solidaire, moins coûteux. C'est ce que l'on appelle la consommation collaborative, et de manière plus large l'économie de partage.
À ses débuts, cette nouvelle économie collaborative était porteuse d'un discours très positif et un peu utopique sur le social et l'environnement, discours que l'on peut retrouver dans les livres de Jeremy Rifkin comme la « Troisième Révolution industrielle ». Mais aujourd'hui, on passe de l'adolescence à l'âge adulte, et les acteurs les plus visibles sont les gros acteurs comme Airbnb. L'économie du partage permet d'étendre le domaine marchand et le domaine de la solidarité. Maintenant, la question c'est de savoir ce que l'on veut : développer de nouvelles formes d'échanges solidaires à côté du marché et de la monnaie, ou bien profiter de nouveaux services efficaces pour regagner un peu de pouvoir d'achat. L'économie du partage a toujours porté en elle cette contradiction entre utopie et big business. D'un côté, il y a une vision libertaire née de l'Internet social qui réunit des gens désireux d'échanger des biens et des services en pair à pair pour renouer du lien, redonner du sens à la consommation, au travail. En résumé : « Je partage mon logement, je te prête ma voiture ou ma tondeuse en échange d'un service, on jardine ensemble parce que c'est cool et que c'est bon pour le vivre-ensemble et l'environnement ». De

l'autre, il y a la vision marchande, voire ultralibérale, qui voit des entrepreneurs se positionner en intermédiaires pour développer cette nouvelle économie et en tirer un maximum de profits.

• Le point commun entre ces monnaies « locales » et les cryptomonnaies, qui sont souvent mondiales, est que ce sont des monnaies « contestataires ». Mais elles ne contestent pas la même chose ni de la même façon. Les monnaies locales contestent les modes dominants de production et de consommation et veulent promouvoir le lien social plutôt que la relation marchande, et ce sont des moyens de paiement, pas des instruments d'épargne ni a fortiori de spéculation. Par contre, les cryptomonnaies se fondent sur une philosophie libertarienne à tendance anarchisante en contestant les institutions monétaires et financières, le pouvoir monétaire que détiennent les Banques centrales, et le pouvoir politique des États qui légitime ce pouvoir monétaire. L'objectif de ceux qui créent des cryptomonnaies est d'instaurer un nouveau style de gouvernance plus participatif, transparent, efficace et équitable. C'est une équipe d'informaticiens, du nom de Satoshi Nakamoto, qui a créé le bitcoin en 2008-2009, c'est-à-dire précisément à la suite de la crise bancaire de 2007-2008, en quelque sorte comme une démonstration de défiance à l'égard des institutions financières et de leurs organismes de régulation et de supervision que sont les banques centrales. Pour Satoshi Nakamoto, la crise bancaire est avant tout une crise de la confiance que l'on mettait dans la fiabilité du système bancaire : « Ce dont nous avons besoin, c'est d'un système de paiement électronique basé sur des preuves cryptographiques au lieu du modèle basé sur la confiance, qui permettrait à deux parties qui le souhaitent de réaliser des transactions directement entre elles sans avoir recours à un tiers de confiance ». Notons que la technologie « blockchain » trouve ses racines dans des articles écrits au cours des années 1990, d'abord des cryptographes Stuart Haber et W. Scott Stornetta, en janvier 1991, puis de Ross J. Anderson en 1996, de Bruce Schneier et John Kelsey en 1998, et de Jean-Jacques Quisquater, Henri Massias et Xavier Serret-Avila en mai 1999. Notons aussi qu'en juin 1996, la NSA publie un rapport « comment produire de la monnaie : la cryptographie du cash électronique anonyme », et qu'en 1999, le prix Nobel d'économie Milton Friedman prédit la création future d'un e-cash fiable pour réaliser des transactions anonymes du Internet.

On peut considérer que ceux qui promeuvent les cryptomonnaies sont dans le même état d'esprit que les « cypherpunks » des années 1980-1990, jeu de mots utilisé pour appeler la liste de diffusion électronique utilisée par des personnes qui voulaient développer l'utilisation de la cryptogaphie de façon à faciliter la vie quotidienne au niveau individuel, en assurant le respect de la vie privée, tout en promouvant au niveau collectif un changement social et politique. Ce mouvement s'exprimera au travers de manifestes au cours des années 1990 : ceux de Tim May en 1992, (le « manifeste crypto-anarchiste »), d'Éric Hugues en 1993 (le « manifeste d'un cypherpunk ») et de Christian Kirtchev (le « cypherpunk manifesto »).

