

CRYPTOMONNAIES ET TECHNOLOGIE DE LA BLOCKCHAIN.

Ancien élève de l'École normale supérieure Paris-Saclay
Agrégé de l'Université
Professeur honoraire de Chaire Supérieure
en Économie et Gestion
www.christian-biales.fr

Ce site se veut évolutif. Pour cela il fait l'objet d'un enrichissement documentaire régulier.

© **Les textes édités sur ce site sont la propriété de leur auteur.**

Le code de la propriété intellectuelle n'autorise, aux termes de l'article L122-5, que les reproductions strictement destinées à l'usage privé.

Pour toute utilisation de tout ou partie d'un texte de ce site, nous vous demandons instamment d'indiquer clairement le nom de l'auteur et la source :

CHRISTIAN BIALÈS

Professeur honoraire de Chaire Supérieure en Économie et Gestion
Montpellier (France)

www.Christian-Biales.fr

Tout autre usage impose d'obtenir l'autorisation de l'auteur.

- 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 quatre 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), à commencer par 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 comme le Bitcoin sont de fait des actifs de spéculation (d'ailleurs, la Banque de France préfère les appeler « cryptoactifs » plutôt que cryptomonnaies). De son côté, la Libra de Facebook sera une cryptomonnaie qui ne remplira a priori que la fonction de paiement.

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. En effet, une ICO est une méthode de levée de fonds, par l'intermédiaire d'actifs numériques appelés tokens (jetons), échangeables contre des cryptomonnaies pendant la phase de démarrage d'un projet. Une fois émis, ces tokens sont négociables sur des plateformes d'échange (ils sont donc très liquides) et ils sont utilisés dans le projet, ce qui fait que leur valeur dépend de celle du service fourni par l'entreprise à l'origine de l'ICO. Les tokens ne sont ni des actions ni des obligations ; ils concrétisent le pré-paiement du bien ou du service appelé à être développé. 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.

La quatrième raison est que la production d'une cryptomonnaie ne répond en rien au principe de la création monétaire que nous avons développé plus haut. En particulier, les banques commerciales créent de la monnaie essentiellement en accordant des crédits.

Le 18 juin 2019, dix ans après la création du Bitcoin, le président-fondateur de Facebook, Mark Zuckerberg, a annoncé la naissance en 2020 de **la Libra** qui se veut être une cryptomonnaie ou plutôt une cryptodevise pour effectuer des paiements et des transferts monétaires grâce à un

portefeuille virtuel directement intégré dans les services de messagerie cryptés Messenger et WhatsApp. Xavier Niel, vice-président du C.A. d'Iliad, qui accompagne le projet de Facebook, considère (dans un point de vue paru dans Les Echos des vendredi 11 et samedi 12 octobre 2019) que « Libra est simplement une proximonnaie, c'est-à-dire une monnaie qui repose sur des devises déjà existantes au prorata de leur usage dans le commerce mondial. Ce système est structurellement plus stable, une valeur refuge dans de nombreux pays en cas d'instabilité monétaire. C'est aussi une alternative à des projets non régulés ou politiquement motivés. Avec le libra, les paiements seront beaucoup plus directs, interpersonnels et rapides. Accessible à tous et pour tous, aussi simple qu'un SMS pour payer, il va devenir un réflexe. Nos pratiques changent et évoluent. Il n'y aura plus d'intermédiaire pour prendre des frais, imposer des délais, ni de monopole bancaire. Par ailleurs, tout le monde n'est pas "bancaarisé". Il existe de nombreuses inégalités en la matière. La population mondiale exclue du système financier et non bancaarisée est de 1,7 milliard, soit environ 31% de la population mondiale, dont 1 milliard possède un téléphone mobile et 480 millions ont accès à Internet selon le rapport Findex de la Banque mondiale (2017). Et l'écart de "bancaarisation" entre les femmes et les hommes dans les pays en voie de développement est de 9% selon la fondation Gates. Ce projet est, en cela, porteur de démocratisation et d'inclusion ». Xavier Niel parle de « proximonnaie », d'autres parlent de « stable coins » en considérant qu'il s'agit d'unités de compte qui remplacent seulement une monnaie existante sur le principe de « un pour un ». Notons qu'une monnaie virtuelle de ce genre est en quelque sorte l'inspiratrice de la libre : c'est le tether lancé en 2014 comme alternative au dollar. Le nombre de tethers en circulation est en principe équivalent à la réserve en dollar. D'autres analystes minimisent l'originalité de ces monnaies virtuelles en considérant qu'elles sont finalement très proches du système Paypal : en effet, dans ce système une monnaie électronique est émise pour être ensuite convertie dans la devise du vendeur.

Le livre blanc précise :

« Le moment est venu de créer un nouveau type de devise numérique basé sur la technologie blockchain. La mission de Libra est de développer une devise et une infrastructure financière mondiales simples, au service de milliards de personnes. Libra est composée de trois éléments qui forment ensemble un système financier plus inclusif:

1. Ce système repose sur une blockchain sécurisée, évolutive et fiable ;
2. Il est soutenu par une réserve d'actifs conçue pour lui offrir une valeur intrinsèque ;
3. Il est gouverné par l'association indépendante Libra, qui est chargée de guider l'évolution de l'écosystème.

La devise Libra repose sur « la blockchain Libra ». Comme son but est d'atteindre une audience mondiale, le logiciel qui met en œuvre la blockchain Libra est open source. Il peut ainsi être utilisé par tous et répondre aux besoins financiers de milliards de personnes. Imaginez un écosystème libre et interopérable de services financiers, créé par des développeurs et des organisations pour aider les particuliers et les entreprises à détenir et à transférer des Libra au quotidien. Grâce à la prolifération des smartphones et des réseaux Internet sans fil, de plus en plus de personnes pourront être en ligne et avoir accès à la Libra par le biais de ces nouveaux services. Pour permettre à l'écosystème Libra de concrétiser cet objectif au fil du temps, la blockchain a été développée dans une optique d'évolutivité, de sécurité, d'efficacité de stockage et de débit, ainsi que pour favoriser son adaptabilité future. (...)

