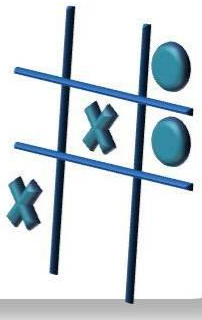
MONNAIES PARALLELES, LOCALES, COMPLEMENTAIRES ET CRYPTO-DEVISES : COMMENT ELLES PEUVENT CREER DE LA RICHESSE.

Janvier 2018

SCORE ADVISOR



Sommaire

I – Monnaies parallèles & monnaies complémentaires

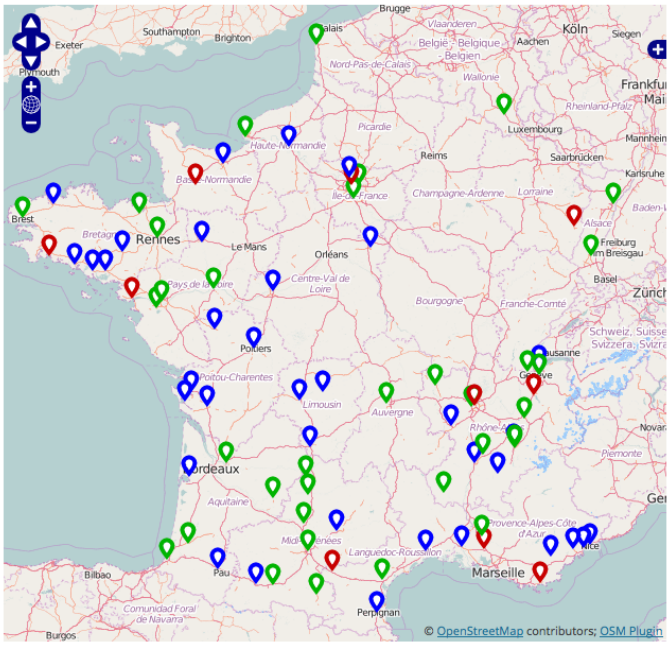
Une monnaie parallèle ou complémentaire, qu'est-ce que c'est ?

C'est une unité de mesure, distincte de la monnaie officielle, qui est utilisée au sein d'un réseau d'acceptation particulier. En d'autres termes, dès lors que des personnes physiques ou morales (entreprises, associations, administrations) acceptent d'échanger des biens ou de se régler des prestations et services sur la base d'une unité de compte autre que la monnaie officielle, une monnaie parallèle est créée : parmi bien d'autres exemples, les *miles* des compagnies aériennes (dès lors qu'ils permettent d'acheter une nuit d'hôtel par exemple) représentent une monnaie parallèle. Les monnaies parallèles peuvent être convertibles ou non dans la monnaie officielle, par rapport à laquelle elles n'ont pas forcément de cours défini. Elles peuvent matériellement exister sous la forme de billets ou de bons, être totalement dématérialisées ou bien les deux. Depuis quelques années, les monnaies parallèles sont en vogue. En 2015, Starbucks a ainsi lancé ses **Stars**, assimilables à des points de fidélité utilisables dans ses cafétérias et qu'il voudrait également voir adoptés par d'autres commerces.

Toutefois, lorsqu'on parle de monnaies parallèles ou locales, on désigne plus exactement des réseaux à dimension sociale et solidaire. Il en existe une trentaine en France et l'on en compterait plus de 13 000 dans le monde. Le site *Complementary Currency* en fournit un panorama international étoffé.

De tels réseaux existent depuis au moins le XIX° siècle mais ils se sont particulièrement développés dans les années 30, puis au cours des années 80, notamment avec les *Local Exchange Trading Systems* américains. Enfin, avec la crise de 2008, de nombreuses monnaies parallèles sont apparues. En France, la loi du 31 juillet 2014 relative à

l'économie sociale et solidaire leur a reconnu le statut de moyens de paiement (ce qui ouvre la possibilité de les utiliser notamment pour payer services publics et impôts).



vert : monnaie en circulation rouge : ne circule plus bleu : en projet

Les discours qui accompagnent la création de ces monnaies sont souvent très ambitieux et peuvent paraître assez disproportionnés par rapport à l'adhésion réelle que ces monnaies suscitent (trente monnaies locales en France seraient utilisées au total par environ 30 000 personnes…). A écouter les promoteurs des monnaies locales, il s'agit de rien de moins que de rompre avec le système bancaire, pour ne pas « *participer à la spéculation ou alimenter les paradis fiscaux* », selon un argumentaire utilisé lors du lancement des **Pêches** à Montreuil, aussi bien que pour nombre d'autres projets – le **Stück** de Strasbourg, l'**Eco** d'Annemasse, la **Touselle** de Comminges, etc.

Charte

LE CAIRN : UNE MONNAIE LOCALE COMPLEMENTAIRE & SOLIDAIRE

Une monnaie locale est une invitation à donner du sens à nos échanges, un pas de plus vers une économie plus juste et solidaire. En utilisant le Cairn, chacun se réapproprie la monnaie et apporte sa pierre afin de

- *Favoriser l'activité économique locale de la Région grenobloise*
- *Etablir la confiance et encourager l'entraide entre tous les utilisateurs*
- *Dynamiser l'économie réelle et résister à la spéculation*
- *Soutenir la transition énergétique et respecter l'environnement*
- *Permettre au citoyen de s'impliquer dans la gouvernance de sa monnaie*

Dans un *Manifeste pour les monnaies locales*, publié en juin 2013, il est affirmé que les monnaies locales « *relèvent d'un engagement citoyen qui refuse la spéculation* ». A travers elles, il s'agit pour les citoyens « *de prendre la responsabilité de leur destin et de contribuer à faire changer le fonctionnement de la société* ». « *La monnaie redevient un moyen au service de la vraie richesse, celle offerte par la nature et valorisée par l'activité humaine, et n'est pas recherchée pour elle-même* ». Nobles principes, sans doute également utiles pour décrocher des subventions mais qui s'alimentent d'analyses assez discutables. Ainsi cet argument souvent repris qui affirme que les monnaies locales ont une vitesse de circulation bien supérieure à celle des euros.

Par ailleurs, si les intentions sont louables : favoriser les circuits courts, les rapports humains, protéger l'environnement, les monnaies locales peuvent néanmoins être critiquées au titre de la tentation de repli et l'esprit de clocher économique qui sont susceptibles de les inspirer. Ne correspondent-elles pas en partie à la volonté de soustraire (et de subventionner indirectement en partie) des commerces peu dynamiques à une concurrence qui pourrait pourtant être synonyme de baisse des prix et

de services améliorés ? Avec leurs banquiers spéculateurs, spoliant les petits épargnants, leurs grandes surfaces ruinant les économies locales et leurs industriels empoisonneurs, les discours qui assurent la promotion des monnaies locales ont souvent des relents poujadistes – pour ne pas dire pétainistes !

Si l'on veut que les nouvelles monnaies parviennent à convaincre au-delà d'un petit cercle de personnes, souvent déjà a priori convaincues, il faut discerner comment elles sont à même de créer des suppléments de richesse. C'est justement ce qu'évitent souvent les promoteurs de ces monnaies, comme s'il s'agissait là d'un gros mot ! Alors que c'est proprement ainsi que les monnaies locales peuvent acquérir une réelle dimension économique, sociale ou environnementale et, véritablement audacieuses, avoir plus d'intérêt que les « colliers » du Club Med !

*

Les monnaies parallèles et complémentaires fondées sur des dons.

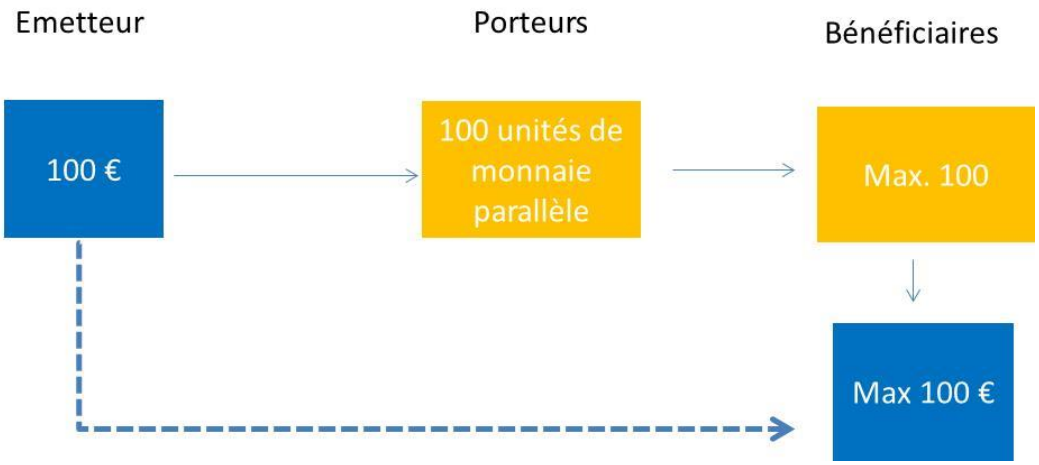
Un acteur économique (entreprise, administration, association, …) décide de soutenir certaines actions ou démarches en particulier. Pour cela, il peut choisir d'émettre une monnaie parallèle qui matérialisera ses dons ou subventions. Il la distribue autour d'elle – à ses clients par exemple, pour une entreprise, exactement comme les points d'un programme de fidélité. Et les porteurs peuvent choisir de donner cette monnaie parallèle à des associations présélectionnées ; lesquelles pourront les convertir en € auprès de l'émetteur.

Ce schéma de monnaie parallèle est assez fréquent. En France, ce sont par exemple les **tookets**, émis et administrés par une coopérative.

La banque en ligne Tookam du Crédit Agricole Pyrénées Gascogne a été la première à distribuer des tookets à ses clients, à l'occasion de l'achat de produits ou services, exactement comme les points d'un programme de fidélité. Le Crédit Agricole d'Aquitaine l'a ensuite suivie, ainsi que d'autres Caisses régionales du Groupe. En Australie, la Bendigo and Adelaide Bank a lancé une solution comparable avec les **Creds**.

Dans ce schéma, **il n'y a pas création de richesse**. La monnaie émise est parallèle à la monnaie officielle, qu'elle remplace à titre symbolique et non monétaire. L'intérêt est ainsi d'attirer et de promouvoir certaines valeurs. Il est aussi d'**associer les clients à la distribution des dons de l'entreprise**, puisque que ce sont eux qui choisissent de distribuer leurs

tookets, par exemple à différentes associations. **L'idée originale est de créer une monnaie particulière pour matérialiser un don potentiel et de faire proprement circuler ce don entre plusieurs acteurs**.