Cette contestation de l'ordre monétaire orthodoxe par les cryptomnnaies fait aussi penser à la théorie monétaire de F. Hayek. Comme l'écrit Gérard Dréan en septembre 2011 dans un document de l'Institut Turgot, « En 1976 (il avait alors 77 ans), Hayek estima urgent de prendre position contre le projet d'une monnaie européenne unique. Pour cela, il interrompit la rédaction du tome III de *Law Legislation and Liberty* pour écrire un livre méconnu intitulé « *Denationalisation of money : the argument refined* », où il propose comme alternative la libre concurrence entre monnaies. (…) Il en conclut que la stabilité monétaire serait mieux assurée par un régime de libre concurrence entre monnaies que par l'actuelle gestion étatique, et s'attache à le montrer en analysant ce qui se passerait vraisemblablement si les pays du Marché Commun s'engageaient réciproquement à ne plus mettre aucun obstacle à la libre circulation sur leurs territoires de leurs monnaies nationales ni au libre exercice de l'activité bancaire ». Il est donc logique que ces thèses de Hayek en termes de désétatisation de la monnaie et de concurrence entre monnaies soient évoquées à propos des cryptomonnaies.

• Alors que le fonctionnement des monnaies locales nécessite une comptabilité centralisée tenue de préférence mais pas nécessairement informatiquement pour enregistrer les transactions faites et pour tenir les comptes des adhérents, les cryptomonnaies nécessitent l'utilisation de l'informatique et mettent en œuvre un protocole très particulier qui vise, par principe, une décentralisation absolue de son fonctionnement et qui peut complètement se passer de tout organisme centralisé de contrôle et de régulation. De plus, quand il y a un transfert monétaire entre deux banques appartenant à deux zones monétaires différentes, il faut que la banque qui est à l'origine du transfert ait un compte dans la banque

d'arrivée (le « correspondant banking ») ; et chaque banque doit vérifier la véracité de toutes les informations concernant la transaction : c'est la « compliance ». Tout cela entraîne des frais coûteux. Le protocole que mettent en œuvre les cryptomonnaies est un instrument puissant non seulement de décentralisation mais aussi de dématérialisation et de désintermédiation (système peer-to-peer). On peut d'ailleurs dire que l'innovation qu'apportent les cryptomonnaies tient uniquement en ce protocole, d'autant plus qu'elles sont en réalité des instruments d'épargne et de spéculation et très peu, voire même pas du tout, des instruments de paiement (la place des cryptomonnaies dans le système monétaire contemporain renvoie au vieux débat entre « free banking » et « central banking »). Ce pouvoir de spéculation que donnent les cryptomonnaies, couplé à une absence totale de régulateur, fait d'elles de redoutables facteurs d'instabilité financière et donc de crises. Le bitcoin est la cryptomonnaie la plus connue mais c'est loin d'être la seule : on en compte entre 4000 et 5000 ; certaines ont un plafond d'émission (le nombre de bitcoins doit tendre vers un maximum de 21 millions selon le programme de son inventeur) d'autres n'en ont pas. C'est le cas de l'ether, principal concurrent du bitcoin. Cette cryptomonnaie, créée au milieu des années 2000 par le canadien Vitalik Buterin, se veut plus généraliste que le bitcoin en ce qui concerne ses applications : sa blockchain - Ethereum - est multi-usage ; elle est « un réseau de création de monnaie décentralisée combiné à une plate-forme de développement de logiciels et d'applications (…) qui fonctionnent exactement comme elles ont été programmées, sans possibilité de panne, de censure, de fraude ni d'interférences ». Cette blockchain sert aussi bien à programmer des paiements de transactions qu'à gérer des campagnes de financement, des titres de propriété, des places de marché ou encore des sociétés par actions et même des élections en ligne.