La devise s'appelle la « Libra ». Il est important qu'elle soit acceptée dans de nombreux endroits et facilement accessible par ceux qui souhaitent l'utiliser. En d'autres termes, les gens doivent savoir qu'ils peuvent l'utiliser et que sa valeur restera relativement stable au fil du temps. Contrairement à la majorité des cryptomonnaies, la Libra est entièrement garantie par une réserve d'actifs réels. Divers dépôts bancaires et titres gouvernementaux à court terme seront conservés dans la réserve Libra pour chaque Libra créée, afin de renforcer la confiance envers sa valeur intrinsèque. La réserve Libra sera administrée dans l'objectif de préserver la valeur de la Libra au fil du temps. (...)

L'association Libra est une organisation indépendante à but non lucratif basée à Genève, en Suisse. Son but est d'offrir un cadre de gouvernance et de coordonner le réseau et la réserve. Elle vise également à fournir des subventions à impact social pour favoriser l'inclusion financière. Ce livre blanc est le reflet de sa mission, de sa vision et de son champ de compétences. Les membres de cette association sont issus du réseau de nœuds de validation qui opèrent la blockchain Libra.

Les membres de l'association Libra seront issus d'entreprises, d'organisations à but non lucratif et multilatérales, ainsi que d'institutions universitaires diverses et d'origines variées. Le groupe initial d'organisations qui collaboreront sur la finalisation de la charte de l'association et deviendront des "Membres fondateurs" une fois la charte terminée concerne, par secteur :

- Paiements : Mastercard, Mercado Pago, PayPal, PayU (Naspers' fintech arm), Stripe, Visa
- Technologies et marketplaces : Booking Holdings, eBay, Facebook/Calibra, Farfetch, Lyft, Spotify AB, Uber Technologies, Inc.
- Télécommunications : Iliad, Vodafone Group
- Blockchain : Anchorage, Bison Trails, Coinbase, Inc., Xapo Holdings Limited
- Capital-risque : Andreessen Horowitz, Breakthrough Initiatives, Ribbit Capital, Thrive Capital, Union Square Ventures
- Organisations à but non lucratif, organisations multilatérales et institutions universitaires : Creative Destruction Lab, Kiva, Mercy Corps, Women's World Banking

Nous espérons que l'association Libra comptera une centaine de membres d'ici son lancement prévu pour le premier semestre 2020. (...)

La Libra est conçue pour être une cryptomonnaie numérique stable qui repose entièrement sur une réserve d'actifs réels (la réserve Libra) et qui est soutenue par un réseau d'échanges concurrentiel pour l'achat et la vente de la Libra. Dans le cadre de ce système, toute personne utilisant la Libra reçoit un degré d'assurance élevé de pouvoir convertir sa devise numérique en devise fiduciaire locale en fonction d'un taux de change, de la même façon qu'une devise peut être échangée contre une autre lors d'un voyage. Cette approche est similaire à la manière dont d'autres devises ont été introduites par le passé : pour aider une devise à gagner la confiance des citoyens et à être adoptée de tous, les billets d'un pays étaient garantis en contrepartie d'actifs réels, tels que de l'or. À la place de l'or, cependant, la Libra sera soutenue par un ensemble d'actifs de faible volatilité, tels que des titres gouvernementaux dans des devises provenant de banques centrales stables et réputées.

Il est important de souligner qu'en conséquence une Libra ne sera pas toujours convertie au même montant dans une devise locale donnée (en d'autres mots, la Libra ne sera pas « arrimée » à une devise spécifique). Au lieu de cela, la valeur d'une Libra dans une devise locale donnée évoluera en fonction de la fluctuation de ses actifs sous-jacents. Les actifs de la réserve sont toutefois choisis pour minimiser le risque de volatilité, et les détenteurs de Libra peuvent donc compter sur la capacité de la devise à conserver sa valeur au fil du temps. Les actifs de la réserve Libra seront détenus par un réseau de dépositaires d'origines variées et disposant de cotes de crédit de premier ordre. Ce réseau sera chargé de la protection et de la décentralisation des actifs.

Grâce à ces actifs sous-jacents, la Libra se démarque des nombreuses cryptomonnaies existantes qui ne possèdent pas cette valeur intrinsèque et dont la valeur fluctue donc considérablement en fonction des attentes. La Libra est toutefois une cryptomonnaie à part entière, et elle bénéficie de ce fait de plusieurs propriétés intéressantes liées à ces nouvelles devises numériques : la faculté de pouvoir envoyer de l'argent rapidement, la sécurité offerte par la cryptographie et la liberté de transférer facilement des fonds d'un pays à un autre. De la même façon que vous utilisez votre téléphone pour envoyer des messages à vos amis partout dans le monde, Libra vous permet d'envoyer de l'argent instantanément, en toute sécurité et à faible coût. (...)

D'où vient l'argent de la réserve ? L'argent de la réserve proviendra de deux sources : les investisseurs de l'Investment Token (qui est séparé) et les utilisateurs de la Libra. L'association versera des primes en Libra aux Membres fondateurs pour encourager son adoption par les utilisateurs, les commerçants et les développeurs. Les fonds liés aux distributions de pièces comme primes incitatives proviendront d'un placement privé auprès d'investisseurs. Du côté de l'utilisateur, pour créer de nouvelles pièces Libra, il doit y avoir un achat équivalent de Libra en monnaies fiduciaires et le transfert de cette monnaie à la réserve. Ainsi, la réserve se développera au

fur et à mesure que la demande de Libra des utilisateurs augmentera. Pour résumer, tant du côté des investisseurs que de celui des utilisateurs, il n'y a qu'un moyen de créer plus de Libra : en achetant plus de Libra en contrepartie de monnaies fiduciaires et en développant la réserve.

Comment la réserve sera-t-elle investie ? Les utilisateurs de la Libra ne reçoivent pas de profit provenant de la réserve. La réserve sera investie dans des actifs à faible risque qui produiront des intérêts au fil du temps. Le chiffre d'affaires issu de cet intérêt servira avant tout à couvrir les dépenses de fonctionnement de l'association (le financement des investissements dans la croissance et le développement de l'écosystème, les subventions aux ONG, les recherches d'ingénierie, etc.). Une fois ces dépenses couvertes, le reste des profits sera utilisé pour payer des dividendes aux premiers investisseurs du Libra Investment Token pour leurs contributions initiales. (...) ».