Cependant, si son caractère participatif est séduisant, le système n'est sans doute pas optimal. Il y a d'abord le risque que la monnaie distribuée n'intéresse pas ou soit oubliée. De sorte que le montant des dons effectivement versés peut être sensiblement inférieur à celui décidé au départ. Ensuite, les associations bénéficiaires ne peuvent prévoir précisément ni combien elles vont recevoir, ni quand. Elles se retrouvent par ailleurs mises en compétition pour attirer les dons, ce qui représente une situation que certaines peuvent vouloir éviter. Ce dernier aspect est contourné par le système allemand de monnaie parallèle dédiée aux associations, le **Chiemgauer**, qui est assez comparable aux Tookets mais qui est aussi plus lourd d'emploi.

Sur le même schéma d'une monnaie-don qui circule librement entre les mains de ceux qui la reçoivent, une étrange entité monétaire – sans doute la plus étonnante de toutes celles qui apparaissent dans le présent dossier – a été créée à Barcelone : le **Social Coin**. Il incite à accomplir des actions généreuses, dont on peut suivre la chaîne sur écran et qui est destiné à disparaitre – on le plante, littéralement ! - après un certain nombre d'usages. Un objet monétaire difficile à identifier, qui mérite une brève présentation.

Je vous rends un service. Vous avez oublié votre portefeuille au guichet d'une gare et je vous le rapporte, par exemple. Je vous tends alors un social coin. C'est un jeton, que vous donnerez à votre tour à quelqu'un auquel vous aurez rendu service ou vis-à-vis duquel vous aurez accompli un acte altruiste, une bonne action – à vous de juger. Il n'y a pas de liste prédéfinie.

Sur l'une des faces du jeton, un QR Code donne accès à un site, sur lequel vous pourrez noter la bonne action que vous prévoyez d'accomplir ou que vous aurez réalisée et à l'occasion de laquelle le jeton aura changé de mains. La chaîne des bonnes actions est traçable et géolocalisée. Le jeton est utilisable dix fois. Ensuite, enterrez-le ! Il n'est pas seulement biodégradable. Il est « compostable » et il contient une semence. Vous ferez ainsi pousser une plante.

Depuis juillet 2013, plus de 20 000 Social Coins ont été distribués. A partir de Barcelone, ils ont voyagé dans 68 pays différents, où ils ont générés 150 000 actes de générosité.

Comment les Social Coins sont-ils mis en circulation ? On peut les acheter et cela est particulièrement proposé aux entreprises, qui peuvent ainsi en doter leurs collaborateurs. Treize compagnies, dont Cisco, Telefonica ou Price Waterhouse, l'ont déjà fait. Pour une entreprise, la formule est certainement originale et surprenante et c'est un peu le revers de la médaille. Le Social Coin a tout d'un gadget qui pourrait rapidement faire long feu ! Mais, à ce titre, bien que porté par une *non profit organization*, il pourrait également être assez lucratif pour ses promoteurs. Le concept sera-t-il élargi ? Trouvera-t-il d'autres prolongements ?

Quoi qu'il en soit, le Social Coin bouleverse complètement les schémas monétaires. On reçoit en général de l'argent en récompense ou en rétribution d'une action. C'est ici le contraire : celui qui réalise la bonne action, distribue également le jeton. Ce dernier ne rémunère donc rien. Pas plus qu'il ne permet d'acheter quelque chose. C'est une monnaie qui ne sert, qui ne pousse, qu'au don. Dénuée de toute valeur fiduciaire, elle est porteuse d'inestimables valeurs humaines. Monnaie sans valeur d'achat en même temps que vertueuse, « fondante » comme d'autres monnaies complémentaires, les Social Coins doivent circuler pour représenter, pour créer une valeur. Ils n'ont aucun sens à être conservés, thésaurisés. Ils ne créent qu'une obligation. Les moyens de paiement, enfin, sont anonymes, interchangeables. On suit à la trace l'utilisation de chaque Social Coin.

Comment une telle idée est-elle apparue ? Sans doute a-t-on d'abord voulu imaginer une sorte d'anti-monnaie, avec pas mal de dérision et une vraie volonté de subversion : inverser les usages courants et spéculatifs de la monnaie. De là est née cependant une initiative originale et cohérente qui ressemble certes assez à un gadget au premier abord mais qui en même temps, invite à poser beaucoup de questions : de tels schémas

« monétaires » pourraient-ils être élargis et prolongés dans l'économie réelle ?

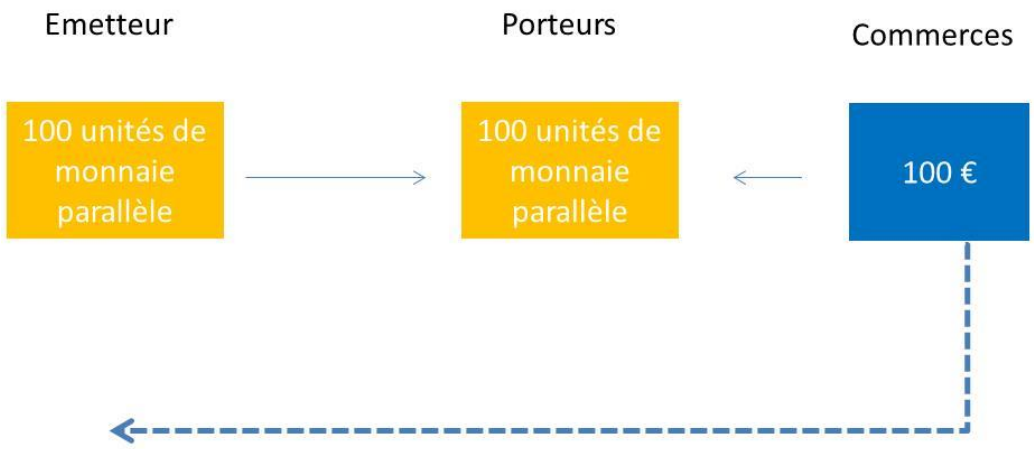
*

Dans le cas des Tookets et des Social Coins, les dons d'entreprises sont matérialisés sous la forme de monnaies parallèles et mis en circulation. Il n'y a pas création de richesse. Les Social Coins n'ont aucune valeur monétaire et les Tookets ont seulement celle des dons qui ont suscité leur création. Il est néanmoins possible de renverser le système : le don consistera à accepter une monnaie créée à cet effet. Il y aura bien alors création de richesse.

A Fortaleza, au Brésil, en 1998, la **Banco Palmas** a été créée pour distribuer des bons récompensant le temps passé par des individus dans la réalisation d'un projet financé par une ONG. Des individus qui furent pour beaucoup autant de nouveaux clients pour les commerçants locaux qui acceptèrent d'être payés en tout ou partie par les bons, marquant de la sorte leur soutien au projet. Ainsi une partie du financement du projet, correspondant au paiement des personnes impliquées dans sa réalisation, put être financée par un système tout à fait comparable à un programme de fidélité donnant des promotions.

Dans le cas des tookets, la monnaie parallèle ne fait que masquer la monnaie officielle, en laquelle les tookets sont convertis au final. Mais dans le cas brésilien, **la monnaie parallèle a permis une rémunération supplémentaire**, supportée par les commerçants, qui a rendu le coût effectif du projet en monnaie officielle d'autant plus avantageux pour ses promoteurs. En rémunérant des travailleurs volontaires, ce que le budget serré de l'ONG ne permettait pas, les dons des commerçants ont permis de mener le projet jusqu'à son terme.

Un appel direct aux dons des commerçants n'aurait sans doute pas produit le même effet car ici, comme dans tout système de promotions, ceux-ci ont accepté de réduire leurs marges ou de travailler à perte tout en gagnant de nouveaux clients. Ils ont enregistré un manque à gagner mais n'ont pas dû autant puiser dans leur trésorerie que ne leur aurait demandé le versement d'un don en monnaie officielle.



La monnaie créée ici a bien été *complémentaire* : elle a créé une richesse supplémentaire, en l'occurrence non pour ses porteurs (qui auraient pu être payés en monnaie officielle) mais pour ses émetteurs. **Elle a permis de surmonter un manque d'argent**.

*

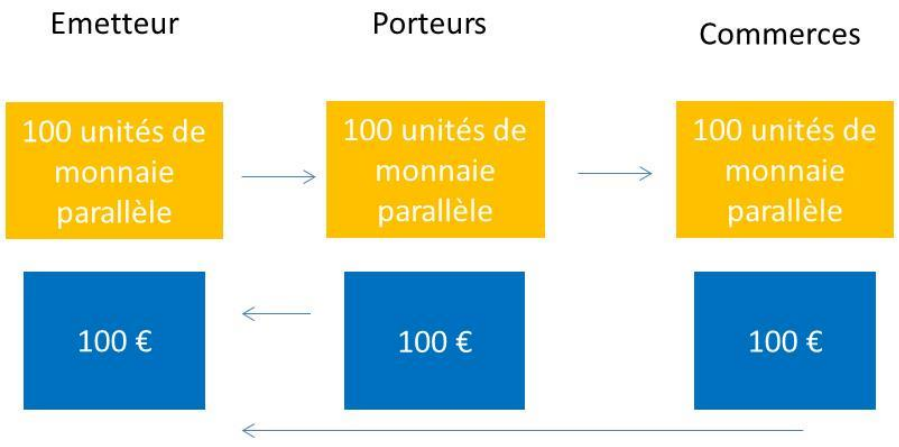
Les monnaies locales.

Les monnaies locales se sont développées à l'échelle de villes, de départements (en France, le **Galléco** d'Ille-et-Vilaine, par exemple) ou de région (Allemagne).