Indiquons que pour détenir des cryptomonnaies, on ne peut pas compter sur l'intermédiation bancaire puisque ces cryptomnnaies ne sont pas reconnues comme de vraies monnaies : il faut passer par des plateformes de change en ligne comme « Coinbase ».

Le protocole qui est à la base de toutes les cryptomonnaies est appelé « blockchain » ou « enchaînement de blocs » et il constitue une innovation de rupture importante (une innovation « disruptive »), surtout que ses domaines d'application s'annoncent nombreux, ce qui peut bouleverser à terme le paysage de nombreux secteurs d'activité, y compris le monde des institutions financières (d'ores et déjà des banques françaises développent des blockchains privées pour leurs usages internes). Le protocole « blockchain » est considéré comme une innovation qui va avoir la même portée disruptive que le protocole TCP/IP avec le développement de l'Internet.

Pour comprendre au mieux la technologie de la « blockchain », nous recommandons, parmi beaucoup d'autres, une vidéo sur Youtube à l'adresse suivante : https://www.youtube.com/watch?v=du34gPopY5Y

Nous en donnons ci-après les principales caractéristiques :

- La base de données qui, au sein de toute banque, rassemble les informations concernant les opérations faites par leurs clients, constitue un fichier informatique centralisé est ici complètement décentralisée en ce sens qu'elle est distribuée entre tous les agents qui sont les nœuds du réseau « peer-to-peer », appelés aussi les « mineurs » : chacun d'eux possède en quelque sorte une copie de la totalité de la base de données. Cela nécessite bien sûr que chacun ait un matériel informatique suffisant et cela ne rend plus nécessaire une autorité centrale pour gérer une telle base de données.
- Quand une transaction a lieu au sein du réseau entre deux de ses nœuds, elle est enregistrée partout, c'est-à-dire par tous les nœuds : on sait d'ailleurs non seulement entre quels nœuds a lieu la transaction mais aussi de quelle transaction antérieure provient la somme que doit verser l'acheteur au vendeur (pas besoin de vérifier la « provision » du compte et « double dépense » impossible).
- Pour assurer la fiabilité de l'enregistrement des transactions dans le réseau, on utilise deux procédés :
    - le procédé de la cryptographie asymétrique (algorithme RSA) en ce sens que chaque nœud possède une clé électronique pour chiffrer ses messages, qui est connue de toute le monde, qui est donc publique, et une autre clé pour déchiffrer les messages qu'il reçoit, qui est au contraire rigoureusement privée ; c'est parce que ce procédé cryptographique,