Il apparaît que la Libra ne sera pas une monnaie à part entière mais un instrument de paiement, ou tout au plus une monnaie de substitution. La « mise en circulation » de la Libra n'augmentera pas la quantité de monnaie en circulation, laquelle augmentation est la seule preuve de la création monétaire (de même que la diminution de la masse monétaire est la marque d'une destruction monétaire). Autrement dit, l'association Libra sera bien en mesure d'émettre de la monnaie mais pas d'en créer (la distinction entre émission de monnaie et création de monnaie est en effet capitale en analyse monétaire).

Cela dit, on peut penser comme Vincent Lorphelin, coprésident de l'Institut de l'Économie, que la Libra peut ouvrir une ère nouvelle : « On sait que Facebook crée de la richesse parce qu'il a inventé un aspirateur à poussières économiques. Ce sont les traces, les commentaires des contributeurs qu'il analyse. Ces clics n'avaient aucune valeur économique. Mais Facebook a réussi à les agréger et en faire un minerai qu'il a ensuite raffiné pour proposer un profilage marketing de qualité et générer des recettes publicitaires. La Libra permet de sortir cet aspirateur à données du carcan publicitaire et de générer de nouveaux marchés, dont on perçoit déjà les signaux faibles aujourd'hui dans la « token economy » (« économie des jetons » qui permettent, par exemple, à de jeunes start-up, de lever des fonds via l'émission de « jetons numériques » échangeables ultérieurement contre de la cryptomonnaie. 2.000 start-up ont déjà bénéficié de ce système). Ces « token » sont des reconnaissances économiques de petites contributions, mais qui, agrégées, raffinées, vont permettre de générer des lingots à partir de minerais qui n'étaient pas exploités. La grande vertu de la Libra, c'est de solvabiliser tout cela en apportant cette masse critique de plus de 2 milliards d'utilisateurs. C'est là où émerge un nouveau continent économique. (...) On change de paradigme. Aujourd'hui, on considère que l'économie, c'est l'affaire des entreprises. Et que les États doivent les réguler pour leur imposer des contraintes sociales et écologiques. La promesse de la token economy, c'est que le social et l'écologique soient intégrés dans le modèle économique. Que ce ne soit plus une contrainte mais une source additionnelle de richesse. (...) ». (Le Soir, édition du 4 juillet 2019).

Au point de vue optimiste de Vincent Lorphelin, on peut opposer un certain nombre de réserves importantes.

Il y en a au moins huit :

- La Libra est décrite comme une cryptomonnaie mais qui peut être sûr qu'elle ne se transformera pas en cryptoactif financier selon l'utilisation qui sera faite de la réserve : doit-on faire confiance dans l'affirmation selon laquelle la réserve sera investie en « actifs à faible risque » ?
- La Libra peut faire courir des risques de fraudes et de blanchiment.
- Même si la Libra reste une cryptomonnaie, se pose alors, comme pour toute monnaie, la question de la régulation de sa quantité mise en circulation. De là découlent deux autres questions, qui sont, dans l'ordre croissant d'importance, celle de la vitesse de circulation de la monnaie et celle du prêteur en dernier ressort. D'abord, on peut penser que le développement de l'économie numérique sera un facteur important d'accélération de la vitesse de circulation. Or, si la Banque centrale est court-circuitée, elle ne pourra pas jouer son rôle habituel de régulation de la masse monétaire en tenant compte des variations de la vitesse de circulation de la monnaie. Ensuite, en cas de surémission de monnaie, l'absence d'un prêteur en dernier ressort, rôle joué naturellement par la Banque centrale, peut s'avérer

critique. Enfin, la Banque centrale perd tout pouvoir en matière de taux de change (euro/libra en ce qui concerne la BCE) puisqu'elle perd le contrôle de la masse monétaire si elle a besoin d'intervenir sur le marché des changes et/ou elle subit les variations du taux de change de sa monnaie si elle n'intervient pas pour une raison ou pour une autre.