Galléco

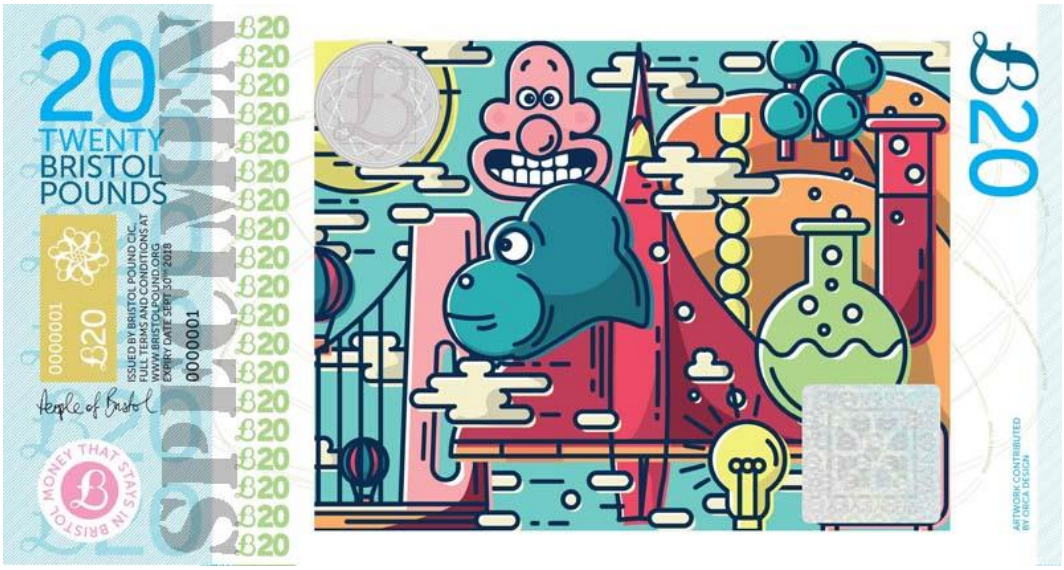
Une monnaie pour agir

Dans la plupart des cas, une association à but non lucratif (qui bénéficie généralement d'une subvention des pouvoirs publics pour son fonctionnement) émet une monnaie parallèle que les particuliers peuvent acheter et qu'ils doivent utiliser dans un réseau de commerces locaux affiliés, c'est-à-dire choisis par l'association selon différents critères, notamment de conformité à des normes et objectifs en matière de responsabilité économique, sociale et environnementale.



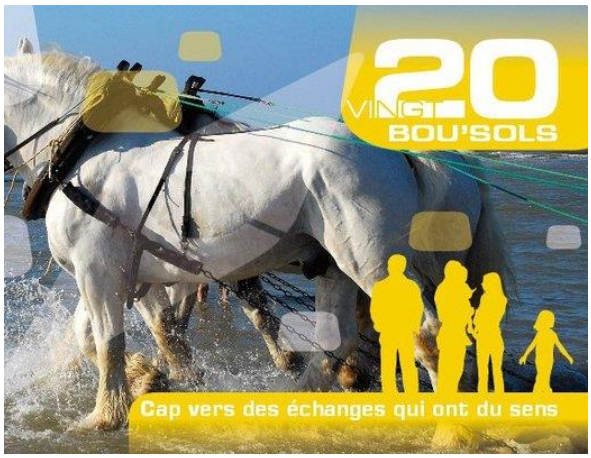
On acquiert une unité de monnaie locale contre un euro (selon le Traité de Lisbonne, seules les monnaies émises par les Banques centrales ont un

cours légal en Europe). Aucun intérêt n'est attaché à la conservation de la monnaie parallèle et il n'y a pas d'intérêt à l'épargner. **Strictement parallèle, la monnaie locale double la monnaie officielle pour les échanges marchands de proximité** (ainsi que, parfois, pour le règlement d'impôts ou taxes). **Il n'y a pas création de richesse**. Porteuses d'un enjeu essentiellement symbolique, ces monnaies – strictement comparables aux « colliers » du Club Med – **fonctionnent comme un label**. Elles veulent tourner vers l'économie locale, favoriser les circuits courts de distribution, sensibiliser à certaines valeurs sociales et environnementales – et maintenir une diversité de commerces à l'échelle locale, comme s'est fixé pour objectif la **Livre de Bristol**, l'une des plus importantes de ces monnaies.



Il est rare cependant que ces monnaies arrivent à convaincre une partie significative de la population. En France, chacune des trente monnaies parallèles qui ont été développées (et pour certaines, comme le **Sol alpin** de Grenoble, arrêtées) rassemble en moyenne 450 utilisateurs particuliers et 90 commerçants. La **Roue**, monnaie régionale créée en 2012 en Provence-Alpes-Côte d'Azur, ne comptait que 200 utilisateurs fin 2015.

Pour les promouvoir, **les collectivités publiques peuvent permettre d'être payées en partie grâce à ces monnaies**. C'est le cas par exemple des **Bou'Sol** de Boulogne-sur-Mer ou de la Livre de Bristol, qui serait utilisée par 10% de la population de la ville.



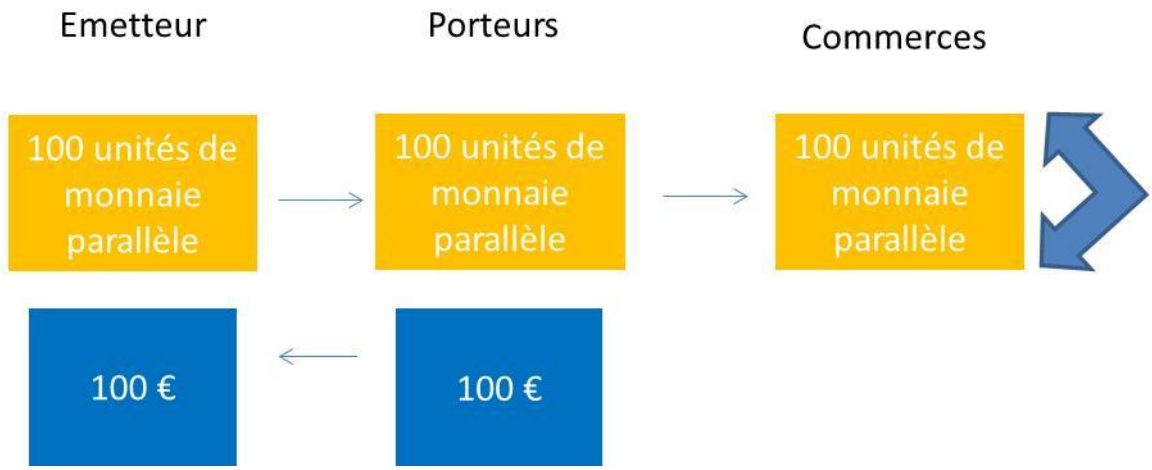
Cette solution entend prévenir l'évasion fiscale que les systèmes de monnaie parallèle peuvent favoriser, jusqu'à permettre l'apparition d'une véritable économie souterraine, comme ce fut le cas avec les « **eco-aspromonte** », la monnaie parallèle mise en place par le Parc régional d'Aspromonte en Italie qui, utilisable à l'intérieur du parc pour tous les achats et librement convertible, donnait lieu à une réduction générale de 5% dès lors qu'elle était employée plutôt que l'€ pour régler des achats.

Toutefois, quel est l'intérêt de payer ses taxes et impôts au moins en partie en monnaie parallèle ? Celle-ci sera reconvertie en monnaie officielle, réduisant d'autant le nouveau circuit économique créé.

Il est tout à fait possible de soumettre les transactions réalisées en monnaie parallèle aux mêmes obligations fiscales que celles qui s'imposent aux transactions en monnaie officielle et, souvent alors, taxes et impôts doivent être réglés en monnaie officielle. C'est que, **pour créer de la richesse, il faut maximiser les encaisses en monnaie parallèle et donc éviter que celle-ci ne soit convertie**.

Il est ainsi possible d'introduire des variantes dans le schéma de base. La première consiste à ne pas permettre aux commerçants qui la reçoivent de convertir la monnaie parallèle en monnaie officielle (cas de la **SoNantes**, à Nantes) ou d'appliquer à la conversion une commission relativement élevée qui pousse les commerçants à tenter d'utiliser plutôt la monnaie parallèle (cas de l'**Eusko**, au pays basque, la monnaie parallèle la plus active en France, réunissant plus de 600 commerçants).

On recherche alors un « **effet multiplicateur local** » : les commerçants et professions libérales locales tendent à s'acheter produits et services entre eux. Un flux d'affaires supplémentaire peut ainsi être produit, qui est une création de richesse.



Et le schéma peut encore être renforcé si les commerçants s'engagent à accorder des promotions pour tous les achats réglés en monnaie parallèle, en contrepartie du fait que celle-ci leur fait gagner et leur fidélise des clients.

C'est alors **comme si l'on avait réalisé une dévaluation compétitive pour les productions locales. La nouvelle monnaie n'est plus seulement parallèle mais devient complémentaire : elle ajoute de la richesse à celle qui est détenue en monnaie officielle**. Ce système de promotion a notamment été développé dans le cas de la SoNantes, ainsi que (plus timidement) avec la Livre de Bristol.

La création de richesse monétaire supplémentaire est néanmoins bien moindre que dans le cas des systèmes d'échanges de biens et de services.

*

Les réseaux monétaires fondés sur l'échange de biens et de services

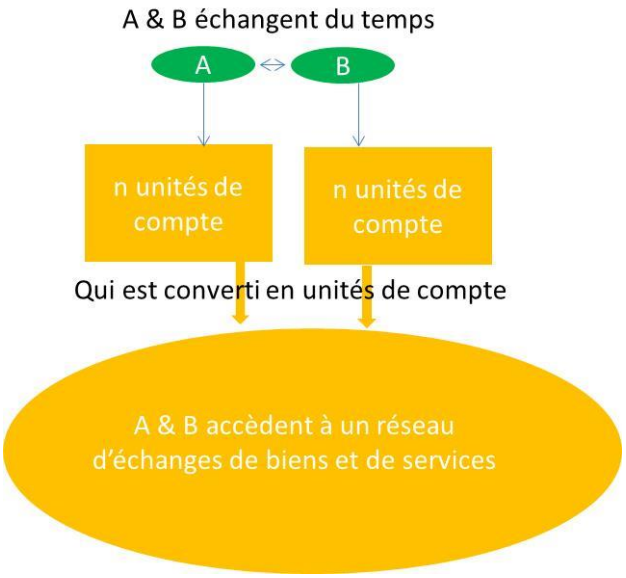
Imaginez un système de pur troc : on échange des biens contre d'autres biens. C'est très mal commode ! Je veux troquer ma voiture contre une moto. Il me faut donc trouver quelqu'un qui a la moto que je cherche et qui veuille bien ma voiture en échange. Ce n'est pas simple. Par ailleurs, s'il veut ma voiture et autre chose, un chapeau par exemple et que je n'ai pas de chapeau… Pour simplifier un tel système, il faut introduire une unité de compte qui permettra d'exprimer la valeur de quelque chose par rapport aux autres et qui pourra servir à échanger toutes ces choses – qui servira donc de monnaie, même si ce n'en est pas vraiment une. Par exemple, en nous limitant à des services simples, comme garder des enfants ou faire le ménage, on pourrait convertir ces services en unité de temps passé : une heure de ménage, une heure de garde et nous pourrions alors par exemple échanger deux heures de garde contre une heure de ménage, etc. Un tel système a ceci de particulier qu'il nous rend tous égaux au départ : nous disposons tous de 24 heures par jour. Nous recevons donc tous la même dotation initiale de monnaie et tout cela peut s'organiser à travers une monnaie parallèle : des **billets de temps**. C'est le principe des **banques du temps** qui, à l'initiative d'une population largement féminine, ont fleuri en Italie – on en compte 300 aujourd'hui – ainsi qu'en Espagne et aux Etats-Unis.