qui remplace la confiance par la preuve cryptographique, et que celle-ci joue un rôle fondamental dans le dispositif général, que ces monnaies sont appelées cryptomonnaies ;
    - le procédé de la signature électronique est un procédé inverse au précédent : chaque nœud possède une clé privée pour enregistrer la transaction dans la base de données décentralisée et partagée par tous les nœuds, lesquels la décodent grâce à la clé publique du nœud qui est à l'origine de la transaction. Celle-ci est ainsi authentifiée : elle ne peut pas être falsifiée, de même d'ailleurs qu'elle ne peut pas être annulée.
    - Par conséquent, quand on adhère à une blockchain, on crée un compte pour vous et on vous attribue deux clés, l'une qui est privée et l'autre qui est publique.
- Comme tous les nœuds du réseau doivent disposer de la même copie de la totalité de la base de données, il faut qu'ils se synchronisent quand une nouvelle transaction a lieu. Lorsqu'une nouvelle transaction a lieu, chaque nœud l'enregistre dans une liste d'attente et à chaque instant les nœuds ont des listes d'attente qui peuvent varier quelque peu : il faut déterminer périodiquement le nœud dont la liste va être prise pour la synchronisation (jusqu'à la fin de 2017, la durée moyenne était de 10 minutes ; elle est passé depuis à 3-4 heures). La liste qui sera choisie est appelée « bloc ».
- Le travail que doit faire chaque nœud pour être choisi est de trouver un identifiant pour caractériser sa propose liste de transactions. Pour ce faire, est utilisée la technique de hashage, qui transforme toute chaîne de caractères en nombre variable en une chaîne de caractères en nombre fixe et déterminée, et qui fait en sorte que le moindre changement de composition dans la 1ère chaîne entraîne un important changement dans la 2ème. Cette technique assure qu'un fichier, même lourd, a été correctement transmis. La 2ème chaîne de caractères que fournit la technique de hashage est en quelque sorte l'empreinte digitale du fichier, son identifiant.
- Avec la technique de hashage, chaque nœud est en mesure de trouver un identifiant pour sa liste, sachant qu'entre aussi dans l'algorithme l'identifiant du bloc précédent : c'est cela qui fait que les blocs sont liés entre eux comme les maillons d'une chaîne, d'où le nom de blockchain, c'est-à-dire une chaîne de blocs, un enchaînement de blocs. La conséquence est que si on voulait modifier le contenu d'une transaction, cela aurait fatalement pour conséquence de modifier l'identifiant, ce qui imposerait de refaire tous les calculs des blocs précédents… !
- Pour renforcer la fiabilité du système, on ajoute dans le processus de hashage de la liste de transactions non seulement l'identifiant du bloc précédent mais aussi un nombre aléatoire, appelé « nonce ». Le problème est alors de trouver le nonce qui satisfait à un certain nombre de conditions. En général, une dizaine de minutes suffisent pour trouver un hash de la forme voulue. Quand un nœud du réseau trouve une solution qui est conforme, sa liste devient le bloc de la dizaine de minutes qui se termine. Quand le bloc est trouvé, les autres « mineurs » vérifient que le « hash » trouvé est bon, ils le valident donc et se synchronisent dessus. Et ainsi de suite. L'activité de calcul des blocs s'appelle le « minage », d'où le nom de mineur. Et tous les mineurs sont intéressés à la recherche des blocs parce que celui qui, pour une tranche de dix minutes, a la liste qui devient le bloc, il reçoit une rémunération (un nombre de bitcoins dans le cas de cette blockchain-là).
- Pour rester dans la blockchain, il faut y contribuer en « minant » et la confiance que l'on a dans la blockchain vient du fait qu'aucun « mineur » ne peut avoir une puissance de calcul suffisante pour compromettre le bon fonctionnement de la blockchain.
- Quand le nombre de nœuds augmente, autrement dit quand le nombre de participants augmente, la puissance de calcul globale s'élève et il faut compliquer les conditions requises pour que l'on reste sur une période de base d'une dizaine de minutes.

En guise de conclusion, faisons deux remarques :

1) On peut opposer la « philosophie » de la blockchain à celle de l'intelligence artificielle au travers de deux expressions – caricaturales pour frapper les esprits – de deux hommes d'affaires et investisseurs de capital-risque. D'un côté, Peter Thiel, cofondateur de PayPal, selon lequel « crypto, c'est libertarien. L'intelligence artificielle, c'est communiste », et de l'autre, Reid

Hoffman, cofondateur du réseau LinkedIn, selon lequel, « crypto, c'est l'anarchie. L'intelligence artificielle, c'est l'État de droit ». Qui a raison des deux ? Un peu tous les deux ??

2) La naissance des cryptomonnaies utilisant la technologie de la blockchain pose en définitive une question fondamentale : avec ces « monnaies », a-t-on toujours affaire à une économie monétaire ? Ne revient-on pas en quelque sorte à une économie de troc ? En effet, à partir du moment où l'échange se fait entre un bien, quel qu'il soit, et une certaine quantité de « cryptomonnaie », n'est-ce pas comme s'il y avait simplement échange entre deux biens, surtout si cette cryptomonnaie joue en priorité un rôle d'actif financier ? Car, comme l'économiste italien Augusto Graziani le démontre magistralement, « tout paiement monétaire doit relever d'une transaction triangulaire, impliquant au moins trois agents : le payeur, le payé et la banque ». Or, les cryptomonnaies fonctionnent en P2P, donc à partir de relations seulement bilatérales.
Autrement dit, les cryptomonnaies nous replongent dans l'univers néo-classique qui est celui d'une économie de troc alors que Graziani décrit l'économie capitaliste monétaire, restant de ce point de vue, avec d'autres théoriciens européens, essentiellement français d'ailleurs, l'un des grands représentants de « l'école du circuit » ; que l'on peut considérer comme authentiquement post-keynésienne.