- Ce « court-circuitage » de la Banque centrale serait d'autant plus dommageable que la Libra voit son succès copieusement alimenté par la logique de réseau dont on parle plus haut. En effet, la monnaie est d'autant plus fiable que le réseau de ses utilisateurs est étendu (« La crainte et la fascination que suscite le projet Facebook tiennent à la puissance d'action inédite de l'entreprise-réseau. Celle-ci peut en effet s'appuyer sur 2,5 milliards d'utilisateurs de ses réseaux sociaux à travers le monde », comme le précise Franck Aggéri). À la limite, n'importe qui peut créer « sa » cryptomonnaie mais pour qu'elle vive et survive, encore faut-il qu'elle soit demandée et acceptée par le plus grand nombre possible d'agents économiques (ce qui explique aussi que la multiplication du nombre de cryptomonnaies finira à un moment ou à un autre par un puissant mouvement de concentration). La monnaie est fondée sur la confiance qu'ont les agents non financiers en elle et elle constitue une convention qui permet de sortir de l'économie de troc et de faciliter les échanges. Comme le dit Yuval Noah Hariri, « la confiance est la matière première dans laquelle toutes les catégories de monnaie sont frappées ». Et Michel Aglietta précise : « la monnaie n'a pas d'utilité intrinsèque mais elle a une utilité sociale formidable, parce qu'on postule qu'elle est acceptée par tous. Elle fait lien social ».
- Dans un entretien accordé le 5 juillet 2019 à La Tribune, Michel Aglietta considère que « le paiement n'est pas un acte individuel mais un système. Pour qu'il y ait finalité des règlements, il faut qu'il y ait une entité supérieure, ultime, qui ne peut être privée, qui est reconnue légitime par la loi. Ce qui ne veut pas dire que cette institution doit être dépendante de l'État. Elle peut même avoir du capital privé et a intérêt à être autonome. La monnaie est un bien public par nature, mais elle n'est pas une créature de l'État : elle est un processus d'unification de la société, légitimée par la puissance publique ».
- Pour ce grand spécialiste des questions de macroéconomie monétaire et financière, le projet Libra est dangereux non seulement parce que pour lui la monnaie doit rester publique mais aussi parce d'autres acteurs que Facebook peuvent également se lancer dans la production d'une cryptomonnaie et transformer ainsi l'ensemble en une « pagaille formidable » et parce qu'il ne faut pas que le pouvoir monétaire « glisse de l'autorité légitime à des monopoles privés ».
- A priori, l'Association Libra doit émettre de la monnaie - une monnaie de substitution - mais pas en créer, pour reprendre la distinction importante faite plus haut. En tant que telle, elle n'ajoute donc rien au financement puisque les devises de la réserve se trouvent stérilisées. Mais surtout, est-on sûr qu'un jour ou l'autre, l'Association Libra ne décidera pas de faire crédit et donc de se transformer en créateur de monnaie, donc en banquier, sans avoir à en respecter la réglementation ni à en supporter la régulation. Cela rappellerait l'histoire du billet de banque. Au départ, le billet n'était qu'un certificat de dépôt d'or et le banquier, qui n'était alors qu'un loueur de coffre-fort, émettait des billets entièrement gagés. Puis, pour augmenter son profit au-delà de la location de coffre-fort, constatant aussi que les dépôts d'or dépassaient quasi systématiquement les retraits, et, surtout, confronté à une demande de billets de la part des agents non financiers pour pré-financer divers projets, il lui vint logiquement l'idée d'émettre des billets pour une valeur supérieure à celle de son encaisse métallique : en faisant ainsi crédit, le banquier se transforme en créateur de monnaie ; ses billets ne sont plus entièrement gagés et la masse monétaire en circulation augmente. Rien ne dit que cette histoire ne va pas se reproduire...
- Si c'est le cas, alors deux problèmes se poseront : une sorte de concurrence déloyale faite aux banques commerciales traditionnelles et un défi lancé aux Banques centrales. On peut compter sur les unes et les autres pour limiter le champ d'action des cryptomonnaies et ne pas perdre ni leur pouvoir monétaire en général ni leur revenu de seigneurage en particulier.

Une raison qui peut aussi justifier l'inquiétude qu'expriment les Banques centrales, spécialement celles dont la monnaie constitue une monnaie de réserve internationale (dollar, euro, yen, livre sterling) est que leur politique monétaire expansionniste peut, un jour ou l'autre, entraîner une défiance des détenteurs de monnaie et des épargnants - une « fuite devant la monnaie » - et que ceux-ci se tournent vers des actifs qu'ils considèrent comme des valeurs refuges : la libra pourrait à ce titre rivaliser avec l'or.

En matière d'analyse monétaire, les relations entre les cryptomonnaies et le système bancaire traditionnel (hiérarchisé en banques commerciales – de second rang - et banque centrale - de premier rang -) renvoient à la célèbre théorie de la monnaie bancaire de Friedrich Hayek (« prix Nobel d'économie » en 1974) qui prévoit une « vraie concurrence des monnaies » pour reprendre le titre de son ouvrage paru en 1976, avec une abolition du monopole de la Banque centrale, et, tout aussi radicalement, aux contributions fondatrices de F. Black en 1970, de E. Fama en 1980 et de R. Hall en 1982 prônant non seulement la disparition de la Banque centrale mais aussi celle de toute monnaie de premier rang, et également à la théorie, un peu moins radicale, du « free banking » qui envisage aussi l'absence d'institut d'émission-banque centrale et de toute réglementation spécifique au secteur bancaire mais admet l'existence d'une base monétaire dont l'offre serait exogène. Il y aurait alors concurrence entre les banques mais pas entre les monnaies. La théorie du free banking postule qu'il y aurait autorégulation du système bancaire, ce que beaucoup d'auteurs contestent (citons en particulier J.-M. Figuet et P. Kauffmann, avec leur article paru dans la Revue française d'économie en 1998). Deux problèmes liés peuvent se poser : celui d'une surémission de monnaie et celui de la crise monétaire et financière entraînée par l'absence d'une Banque centrale dans son double rôle de régulateur de la masse monétaire en circulation et de prêteur en dernier ressort.

Plus fondamentalement, ces théories vont beaucoup plus loin que les thèses monétaristes et néo-classiques habituelles. Elles peuvent même être qualifiées de libertariennes dans la mesure où elles s'opposent à toute intervention étatique, non seulement parce qu'elles estiment que le marché concurrentiel est en mesure de s'autoréguler parfaitement mais aussi parce qu'elles considèrent que les interventions étatiques sont totalement contreproductives. Notons que Peter Thiel, « l'idéologue » du projet Libra de Facebook est un libertarien et que c'est un opposant notoire à toute régulation publique.

Nous reprendrons d'ailleurs plus loin ce qualificatif de « libertarien » ... Remarquons que ces théories, et par conséquent les conceptions qui soutiennent les cryptomonnaies, renouent paradoxalement avec les tout débuts de l'économie bancaire. En effet, au départ, les monnaies étaient le résultat d'initiatives privées. Les États se sont mis à utiliser la technique bancaire de création de billets pour financer le Trésor public, sans avoir en réalité la contrainte de la contrepartie comme c'est le cas pour une banque privée (dépôts de métal précieux, cession de titres ou demande de financement d'un projet producteur de revenus) ; d'où la notion de « planche à billets » dans un sens péjoratif. Mais les États ont au-delà de cette opportunité ressenti la nécessité de contrôler l'émission monétaire des banques commerciales dont le comportement pouvait être excessif et menacer par là l'équilibre de tout le système : cela a commencé en accordant des privilèges à certaines banques commerciales ou plus généralement à une seule, qui sera la préfiguration de la Banque centrale. Alors qu'à Amsterdam la banque en question est publique dès le départ, en Angleterre, la banque qui deviendra en 1694 la « Banque d'Angleterre » est initialement privée, de même d'ailleurs que celle qui deviendra la Banque de France en 1800 (mais avec des modalités d'émission de billets bien différentes puisque les Anglais mettaient en œuvre le « currency principle » alors que les Français fonctionnaient avec des plafonds d'émission). Par conséquent, les cryptomonnaies veulent se libérer de la tutelle des Banques centrales en considérant que celles-ci sont au service des pouvoirs publics. Alors que l'avènement des Banques centrales n'a plus eu comme seule raison le financement éventuel des Trésors publics mais aussi la régulation indispensable de l'émission des monnaies bancaires, la sauvegarde du bon fonctionnement du système dans sa globalité (rôles d'institut d'émission

de la monnaie à cours légal et de prêteur en dernier ressort), et la conduite d'une politique - monétaire - considérée de plus en plus comme un levier important pour conduire les affaires économiques et sociales du pays (politiques de stabilisation et de relance) ; son rôle gagnera d'ailleurs en importance avec la naissance des États-providence.