En France, venant du Québec (où elles furent lancées en 2002), huit « **Accorderies** » se sont développées.

Bien entendu, le principe peut être étendu aux échanges de biens, comme avec les **Local Exchange Trading System (LETS)**, lancés à Vancouver en 1983 et qui se sont ensuite développés dans bien d'autres pays, comme les **Systèmes d'échange locaux (SEL)** en France ou les **Tsukisara** au Japon.

On peut alors échanger des biens contre des services, des services contre d'autres services, des biens contre d'autres biens. Tout est exprimé dans une même unité de compte, qu'on gagne à travers des carnets que les adhérents au système se signent réciproquement. Le troc est dépassé : ce qu'on gagne en rendant tel service à quelqu'un peut être dépensé en achetant un bien à quelqu'un d'autre.

Dans ces systèmes, l'unité de valeur est souvent le temps passé. Pour les SEL (on en compte de 350 à 400 en France), la monnaie parallèle est le **piaf**, qui vaut une minute, une heure valant 60 piafs, etc. Mais le prix des biens et des services est fixé de gré à gré par ceux qui les échangent. Ils peuvent ainsi varier au gré des transactions, sur la base d'un catalogue des offres et des demandes formulées par les adhérents au système (dont les frais de fonctionnement sont acquittés à travers les cotisations en € versées à l'entrée par les adhérents).



Dans ce schéma, **deux éléments sont à distinguer : 1/ le circuit d'échange que la monnaie complémentaire permet d'instituer ; 2/**

l'acquisition de cette monnaie d'échange, qui ne correspond pas à une conversion de la monnaie officielle dans la monnaie complémentaire mais à une création de cette dernière. Il s'agit donc bien de créer une richesse supplémentaire, particulièrement quand la monnaie officielle vient à manquer ou ne recueille plus guère de confiance. La nouvelle monnaie est bien complémentaire de la monnaie officielle et elle peut même se substituer à elle en tout ou partie et devenir ainsi une monnaie **alternative**.

Ce genre de solution éclot donc particulièrement dans le contexte d'un affaissement économique conjoncturel, marqué par des encaisses en monnaie faibles chez les agents économiques ou par une forte dépréciation de la monnaie officielle, sous l'impact d'une dévaluation monétaire ou d'une crise de confiance. En Argentine, au début des années 2000, se sont ainsi développées différentes monnaies comme le **Patacon** (Buenos-Aires) ou le **Bocade** (province de Tucuman), avant d'être interdites en 2003 par le FMI. En Grèce, depuis 2010, une quinzaine de monnaies complémentaires sont apparues, comme le **TEM**. Le gouvernement grec fut même tenté de lancer une monnaie complémentaire d'échelle nationale, prenant pour modèle les **IOU** (*I Owe You*) émis en Californie en 2008.

Ce genre de monnaie peut également apparaitre dans un contexte de marasme économique et notamment dans une situation dite de « **trappe à liquidité** » quand, inquiets, les agents économiques limitent leurs dépenses au maximum et thésaurisent par précaution (plutôt qu'ils n'épargnent pour profiter de taux d'intérêts avantageux). Dans un tel cas de figure, les monnaies complémentaires créées peuvent être « **fondantes** ».

L'idée en revient à l'économiste Silvio Gesell, initiateur d'un système de monnaie parallèle à Wörgl, dans le Tyrol autrichien, dans les années 30. Pour répondre au marasme économique créé par la crise de 1929, Gesell voulait en effet **favoriser la circulation monétaire pour relancer l'économie**. Il eut donc l'idée de **déprécier la monnaie en circulation** elle-même. De nos jours, ce schéma est parfois repris par certaines monnaies parallèles, dans le même but : accélérer la circulation monétaire. A Toulouse, ainsi, les **Sols violette** perdent 2% de leur valeur s'ils ne sont pas échangés dans les trois mois après leur émission (dans les six mois pour l'**Abeille**, lancée en 2010 par l'association Agir pour le vivant).

S'agit-il cependant d'une si bonne idée ? Les monnaies parallèles et complémentaires ne produisent pas d'intérêt et ne présentent donc guère d'avantage à être épargnées. Si elles perdent en plus automatiquement de la valeur, les commerçants qui les encaissent ne peuvent que s'estimer lésés. Le système n'aboutit alors qu'à favoriser l'inflation.

L'approche de Silvio Gesell n'en était pas moins intéressante en ce qu'elle contestait la loi classique des débouchés de Jean-Baptiste Say, voulant que la monnaie soit neutre et ne puisse en rien impacter le fonctionnement des marchés, empêchant notamment, si elle manque, qu'une offre trouve sa demande. C'est à ce titre que Gesell intéressera John Maynard Keynes (qui ira jusqu'à écrire que la postérité retiendra le nom de Gesell bien plus que celui de Marx !). Gesell pointe le fait qu'entre

les agents économiques **la répartition de la monnaie peut être très inégale ou sa circulation très compromise**. Dès lors, des activités économiques peuvent se heurter à un manque d'argent pour se réaliser. C'est là proprement l'objet des monnaies complémentaires qui est de permettre **la création d'un supplément de richesse, puisqu'elles permettent à des services ou des biens de trouver preneurs, ce qui ne serait pas le cas s'ils devaient être payés en monnaie officielle**. A cet effet, la monnaie complémentaire est créée soit en monétisant un échange de biens ou de services physiques, soit en accordant, à l'entrée des nouveaux adhérents sur le réseau, un crédit ou découvert. En quoi elles fonctionnent comme les banques privées qui créent de la monnaie à travers les crédits qu'elles accordent : les crédits créent des dépôts. Mais, à la différence des banques privées, elles n'ont pas la contrainte de disposer des liquidités correspondantes pour permettre aux dépôts d'être dépensés. Elles peuvent créer autant d'unités de compte qu'elles veulent. A l'instar des banques centrales, elles disposent d'une « planche à billets ».

Il y a là **un schéma porteur qu'il serait trop restrictif de limiter seulement aux situations de crise**, comme si les monnaies complémentaires représentaient une sorte de « système D » en cas de débâcle financière. Les monnaies complémentaires peuvent également et sur une plus longue durée être utiles pour lutter contre des situations de sous-développement ou de paupérisation dans des régions où l'activité économique décline ou peine à décoller. C'est ainsi qu'une « **monnaie franche** » fut développée en France en 1956 dans le canton de Lignière-en-Berry mais, ne plaisant guère au Ministère des Finances, fut arrêtée deux ans après.

La crainte, pour les autorités monétaires, est en effet de voir les monnaies complémentaires devenir alternatives, au moins en partie, par rapport à la

monnaie officielle, favorisant ainsi l'évasion fiscale. D'abord, en effet, la limite avec le travail au noir peut paraitre ténue ; quoique les poursuites exercées contre des SEL dans les années 90 pour travail clandestin n'aient pas abouties. Finalement, les SEL ont été exonérés de TVA dans la mesure où ils financent des activités non répétitives, non professionnelles. De fait, les réseaux d'adhérents aux monnaies complémentaires atteignent rarement une taille significative. Dans les réseaux les plus conséquents, comme les LETS, elles couvrent peut-être de 3% à 5% des besoins de leurs membres, guère plus.

Ensuite, il est possible de voir les monnaies complémentaires se substituer à la monnaie officielle et favoriser la formation d'une économie parallèle, dans la mesure où, évitant taxes et coûts de transaction (notamment bancaires), elles permettent de fixer des prix moins élevés pour les services et les biens – exactement, comme dans le cas de certaines monnaies parallèles, présenté ci-dessus, comme s'ils avaient connu une dévaluation compétitive. **Tout dépend** cependant **de l'attitude des autorités fiscales et monétaires**.

L'un des exemples les plus aboutis de monnaie complémentaire sont les **Ithaca hours** – une monnaie fondée sur le temps travaillé - mis en place dans la ville d'Ithaca aux USA en 1991 (une librairie fait office de banque centrale).

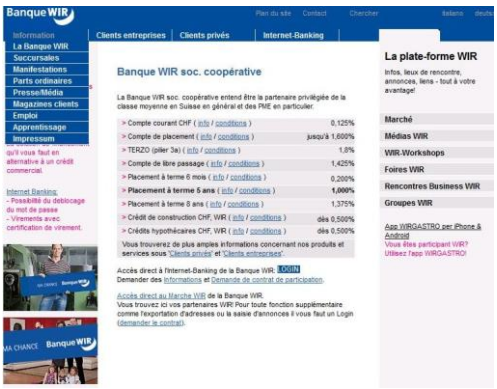
L'exemple a été suivi par 25 autres villes proches et les autorités du Comté se sont engagées à garantir les *Ithaca hours* contre les contrefaçons exactement comme pour les $. Une réaction assez différente de celle des autorités françaises donc, qui s'explique par **une tradition de *free banking* (libre émission de monnaie) propre à la culture américaine** – en prélude à l'Indépendance, la Nouvelle-Angleterre puis d'autres Etats créèrent leurs propres monnaies pour s'affranchir de la rareté des Livres anglaises bloquant leur développement.

Cet exemple illustre le fait que l'essor des monnaies complémentaires n'est pas forcément réservé aux situations de crise. C'est notamment le cas avec les barters.