Les cryptomonnaies mettent en cause la souveraineté monétaire des États. Ceux-ci vont-ils alors être en mesure de défendre non seulement leur souveraineté monétaire dans le capitalisme financier mondialisé mais aussi leur souveraineté numérique qui se trouve largement contestée par le capitalisme de plateforme ? Comme le dit Franck Aggéri dans la conclusion de son article (*Alternatives-économiques.fr*, 27/08/2019), « avec ce projet de monnaie, Facebook a franchi une barrière symbolique en empiétant sur le domaine de la souveraineté des États. Le combat risque d'être long et il n'est pas sûr que le principe de la liberté d'entreprendre l'emporte sur la raison d'État ».

Pour compléter notre réflexion sur la théorie qui sous-tend les cryptomonnaies et pour confirmer que la dose « libertarienne » peut différer selon les approches, notons que le récent livre de Frédéric Antonini, « Pour une économie libertaire », paru chez « nada éditions » fin avril 2019, reste relativement classique quant aux questions monétaires. En effet, pour lui, « le système bancaire est composé d'organismes bancaires chargés notamment des dépôts et du crédit monétaires et d'un organisme bancaire central. Ce dernier pilote la politique relative à la monnaie, voulue par la société. (...) Seuls les organismes bancaires certifiés sont habilités à pratiquer le crédit monétaire à partir d'une création de monnaie ».

Une information importante à approfondir : le 26 août 2019, l'Autorité fédérale suisse de surveillance des marchés financiers - la FINMA - explique dans un communiqué « de quelle manière elle applique les prescriptions suisses en vigueur en matière de blanchiment d'argent aux prestataires de services financiers soumis à sa surveillance qui sont actifs dans le domaine de la *blockchain*. La FINMA a, par ailleurs, octroyé une autorisation en tant que banque et négociant en valeurs mobilières à deux nouveaux prestataires financiers dans le domaine de la *blockchain*. La FINMA reconnaît le potentiel d'innovation des nouvelles technologies pour les marchés financiers. Elle applique les dispositions du droit des marchés financiers en vigueur indépendamment des technologies sur lesquelles les services proposés reposent. Les modèles d'affaires fondés sur la *blockchain* ne doivent toutefois pas pouvoir contourner le cadre réglementaire, lequel a fait ses preuves. Cela vaut en particulier pour les règles de lutte contre le blanchiment d'argent et le financement du terrorisme dans le domaine de la *blockchain*, où l'anonymat implique des risques accrus. (...) La FINMA a, pour la première fois, octroyé une autorisation en tant que banque et négociant en valeurs mobilières à deux prestataires financiers actifs dans le domaine de la *blockchain*. Il s'agit des entreprises SEBA Crypto SA, dont le siège est situé à Zoug, et Sygnum AG, installée à Zurich. Elles proposeront des services destinés aux clients institutionnels et professionnels. Exercer cette activité implique, comme d'habitude, de remplir certaines conditions garantissant un développement commercial conforme. La FINMA applique aussi, pour surveiller les deux établissements, les principes décrits dans la communication sur la surveillance publiée aujourd'hui. (...) ». Dans le communiqué on lit aussi, pour rassurer, que les établissements soumis à la surveillance de la FINMA peuvent en principe envoyer des cryptomonnaies ou autres jetons uniquement à des portefeuilles (*wallets*) externes appartenant à leurs propres clients, déjà identifiés, et accepter des cryptomonnaies ou des jetons uniquement de tels portefeuilles. Les établissements assujettis à la FINMA ne peuvent pas recevoir de jetons de clients d'autres établissements ni en envoyer à des clients d'autres établissements. Cette règle s'applique tant que les données sur l'expéditeur ou le destinataire ne pourront pas être transmises fiablement dans le système de paiement concerné ».

Comme l'écrit Anne Drif dans le numéro des Échos paru le lendemain, « le front des régulateurs bancaires européens face aux cryptomonnaies se brise. En pleine campagne pour doter la Suisse du statut de « cryptonation », l'Autorité fédérale de surveillance des marchés financiers (Finma) vient

d'accorder les premières licences bancaires à deux acteurs, SEBA et Sygnum. Un contre-pied aux critiques de ses pairs du Vieux-Continent ».

Une réflexion intéressante de l'équipe de recherche de Natixis (Flash Economie n° 1364 du 10 octobre 2019) :

« Les agents économiques souhaitent détenir une monnaie dont le processus d'offre est "raisonnable", ce qui est difficile aujourd'hui :

- les monnaies "officielles" (dollar, euro, yen...) ont une offre de monnaie qui a anormalement et dangereusement augmenté avec les politiques monétaires très expansionnistes, ce qui détériore la confiance dans ces monnaies ;
- l'or, les crypto-monnaies ont une offre de monnaie qui est exogène, qui n'est pas gérée ; ceci conduit à une variabilité excessive des prix de ces monnaies qui en décourage la détention ;
- il faudrait donc créer une monnaie dont l'offre serait gérée "intelligemment" : pas de croissance excessive, une quantité offerte qui compense partiellement les mouvements de la demande pour cette monnaie afin de limiter la variabilité du prix (du taux de change) de cette monnaie. Bien sûr, ceci implique qu'il faut des interventions discrétionnaires dans l'offre de monnaie, ce qui peut inquiéter, afin de stabiliser le prix (le taux de change) de la monnaie. Le libra aura peut-être ces caractéristiques efficaces ».