*

Les réseaux de compensation ou barters

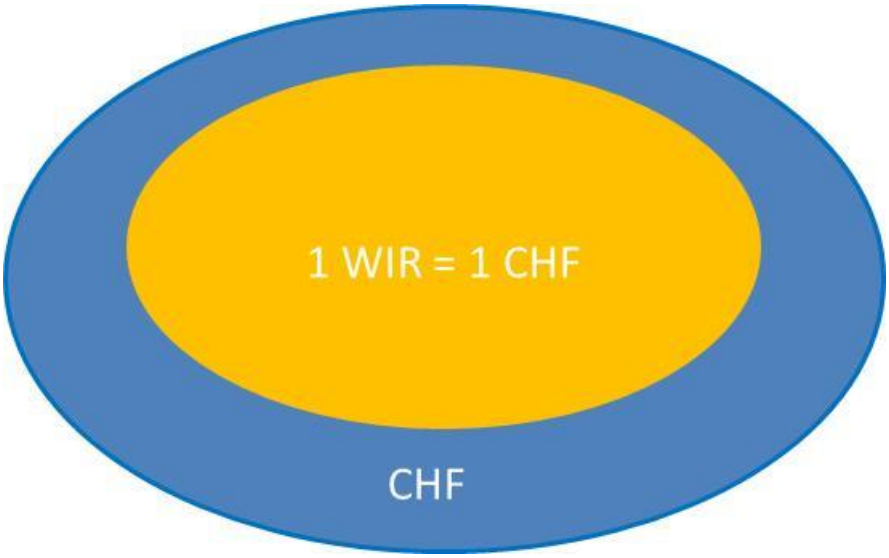
La coopérative **WIR** (abréviation de *Wirtschaftsring* : cercle économique) a été créée à Bâle en 1934 par deux hommes d'affaires, dans un contexte de manque de liquidités suite à la crise de 1929 – on a pu estimer que, dans les années 30, 20% des billets de francs suisses avaient été soustraits de la circulation par thésaurisation. Au départ, la nouvelle monnaie, le WIR, était fondante, ce qui fut abandonné par la suite.



Devenue une banque en 1998, WIR existe toujours et réunit aujourd'hui 60 000 clients, dont 45 000 PME (soit 7% de toutes les entreprises

suisses). Elle a développé une gamme classique de produits et de services bancaires (des chéquiers, des cartes bancaires à double entrée en WIR et en CHF, des produits de placement, etc.) à l'adresse des entreprises et des particuliers.

WIR est un **Barter** : une plateforme d'échange interentreprises. WIR émet un catalogue de biens et services produits par les PME adhérentes à la plateforme, qui sont réglables en tout ou partie en WIR, c'est-à-dire finalement en tout ou partie échangeables en d'autres services ou biens. Mais cela n'apparait plus. Les participants utilisent simplement une monnaie particulière, exactement comme ils peuvent le faire avec le francs suisse. WIR est **une monnaie complémentaire totalement intégrée**. Elle permet l'échange de biens et services à travers des moyens de paiement, exactement comme la monnaie officielle.

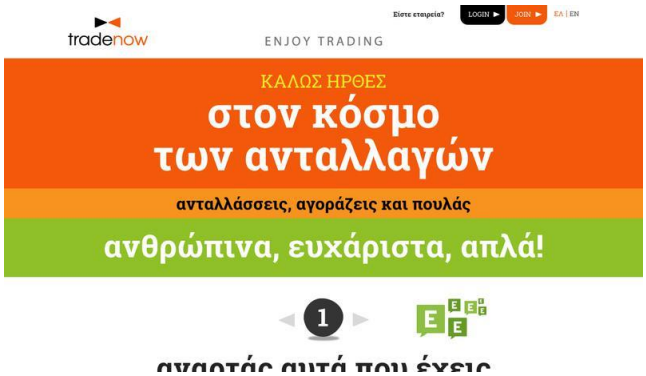


Pourquoi utiliser des WIR alors ? Surtout dès lors qu'ils sont à stricte parité (1 = 1) avec les francs suisses ? Parce qu'ils permettent d'acquérir des biens et services sans avoir à mobiliser, au moins en partie, sa trésorerie en francs suisses – à la seule réserve que les taxes qui s'appliquent aux transactions (qui sont les mêmes que pour toutes les transactions) doivent être acquittées en francs suisses. Il y a bien une

création de richesse supplémentaire pour l'économie suisse puisque l'on peut entrer dans le système à travers un crédit en WIR. Il faudra donc vendre sur la plateforme et ne pas se contenter d'acheter et l'on sera poussé à y entretenir un flux d'affaires régulier, dans la mesure où les soldes en WIR ne sont pas convertibles en francs suisses.

*

D'abord formés dans les secteurs de la publicité et du tourisme, on compte aujourd'hui plus de 800 barters dans le monde. Aux USA, ils rallient plus de 200 000 entreprises. En Grèce, Yanis Deliyannis a créé en 2013 la plateforme en ligne de troc **Tradenow**, qui fonctionne en **tradepoints** (1 tradepoint = 1 euro).



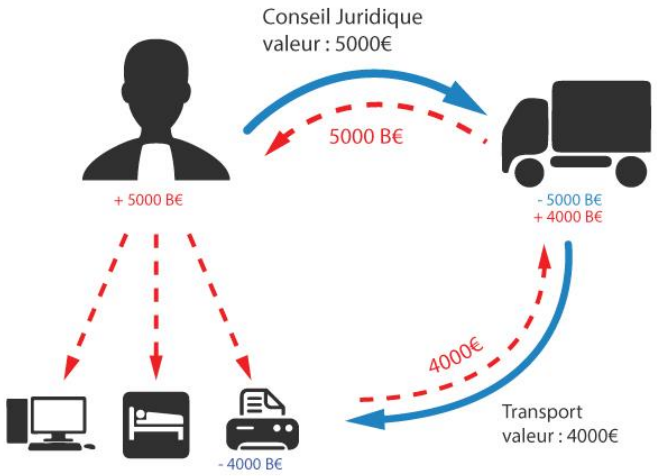
Ces plateformes se rémunèrent (en monnaie officielle) généralement à travers l'abonnement de leurs utilisateurs, qui peuvent également être des particuliers, ainsi qu'à travers une commission prise sur les transactions ; lesquelles ont souvent lieu dans une monnaie complémentaire, comme les « **trade-euros** » du barter belge RES (lancé en 1996).

Les réseaux de compensation interentreprises apportent **des avantages**, qui expliquent la croissance actuelle des barters à travers le monde :

- ils diminuent les besoins en trésorerie des entreprises et donc leurs besoins en fonds de roulement

- Tout en leur offrant un circuit de distribution privilégié, à forte fidélisation.
- Ils sont à même d'améliorer les délais et la sécurité des règlements

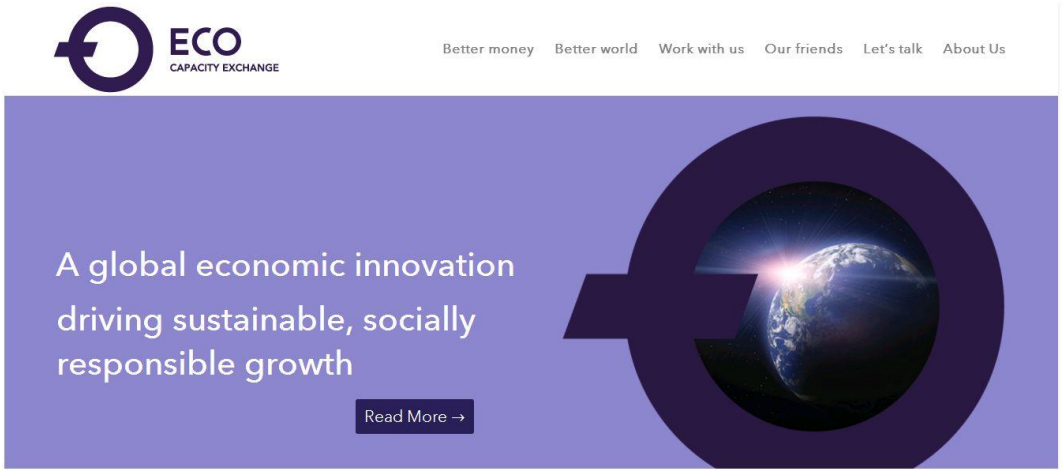
En France où, à part dans quelques secteurs, les systèmes de troc se sont peu développés, un barter a été lancé en 2014 avec le soutien des pouvoirs publics et du Crédit coopératif : **France Barter**. Il fonctionne de la même manière que les autres : les entreprises s'abonnent à la plateforme (pour 235 € par an). Elles échangent des services et des biens en une unité monétaire, le **B€** (prononcez « Barter euro »). Par ailleurs, France Barter a constitué un réseau d'animateurs commerciaux qui recherchent les prestataires répondant à des besoins précis et qui n'auraient pas encore intégré la plateforme. Début 2017, France Barter comptait 600 entreprises clientes, qui avaient échangé l'équivalent de 3 millions €.



En général ces plateformes relèvent d'initiatives prises en marge du système financier en place et sous le registre de l'économie sociale et solidaire. Cependant, **l'exemple de WIR invite à demander qui mieux que les banques serait à même de développer de tels systèmes auprès de leurs clientèles d'entreprises ?** C'est une grande partie des achats de ces dernières qui pourraient être directement traités par

compensation, de compte en compte, entre PME clientes d'un même établissement et une forte incitation pour celles qui ne sont pas clientes de rejoindre l'établissement qui proposerait une telle solution.

Les banques n'auraient-elles pu, seules ou à plusieurs, monter une plateforme comme l'**Eco Capacity Exchange** ?



Fondée sur une monnaie propre, l'**ECO** (*Entreprise-based Credit Obligation*), cette plateforme qui vise d'abord multinationales et institutions publiques, permet l'échange direct entre entreprises, contre services et produits de tous types, de capacités inutilisées dans les grands domaines des ressources de fonctionnement (énergie, informatique, etc.). A la différence des barters, généralement spécialisés par marchés, ECO est une *marketplace* globale.

Que des banques ou d'autres institutions développent ou soutiennent des barters aurait du sens dès lors que nous vivrons sans doute demain dans un contexte de monnaies plurielles, comme invitent à l'envisager les crypto-devises.

*

II – Les crypto-devises

Les crypto-monnaies (ou crypto-devises) sont des monnaies numériques dont des clés cryptographiques assurent la sécurité. On en compte aujourd'hui plus de 700 à travers le monde. Les plus connues – **Ethereum**, **Ripple**, **Litecoin** (un *fork* du bitcoin), **NEM** ou **Dash** ont atteint une valeur de marché supérieure à un milliard de dollars. Les autres, dans leur très grande majorité, se situent à des niveaux très nettement inférieurs. Certaines n'ont cependant pas un objectif de profit mais veulent exercer une responsabilité sociale, environnementale ou identitaire. Le **MazaCoin** est ainsi la monnaie propre de la tribu sioux des Lakota. L'**ImpakCoin** veut favoriser l'économie d'impact.

La plus célèbre des crypto-devises est le **bitcoin**. Il a été inventé par Satoshi Nakamoto et lancé le 3 janvier 2009. C'est une extension du concept de **b-money**, un système électronique de trésorerie anonyme développé par Wei Dai en 1998 et du **bitgold**, une monnaie numérique chiffrée lancée par Nick Szabo, qui était déjà fondée sur une chaine de preuves de travail sur un réseau décentralisé.

Personne ne sait qui est exactement Satoshi Nakamoto, ni qui se cache derrière ce nom qui est très probablement un pseudonyme. Plusieurs

personnes ont déclaré être Nakamoto et d'autres ont été soupçonnées de l'être. L'identité de l'inventeur du bitcoin reste cependant sujette à caution. Depuis un message du 12 décembre 2010, Satoshi Nakamoto n'a plus donné signe de vie. Dans ce message, il désigne Gavin Andresen comme son successeur.

*

Le bitcoin, qu'est-ce que c'est ?

Pour bien saisir la spécificité du bitcoin, par rapport aux monnaies classiques, il faut commencer par souligner deux aspects :

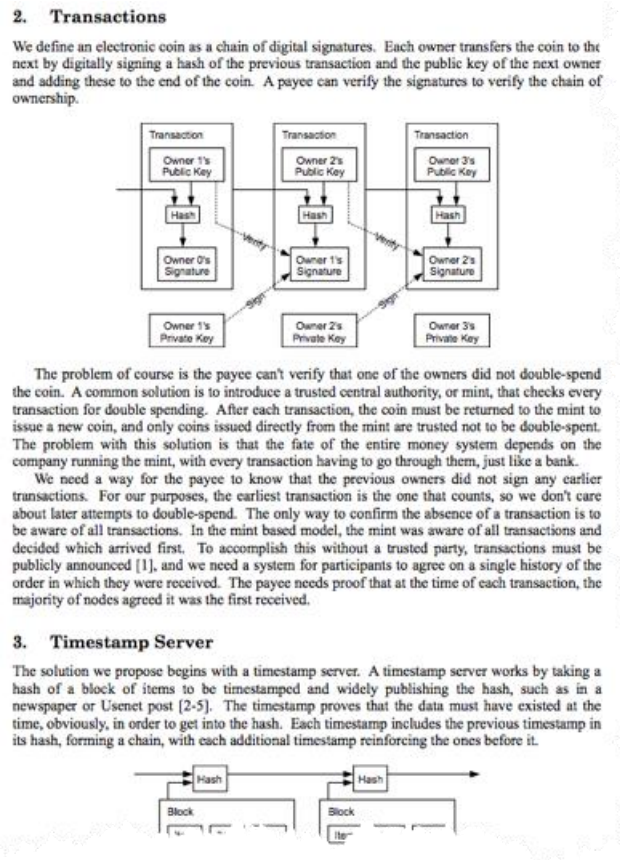
- **Le bitcoin est une monnaie**, qui peut servir à acheter des biens, mais une monnaie **inséparable d'un système de règlement particulier, qui repose sur un protocole informatique nommé « blockchain »**. Les bitcoins n'existent qu'à travers la blockchain. C'est comme si toutes les transactions en dollars ne pouvaient avoir lieu qu'à travers le débit/crédit de comptes ouverts dans les livres de la banque centrale américaine.
- Comme pour toute monnaie, la valeur du bitcoin est fixée par le jeu de l'offre et de la demande. Néanmoins, le bitcoin est **une monnaie dont le nombre d'unités a été fixé a priori et qui n'a pas fini d'être créée**. Dès le départ, il a été décidé qu'il n'existera que 21 millions de bitcoins. Actuellement, 14,5 millions de bitcoins auraient été créés mais, leur émission étant divisée par deux à peu près tous les quatre ans, on estime que le dernier bitcoin sera créé le 7 mai 2140. Au cours le plus haut qu'ils aient atteint à ce stade, la totalité des bitcoins en circulation ont représenté une masse monétaire dépassant les 100 milliards de $. Pour mémoire, le marché de l'or représente 8 200 milliards de $, la totalité des valeurs boursières mondiales près de 70 000 milliards de $ et la masse monétaire planétaire 83 600 milliards de $. **Environ 3**

millions de personnes dans le monde posséderaient des crypto-devises. On estime qu'elles seront 5 millions en 2020.

Il est néanmoins impossible de prédire ce qu'il adviendra du bitcoin. On peut aussi bien imaginer que sa valeur, extrêmement volatile, puisse ne plus rien valoir ou qu'elle devienne une et même la valeur refuge internationale. Par certains côtés, on peut considérer que le bitcoin représente l'une des plus grandes mystifications financières jamais réalisées. Mais, même s'il disparait demain, il aura profondément changé les perspectives monétaires.

*

Tout est donc parti d'un PDF de quelques pages mis en ligne en 2008 par un certain Satoshi Nakamoto.



2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

L'idée était de développer une nouvelle monnaie entièrement numérique sans serveur ni administrateur central. Toutes les transactions y seraient cryptées et le registre serait tenu simultanément sur tous les ordinateurs acceptant de l'héberger. La blockchain est ainsi **un réseau d'appareils informatiques qui forment autant de « nœuds »**, selon le principe du Peer to Peer (pair à pair), à l'image des Torrents, qui permettent d'échanger des fichiers par ordinateur. Il n'y a pas d'ordinateur central qui conserverait la blockchain. Le bitcoin ne fonctionne pas selon une logique informatique client/serveur.

A partir de là, les présentations de la blockchain décrivent pour la plupart celle-ci comme un grand livre de comptes, ou registre partagé – en anglais on parle de *Distributed Ledger*, de livre de comptes distribué - sur lequel on inscrit des transactions. Ce livre de comptes est « partagé » car chacun des nœuds en possède une copie. Le registre est donc sous la surveillance de tous les utilisateurs. **Tout est public et transparent et le principe est de faire confiance au réseau dans son ensemble, sans avoir à faire confiance à quiconque en particulier**. Beaucoup de commentateurs voient là une véritable révolution, qui explique en large partie l'intérêt que recueille la blockchain depuis quelques années. Jusqu'à présent, explique-t-on, on mettait sa confiance dans des acteurs centraux comme les banques, les assurances ou les gouvernements. Mais aujourd'hui, il est possible de fabriquer, avec la technologie de la blockchain, des applications transparentes et inaltérables, dans lesquelles on peut avoir directement confiance sans recourir à un tiers de confiance centralisateur.

Toutefois, si l'on dit souvent que la blockchain est intégralement « décentralisée », ce terme assez confus génère quelques fausses idées. En fait, **le système bitcoin est plus centralisé que celui de toute autre monnaie classique**. C'est comme si la banque centrale américaine tenait registre dans le détail de chacune des transactions que font tous ceux qui

possèdent et utilisent des dollars ! Pour autant, il n'y a pas d'instance en tant que telle qui le fasse. Il n'y a pas d'administrateur central pour gérer les transactions en bitcoins. **Mais ce n'est pas que cette fonction centrale ne soit pas remplie. C'est que la blockchain l'assure**. Quiconque peut la consulter peut normalement voir toutes les transactions dans le détail. On lit par exemple sur Wikipedia que « *le bitcoin se distingue par le fait que son fonctionnement ne requiert pas l'utilisation d'une infrastructure centralisée tenant les comptes des montants détenus afin d'assurer les transactions* ». Mais qu'est la blockchain, sinon une telle « *infrastructure* » !? Le **bitcoin est** plutôt une monnaie dont la fonction de banque centrale a été entièrement privatisée et distribuée entre tous ses utilisateurs (ou presque, voir ci-après).

Dans de nombreux domaines (services financiers, administratifs, de conservation, …), la technologie de la blockchain pourrait avoir un impact considérable et beaucoup veulent même envisager, avec elle, la fin des structures hiérarchiques traditionnelles (!). La blockchain ouvrirait la voie à ce qui était jusqu'ici inaccessible : une gouvernance et une gestion des organisations réellement décentralisée ; entrainant de nouveaux modes de prise de décision, de nouvelles manières de penser la stratégie des entreprises, les objectifs d'une communauté ou de s'accorder sur des valeurs dans un groupe.

Les banques, particulièrement, ont très rapidement réalisé quelle menace la technologie de la blockchain était à même d'exercer sur leurs activités. **Si les transactions se font directement d'acheteur à vendeur, en effet, sans un intermédiaire percevant des frais correspondant au fait qu'il les rend possibles et les sécurise, il n'est plus besoin de banques !** Mais cela signifie moins la fin des banques que la possibilité offerte par un outil informatique à n'importe qui d'exercer un rôle de banquier – et même de banquier central car une monnaie ne représentant plus aujourd'hui qu'un historique d'écritures numériques, des monnaies nouvelles peuvent

apparaître et se multiplier (mais cela pose d'autres problèmes ; le rôle d'une banque centrale ne se limite pas à enregistrer des transactions ; elle remplit notamment une fonction de refinancement qui assure la liquidité du marché interbancaire, fonction qui n'est justement pas remplie avec le bitcoin, voir ci-après).