Deux analyses synthétiques et critiques de deux économistes spécialistes des questions monétaires.

La première est celle de Michel Aglietta dans Challenges n° 620 du 5 septembre 2019 :

« Deux caractéristiques fortes permettent de définir la monnaie. Elle est d'abord un bien public : il n'y a pas de monnaie sans soutien de la puissance publique. Elle est ensuite un système de paiement. Le réseau doit être solide, tous les maillons, même les plus faibles, doivent pouvoir tenir. Le problème du projet Libra est la confiance que les acteurs économiques peuvent avoir en un opérateur privé émettant une forme monétaire qui n'est liée à aucune monnaie nationale. Le lien à un panier est purement fictif dès lors que les rapports entre les devises constituantes ne sont pas régulés. Il faudrait que les banques centrales maintiennent la stabilité des changes au sein du panier pour offrir une garantie. Pour que l'émetteur de Libra le fasse lui-même, il faudrait qu'il dispose de réserve égale au montant des transactions à garantir dans toutes les devises du panier et dans les bonnes proportions, ce qui ferait de Libra une "monnaie étroite" dont l'intérêt serait réduit.

Une autre solution serait d'avoir l'assentiment des banques centrales émettrices des devises composant le panier comme prêteurs en dernier ressort. (...)

Un autre modèle serait une monnaie digitale de banque centrale avec une institution publique distribuant directement de la monnaie aux particuliers, sans intermédiaires. Certains estiment que cela renforcerait l'efficacité du fameux "quantitative easing", que pratique notamment la banque centrale européenne via le système bancaire.

En résumé, le projet tel qu'il est présenté par Facebook est trop dangereux pour générer de la confiance. Il est donc voué à l'échec. Je crois cependant au développement du multilatéralisme et donc, pourquoi pas, à la création d'une monnaie universelle. Mais il faudra une gouvernance établie sur la base d'un traité international entre les États-nations. On peut toujours rêver ! ».

Notons que le mercredi 4 décembre 2019, la Banque de France, par la voix de son Gouverneur, a annoncé un appel d'offre à projets qu'elle lancera à la fin du 1^{er} trimestre 2020 pour une « monnaie digitale de banque centrale ». Ces « e-euros » ne seront utilisés au départ que pour régler des transactions dites de « gros », c'est-à-dire celles réalisées sur les marchés financiers par les acteurs institutionnels (par la suite, ces e-euros pourraient aller jusqu'à remplacer les billets et les pièces, comme c'est déjà pratiquement le cas en Suède et en Chine). Si les tests qui s'ensuivront s'avèrent positifs, la BCE devrait généraliser le système à l'ensemble des pays de la zone euro. Comme l'affirme François Villeroy de Galhau, « la mise en place d'une monnaie digitale de banque centrale au niveau européen permettrait de disposer d'un puissant levier d'affirmation de notre souveraineté face aux initiatives privées du type Libra ».

La seconde est celle de Barry Eichengreen, dans une chronique parue dans Le Monde du 24 octobre 2019, qui relaie Project Syndicate (notons qu'en date du 2 juillet 2019, Project Syndicate a publié un article également critique de Joseph Stiglitz) :

« Le projet de cryptomonnaie de Facebook, le libra, semble compromis depuis que PayPal, Visa, Mastercard, Stripe, eBay et Mercado Pago ont refusé d'en être les sponsors [voir ci-après]. Ce refus n'a rien de surprenant, compte tenu des inquiétudes croissantes sur le libra, propice à l'évasion fiscale, au blanchiment d'argent, au financement du terrorisme – mais aussi à l'accès de Facebook aux informations financières de ses utilisateurs.

Le libra crée par ailleurs un certain nombre de risques pour la stabilité économique et financière. Même si la monnaie de Facebook était soutenue par un portefeuille d'actifs faiblement volatils, quiconque a vécu la crise financière mondiale de 2008 sait que la "faible volatilité" tient davantage à un état d'esprit qu'à la nature d'un actif. Si les prix des actifs du portefeuille de réserve venaient à chuter en raison d'une augmentation des taux d'intérêt, l'émetteur de la monnaie ne pourrait racheter tout le libra en circulation, et l'on assisterait à l'équivalent d'une panique bancaire. D'autant qu'aucun prêteur de dernier recours (État, banque centrale) n'interviendrait.

La cryptomonnaie de Facebook pourrait également affecter la capacité stabilisatrice des politiques monétaires et réglementaires. Si la population d'un État troquait sa monnaie nationale pour le libra, les politiques nationales de taux et de change seraient viciées : il suffit d'observer la longue et douloureuse expérience de dollarisation en Argentine pour le comprendre.

Les partisans du libra en font valoir les bienfaits sociaux : il réduirait le coût des paiements transfrontaliers et des envois de fonds à l'étranger et offrirait des services financiers aux populations non bancarisées.

Ces arguments sont recevables, mais superflus. Le coût des paiements transfrontaliers est d'ores et déjà en baisse. La société Ripple, basée à San Francisco, recourt par exemple à une technologie de registre distribué et à une cryptomonnaie brevetée afin d'effectuer les transferts pour une fraction du coût initial. Ripple coopérant avec des banques commerciales soumises aux contraintes réglementaires, sa technologie ne soulève pas de problèmes. Des banques telles que Santander l'utilisent d'ores et déjà pour relier l'Europe aux États-Unis, et prochainement les États-Unis à l'Amérique latine.

Service déjà surpassé

La Society for Worldwide Interbank Financial Telecommunication (Swift), le réseau traditionnel des transferts interbancaires, teste un système baptisé SWIFT gpi Instant pour les transferts entre Amérique du Nord, Europe et Asie, avec un règlement en seulement treize secondes. On peut citer aussi le Fast and Secure Transfers (FAST) de Singapour, le Target Instant Payment Settlement (TIPS) de la Banque centrale européenne. La Réserve fédérale américaine déploiera le sien d'ici à 2023 ou 2024.

Par ailleurs, des avancées majeures ont été accomplies dans les services financiers mobiles, tel M-Pesa, né au Kenya et aujourd'hui utilisé de l'Afghanistan à l'Albanie. Les utilisateurs n'ont pas besoin d'un compte bancaire, mais d'un téléphone portable et d'un contrat auprès de leur opérateur. Ils peuvent recharger leur solde à la boutique du coin, le protéger par un code PIN et l'utiliser pour effectuer des paiements à quiconque dispose d'un compte. Ces plates-formes permettent aussi de bénéficier de services financiers, tels les microprêts. Elles surpassent d'ores et déjà le libra dans la bancarisation des non-bancarisés !

Ces services sont coûteux dans les pays où le secteur des télécoms est peu concurrentiel, l'opérateur dominant réalisant alors des marges élevées. Le libra peut-il apporter une rupture concurrentielle ? Il s'agit, ici encore, d'une douce illusion, car ces quasi-monopoles feront obstacle à son autorisation réglementaire. Si le problème est le manque de concurrence, les populations des pays en développement doivent se tourner vers leurs décideurs politiques. Ce n'est pas Mark Zuckerberg qui les aidera ».

Dernières actualités :

- ➔ Devant les pressions politiques et autres, plusieurs partenaires ont déclaré forfait et se sont retirés du projet au cours de la 1^{ère} quinzaine d'octobre 2019 : PayPal, eBay, Mastercard, Mercado, Pago, Stripe, Visa et Booking. Cela n'a pas empêché que se tienne le 14 octobre à Genève la 1^{ère} réunion officielle des membres de la Libra.

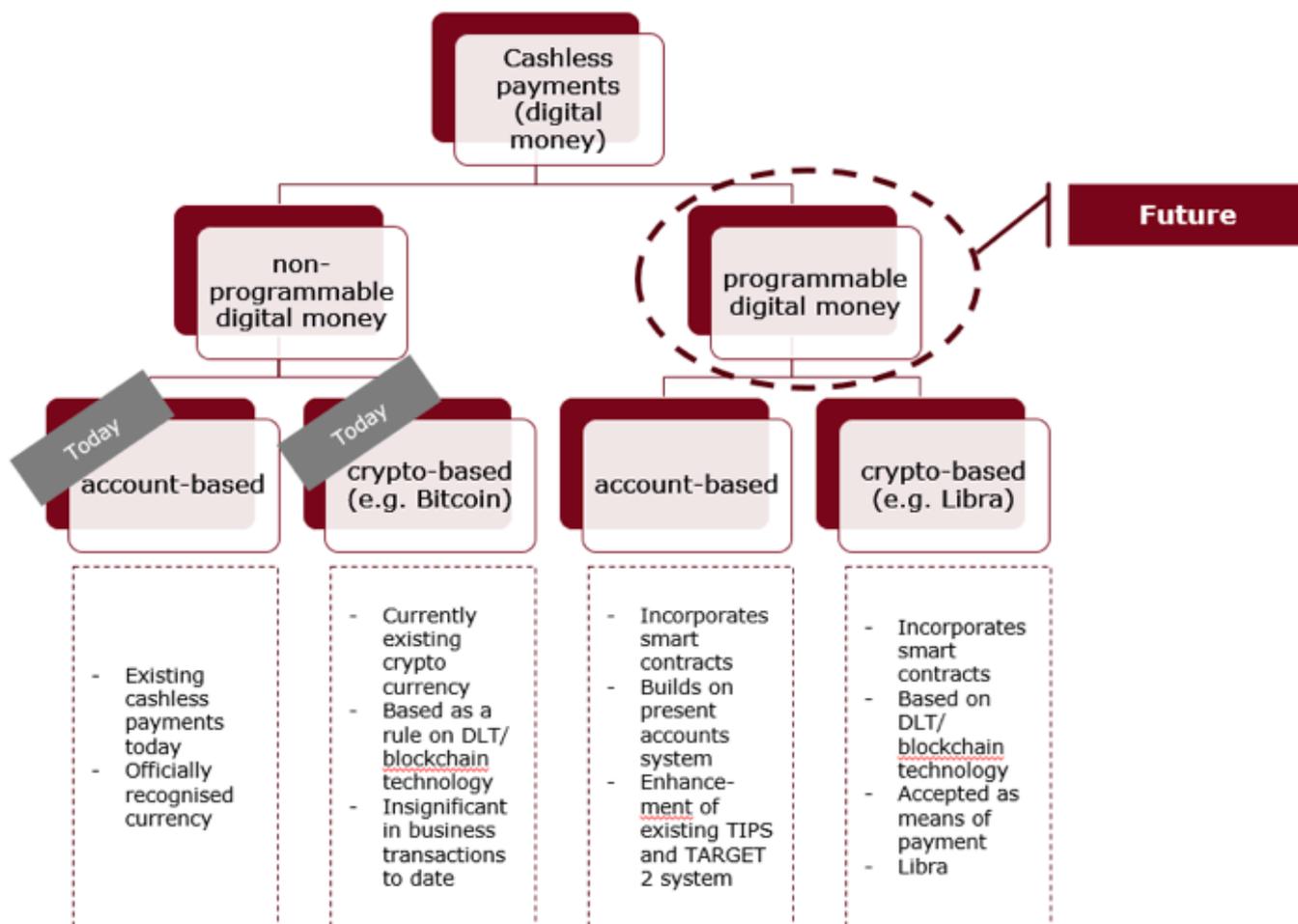
Dans le même temps, Lucas Geiger, cofondateur de Wireline, lance le projet « Open Libra ». C'est un « fork » présenté comme parfaitement compatible avec le réseau Libra mais sans la mainmise de Facebook et devant effectivement permettre de donner accès aux services financiers aux populations qui en sont aujourd'hui privées. Dans la présentation qui en est faite sur le site qui lui est consacré (<https://www.openlibra.io>), on lit :

« OpenLibra est une plateforme technologique et une devise d'inclusion financière. Une alternative à la Libra de Facebook, qui met l'accent sur la gouvernance ouverte et la décentralisation économique. Le projet OpenLibra est un collectif informel d'individus. Nous n'avons ni "membres d'association", "partenaires", ni "employés" ni "leaders". Nous appartenons à des projets de blockchain et à des fondations à but non lucratif parmi les meilleurs de notre catégorie et travaillons sur une solution crypto-native concernant la Libre. Notre stratégie consiste à exploiter les atouts de la Libra, mais à l'étendre là où cela est nécessaire ».