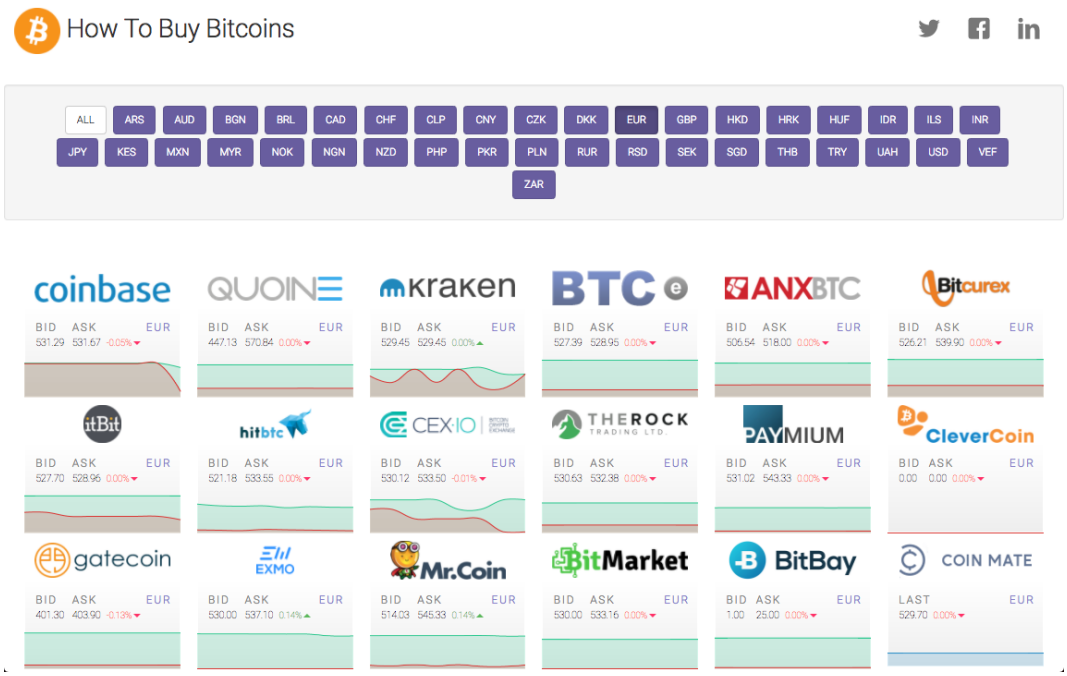
Ce qui menaçait de disparaître avec la technologie de la blockchain, c'est la notion même de banque commerciale, telle qu'elle est apparue avec les lettres de change dans l'Italie du XV° siècle : un tiers de confiance dépositaire qui permet le règlement et ainsi éventuellement le financement par crédit, des transactions de commerce, parce qu'il est capable d'en attester à la fois l'existence et la régularité. D'ailleurs, les contrats, la documentation associée aux transactions et même la notion de signature sont également bouleversés avec un système de *blockchain*. En d'autres termes : **pour organiser un système de transactions, il n'est plus besoin d'un tiers de confiance qui en assure la traçabilité et se rémunère en conséquence**. Qu'il s'agisse de paiements, virements, opérations sur titres, mouvements en compte, etc., il n'est donc plus besoin de banques. Cela explique que, ayant très rapidement identifié la menace, les banques ont été les premières à… investir sur la blockchain !

La menace était-elle réelle cependant ? Pour en revenir au bitcoin, tout ce qui est affirmé ci-dessus quant à la révolution qu'il représente – qui correspond à ce qu'on peut lire le plus généralement – est largement inexact dans les faits. Et **quant à croire que les blockchains, telles qu'elles existent aujourd'hui, pourraient remplacer les systèmes centraux existants, cela parait simplement absurde dans la plupart des cas !** Tous ces discours ne tiennent qu'à ignorer au fond comment fonctionne réellement une blockchain et une crypto-devise comme le bitcoin. De sorte qu'on ne peut éviter d'entrer dans le détail de son fonctionnement.

*

Se procurer des bitcoins

Cela est possible de différentes manières. Comme pour les autres principales crypto-devises, le plus simple est d'acheter des bitcoins sur une plateforme comme **Coinbase**, leader mondial. On y ouvre un compte sur lequel pourront être conservés les bitcoins.



A travers les différentes plateformes, il est donc possible de posséder des bitcoins sans entrer directement dans le système bitcoin lui-même. Une plateforme comme Coinbase, qui affirme conserver les avoirs de 10% des détenteurs de bitcoin dans le monde, fonctionne exactement comme une banque et permet à ses clients d'accéder, via son intermédiaire, à des places de marché de crypto-devises comme GDAX.

Conserver des bitcoins.

Comme il vient d'être souligné, ceci peut être fait à travers les plateformes spécialisées, sans entrer dans le système lui-même. Cela suppose néanmoins d'avoir confiance dans la plateforme choisie, ce qui, à ce

stade, peut paraitre encore hasardeux. Il est donc recommandé de télécharger un parmi les nombreux portefeuilles électroniques spécialisés, ou *wallet*, qui existent :

Certains de ces portefeuilles, comme Bitcoin Core, imposent de télécharger toute la blockchain (moins de 200 Go à ce stade) et de devenir ainsi un « nœud » du réseau. D'autres portefeuilles ne l'imposent pas.

Il n'est donc pas tout à fait exact de dire que la blockchain est partagée entre tous les participants au système. Même les nœuds du réseau peuvent décider d'installer un "nœud complet" (*full node*) sur leurs appareils, c'est-à-dire un exemplaire local et total de la blockchain. Ou bien, ils peuvent se contenter d'un nœud léger (*lightweight node*). Les nœuds « complets », dont le nombre correspond à celui des exemplaires de la chaîne de blocs réellement disséminés entre les membres du réseau bitcoin, sont estimés à environ 6 000 sur un total de nœuds qui se comptent probablement en dizaine de milliers dans 85 pays sur tous les continents. **Toute la blockchain et la confiance qu'on peut placer en cette dernière reposent ainsi sur le principe d'un système partagé, accessible à tous et donc parfaitement transparent qui n'est en fait pas du tout respecté !** En fait, le contraire serait tout à fait étonnant car, à part les « mineurs » (voir ci-après), quel intérêt pourraient bien avoir les

possesseurs de bitcoin à stocker sur leur ordinateur une base de transactions chiffrées, longue à télécharger et dont la taille excédera bientôt les capacités de stockage de la plupart des ordinateurs courants ? **Le principe de registre partagé, qu'on présente comme révolutionnaire, se heurte d'emblée à deux épreuves de réalité assez insurmontables : 1) l'incapacité technique** - si Visa tournait sur une blockchain, chaque possesseur d'une carte bancaire devrait-il s'équiper des gigantesques serveurs nécessaires pour stocker les transactions !? ; **2) le manque d'intérêt**. Cela sera en effet souligné plus loin, sauf à compter au départ sur le dévouement de quelques *geeks*, une blockchain, telle que celle du bitcoin, ne peut tourner que si elle ménage des possibilités d'enrichissement. Contrairement à ce qu'on dit le plus souvent, une blockchain repose sur un mode opératoire extrêmement onéreux. Pour le reste, comme indiqué, **il est possible pour les participants – et cela semble en fait assez nécessaire ! - de s'affranchir de la nécessité de charger la base mais c'est alors le principe même de la blockchain qui est abandonné !**

Payer en bitcoin.

A partir d'un portefeuille, il est possible de réaliser des transactions en bitcoins. Pour cela, le portefeuille génère deux types de clés. La première, privée, permet de signer ses transactions ; la seconde, publique, permet d'être reconnu au sein du réseau.

Rien n'oblige à associer son identité réelle aux deux clés. Cette disposition est sans doute celle qui a fait le succès du bitcoin : il permet de réaliser des transactions monétaires dans un total anonymat. Le réseau ignore qui sont réellement ses membres. Cela, est-il souvent souligné, est à même de bénéficier à des entreprises criminelles. Mais, plus généralement, cela peut surtout favoriser l'évasion fiscale.

Il convient néanmoins de souligner que les plateformes sur lesquelles il est possible d'acheter et de vendre des bitcoins sont censées enregistrer

l'identité de leurs clients. Elles sont en effet de plus en plus soumises aux obligations bancaires en matière de lutte contre le blanchiment. En Australie, tous les échanges de crypto-devises réalisés à partir d'une plateforme nationale doivent désormais être immatriculés auprès de l'Australian Transaction Reports & Analysis Centre, lequel est libre de créer des règles pour élargir ou restreindre la portée de la définition de la monnaie numérique. Le Japon a mis en place de semblables dispositions en 2014 – ce qui a d'ailleurs eu pour effet, a-t-on noté, de renforcer la valeur du bitcoin !

A partir de là, serait-il possible de tracer les transactions sur la blockchain d'un individu dont on saurait qu'il s'est procuré tant de bitcoins à telle date, c'est-à-dire de l'identifier à travers sa clé publique ? Il n'est pas de réponse tout à fait claire à cette question et les réponses varient avec les spécialistes. Si l'on veut protéger son anonymat, il est néanmoins recommandé de multiplier ses adresses et donc de générer plusieurs paires de clés (ce que proposent d'ailleurs les portefeuilles)…

Fondée sur une méthode cryptographique nommée ECDSA, la clé privée est une signature numérique qui permet de s'assurer que personne n'initie une opération à la place d'une autre (la probabilité que deux clés privées identiques soient générées par hasard est quasi nulle). Il convient donc de la garder secrète et de pas l'oublier ou la perdre car les bitcoins seraient alors irrémédiablement perdus – en 2013, quelqu'un a ainsi perdu 7 500 bitcoins en jetant… le disque dur sur lequel était enregistrée sa clé privée ! Fin 2017, l'équivalent de plus de 3 millions $ ont été dérobés à travers un portefeuille électronique truqué, **mybtgwallet**, qui demandait à ses utilisateurs et acquéreurs de bitcoin gold leurs clés privées.

Sur la blockchain bitcoin (à la différence d'Ethereum, voir ci-après), les avoirs en bitcoins d'un participant doivent être reconstitués à partir de ses différentes transactions, inscrites sur le registre. **Il n'y a pas de compte**

personnel retraçant la balance des transactions et donnant un solde disponible en bitcoins. C'est **l'une des principales lacunes du système** car il n'y a pas en conséquence de dispositifs bloquant des opérations dont les montants excéderaient ce solde disponible. **Cela a obligé à définir un dispositif de validation des transactions très lourd, qui représente le cœur du système**.

Lancer une transaction.

Un seul type de transaction est possible sur la blockchain bitcoin : transférer des fonds. Et pour prouver qu'on dispose bien de ces fonds, en l'absence de compte, il faut faire référence à la précédente transaction, laquelle fait référence à la transaction qui l'a précédée, etc. Pour que A paie B, via le réseau, A a besoin de la clé publique de B, qui doit la lui communiquer, et de sa propre clé privée. A n'envoie pas des bitcoins – lesquels sont totalement dématérialisés. Il envoie un message à B, un script. Ou plutôt – B ne disposant pas d'une sorte de « boite mail » sur le réseau – il envoie sur le réseau un message, visible par tous, dont B est le destinataire à travers sa clé publique.