➔ Le 30 octobre 2019, la Bankenverband, association qui regroupe plus de 200 banques commerciales allemandes, dont la Deutsche Bank, s'inquiète du lancement de la Libra et de la cryptomonnaie d'État chinoise. En réponse, elle souhaite la création de toute urgence d'un « euro numérique programmable », qu'elle exprime dans un véritable manifeste (<https://en.bankenverband.de/newsroom/comments/programmable-digital-euro/>).

On y lit notamment : « (...) contrairement à la monnaie numérique traditionnelle, les nouvelles formes de cryptomonnaies constituent une innovation technologique importante : elles peuvent être connectées à ce que l'on appelle des “contrats intelligents“. Les contrats intelligents sont des protocoles informatiques qui mappent ou vérifient les conditions du contrat et, par exemple, initient automatiquement des paiements lors de l'exécution d'une transaction. C'est pourquoi l'industrie parle aussi de “monnaie numérique programmable“. (...) Il est donc logique de faire la distinction entre monnaie numérique programmable et non programmable. La Libra est une monnaie numérique programmable basée sur une cryptographie.

Le graphique ci-dessous donne un aperçu des différentes formes de monnaie numérique :



→ Le 16 avril 2020, Libra Association publie le communiqué suivant :

« L'Association Libra a officiellement lancé le processus d'octroi de licences pour les systèmes de paiement avec l'Autorité fédérale de surveillance des marchés financiers (FINMA). Le lancement du processus d'octroi de licences est une étape importante à mesure que la Libra Association passe à une phase plus opérationnelle du projet. Le processus d'octroi de licences a, et continuera d'avoir, la contribution des banques centrales et d'autres autorités financières de réglementation, de surveillance et d'application dans le monde qui ont été réunies dans le cadre du Collège de surveillance réglementaire de la FINMA.

Depuis la publication initiale du livre blanc de la Libra Association en juin 2019, la Libra Association a consulté et engagé de nombreuses parties prenantes mondiales et a intégré des éléments de rétroaction clés dans la conception du système de paiement Libra. Cela comprend la capacité du système de paiement Libra à offrir des pièces stables en une seule monnaie en plus de la pièce Libra multidevises. De plus, la Libra Association a adopté une blockchain autorisée ouverte et compétitive qui renonce à la transition future vers un système sans autorisation, mais conserve de nombreuses propriétés économiques et de gouvernance de la conception originale. Enfin, la Libra Association a amélioré la sécurité du système de paiement Libra avec un cadre solide pour la conformité financière et la gestion des risques à l'échelle du réseau, ainsi que des normes strictes pour la lutte contre le blanchiment d'argent, la lutte contre le financement du terrorisme et la prévention du trafic illicite. Activités. Les détails sont disponibles dans un livre blanc mis à jour de la Libra Association.

Outre la demande de licence FINMA et la mise à jour du livre blanc, les charges d'exploitation à court terme de Libra Association sont désormais financées par ses membres. L'Association Libra est une organisation suisse indépendante, composée d'entreprises et d'organisations à but non lucratif réparties géographiquement et diversifiées. La Libra

Association développe un système de paiement basé sur la blockchain soutenant l'inclusion financière et l'innovation dans les services financiers responsables.

La version actualisée du « livre blanc » est à l'adresse : <https://libra.org/en-US/white-paper/#cover-letter>

C'est sous la pression des régulateurs que Libra association révisé un peu à la baisse ses ambitions. Alors que dans le projet initial, la Libra devait seulement être adossée à un panier de monnaies, il est décidé d'ajouter à cette monnaie autant de monnaies numériques, dites « libracoins » ou « stable coins », chacune étant adossée à une devise particulière telle que le dollar, l'euro, etc. Parce qu'ils seront plus faciles à faire accepter et à gérer, ces libracoins seront sans doute lancés avant la Libra elle-même. Pour les consommateurs, il y aura peu de changements et la Libra servira toujours à faciliter les transferts d'argent ; et la Libra originale, adossée à un panier de devises, servira surtout aux règlements transfrontaliers. Sur le plan de la gouvernance, Libra association abandonne le type de blockchain adopté par exemple par le Bitcoin où la chaîne informatique est intégrée par tous les participants aux échanges qui ont matériellement la possibilité de valider les transactions, pour aller vers un système « permissionné », autorisé, en ce sens que seuls les membres de l'association pourront « faire tourner les nœuds de validation sur le réseau ». Comme on le lit sous la plume de Michael Engle, de la Libra Association, « Dans le premier livre blanc sur la Balance, nous avons annoncé une voie pour éventuellement faire la transition du réseau vers un système sans autorisation. Au cours des mois qui ont suivi, l'une des principales préoccupations que nous avons entendues est qu'il serait difficile pour la Libra Association de garantir le maintien des dispositions de conformité du réseau. Dans le livre blanc mis à jour, nous présentons l'approche que nous explorons pour offrir aux nouveaux entrants la possibilité de concourir pour la fourniture de services de réseau de base et de participer à la gouvernance du réseau Libra tout en garantissant la capacité de l'Association à répondre aux attentes réglementaires ».

- 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 1^{er} 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 3^{ème} 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 cryptographie 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 cryptomonnaies 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 cryptomonnaies 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 :
 - o 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 ;
 - o 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 décotent 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 passée 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 propre liste de transactions. Pour ce faire, est utilisée la technique de hachage, 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 1^{ère} chaîne entraîne un important changement dans la 2^{ème}. Cette technique assure qu'un fichier, même lourd, a été correctement transmis. La 2^{ème} chaîne de caractères que fournit la technique de hachage est en quelque sorte l'empreinte digitale du fichier, son identifiant.
- Avec la technique de hachage, 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 hachage 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.

Pour terminer ce paragraphe, 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 ».
- 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.

Christian-biales.fr