Toutefois, **cette formulation** – sur laquelle repose en grande partie la séduction de la blockchain comme grand livre totalement ouvert à ses participants - **est tronquée**. **La blockchain n'est justement pas une application centrale à laquelle tous les participants pourraient accéder en même temps !** La blockchain est un réseau de nœuds. C'est un système de pair à pair, dans lequel chaque nœud n'est pas connecté à tous les autres en permanence. A envoie donc sa transaction à un ou à d'autres nœuds qui la transmettent à d'autres, etc., **sans que rien ne les oblige à le faire !** Le système a donc prévu l'envoi par défaut à au moins huit nœuds différents de chaque transaction. Apparait ici **l'un des caractères les plus critiques du système bitcoin** – auquel certains assurent que l'on peut faire davantage confiance qu'à tout autre – **rien n'y**

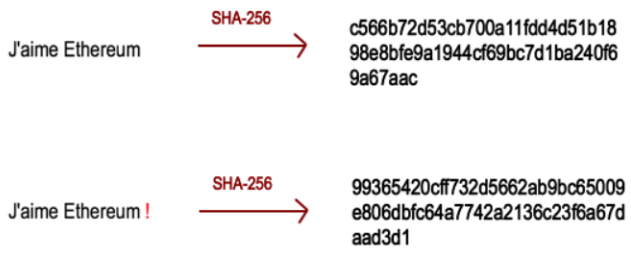
assure la bonne fin d'une transaction ! Plus loin, d'autres aspects le confirmeront.

Chiffrement.

Tous les messages sont chiffrés sous la forme de « hash ». C'est un procédé cryptographique bien connu (nommé SHA-256) qui est à même de caractériser, à travers une fonction mathématique, à peu près n'importe quel contenu numérique. En d'autres termes, tout message ou fichier numérique peut avoir une empreinte ou hash, qui est un code composé de lettres et de chiffres. Par exemple, « *bonjour* », peut être « hashé » sous l'empreinte :

f30ecbf5b1cb85c631fdec0b39678550973cfcbc

Il s'agit bien d'une simple empreinte et non d'un résumé du message : à partir du hash, on ne peut que très difficilement retrouver le contenu du message (seul celui qui a formé le hash avec une clé privée peut inverser la fonction). On parle ainsi de « cryptographie à sens unique ». De plus, le hash ne sera pas plus long parce que la taille du message est plus importante. La spécificité du hash est de traduire à sa façon l'état d'un contenu informatique donné à un instant t. Dès lors, si une modification, même tout à fait mineure (un caractère en plus par exemple, comme « ! »), est introduite dans le message, son hash ne sera plus le même.



Si la donnée entrée change d'un caractère, alors l'image est totalement différente.

*

Ceci posé, on ne peut concevoir que A adresse simplement son paiement en bitcoins à B. A dispose-t-ils des fonds qu'il transfère ? Ne réalise-t-il pas plusieurs paiements dont le montant total excède la somme de bitcoins dont il dispose effectivement ? Sur un système centralisé, il est très facile de répondre à ces questions. Dès lors que l'on adopte le principe d'une gestion partagée, on peut admettre que les choses soient un peu plus compliquées. Sur la blockchain bitcoin, elles sont en fait beaucoup plus complexes. A quel escient ? Pour parvenir à une solution plus performante ? C'est souvent ce que soutiennent les promoteurs de la blockchain, bien qu'il ne soit en fait **guère possible d'assurer que les contrôles, sur la blockchain sont toujours correctement et exactement remplis !** Et sur ce point crucial, le flou dont se contentent la grande majorité des commentateurs ne peut manquer de surprendre. Le processus de validation des transactions représente en tous cas le cœur de la blockchain.

Validation des transactions.

La blockchain suit un principe de gestion non seulement partagée – toutes les transactions sont (en principe, voir ci-dessus) visibles par tous les nœuds – mais par **consensus** : au moins une **majorité** des nœuds doit s'entendre sur un historique commun des transactions valides.

Les transactions en attente de validation entrent dans une liste d'attente (*pending pool*), en principe accessible à tous les nœuds du réseau, sans que rien ne puisse assurer que cette condition sera pleinement remplie (voir ci-dessus). Sachant que la validation des transactions est rémunérée, les nœuds vont entrer en concurrence pour le faire. L'ensemble des transactions en attentes représentant ainsi comme une source de profit, les nœuds qui vont tenter de gagner une certaine somme en les validant sont appelés « mineurs ». L'idée s'est répandue que, décentralisée, la blockchain marche « toute seule », sans aucune

intervention humaine. En fait, une validation de chaque transaction doit être assurée par des mineurs.

Ces mineurs rassemblent un certain nombre de transactions dans un « block » (ce qui allège le processus et permet de ne pas avoir à le reproduire pour chaque transaction) puis ils les valident normalement en reconstituant l'historique de chacune, pour vérifier que chaque vendeur détient bien la somme qu'il cède en retraçant l'historique de toutes ses transactions passées, répertoriées dans les blocs précédents. A ce stade, **rien n'assure formellement que chaque transaction a été effectivement validée**, sinon que les autres nœuds, ou plutôt une majorité d'entre eux, pourront refuser le bloc s'ils estiment qu'il n'est pas valide. La seule parade qui a été mise en place a consisté à limiter la taille des blocs à 1 Mégaoctet (un bloc contient ainsi en général de 1 000 à 2 000 transactions) afin qu'on ne puisse « spammer » le réseau, le saturer avec des blocks d'une taille telle qu'elle dissuade d'en valider toutes les transactions. Mais il peut très bien exister des transactions contradictoires (cas de « double dépense » : une même somme de bitcoins est utilisée plusieurs fois) dans des blocs différents. Quoi qu'il en soit, dès que le bloc sera validé, les transactions qu'il contient seront réputées valides (ou presque, voir ci-après).

Valider un bloc, c'est l'inscrire dans la chaine des blocs déjà validés qui, tous ensemble, forment la blockchain. Mais cela, tous les mineurs le font. Quels blocks seront donc retenus au total ? Ceux dont les mineurs parviendront à trouver le hash particulier, ce qui représente leur « preuve de travail ». Pour chaque block, il s'agit en effet de hasher les éléments suivants :

- Le hash du block dont il veut prendre la suite
- Le hash racine qui est une sorte de hash des différents hash de chacune des transactions que contient le block (à travers un

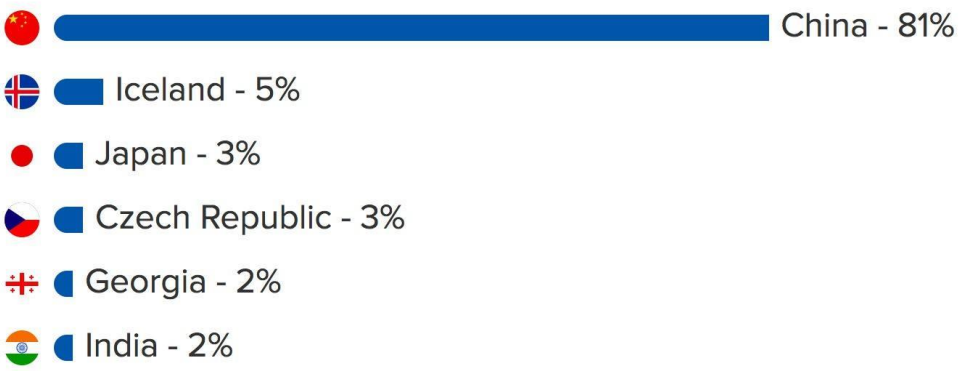
procédé de compression des données nommé « arbre de Merkle »).

- Un horodatage
- Un nombre aléatoire, le « nonce », que le mineur ne connait pas mais qu'il doit trouver.

Pour cela, le système lui indique que le hash final est inférieur à une certaine valeur. Dès lors, un seul nonce convient au hash final et, pour le trouver, il n'y a qu'une seule solution : essayer tous les nonces possibles jusqu'à trouver le bon. L'objectif est de parvenir à valider un block toutes les dix minutes. Plus les mineurs y parviennent dans un laps de temps inférieur, plus la valeur (ou « difficulté ») que le hash final ne doit pas dépasser est importante, ce qui alourdit les calculs et réciproquement.

Au début du système, il était possible de « miner » avec un PC standard. Mais les mineurs se sont équipés de cartes graphiques bien plus puissantes et moins consommatrices d'énergie. Cela a donc accru la difficulté et certains mineurs sont passés à des processeurs FPGA, puis ASIC. Bien entendu, tout cela coûte cher : de l'ordre de 70 000 à 100 000 pour avoir une chance de parvenir à confirmer un block, est-il estimé, sans parler de la consommation électrique. Pour rentabiliser de tels investissements, il faut en fait dépenser bien davantage (et compter sur l'appréciation du bitcoin), pour être à même de confirmer un grand nombre de blocks. Sont ainsi apparues des « fermes » de minage, notamment en Chine, pouvant compter plusieurs milliers d'unités de minage et qui, pour parvenir à gagner 25 bitcoins par jour, dépensent en moyenne 80 000 $ par mois. Dans ces conditions, les mineurs se regroupent en coopératives, afin de réduire leurs coûts mais aussi augmenter leurs chances, qui sont d'autant plus fortes qu'ils sont moins nombreux. Ainsi, **le principe d'une gestion totalement décentralisée a finalement abouti à une centralisation de plus en plus forte – aujourd'hui, cinq**

coopératives se partageraient 80% de la validation des blocks - tout en rencontrant rapidement des limites matérielles.



L'agence Reuters a estimé qu'en 2015 le réseau Bitcoin a consommé 43 000 fois plus d'électricité que les 500 ordinateurs les plus puissants de la planète. En 2020, il est prévu qu'il en consomme autant qu'un pays comme le Danemark ! Bien qu'il soit totalement numérique, **un bitcoin coûte nettement plus cher à produire (1 800 $) qu'une once d'or (1 115 $). Enfin, le principe d'une gestion par consensus est ainsi complètement détourné puisque la validation des opérations repose en principe sur la mise en concurrence des mineurs, ce qui suppose que ceux-ci soient suffisamment nombreux.**

Mais si les mineurs supportent de tels coûts, c'est à proportion de leur rémunération en bitcoin (et donc finalement de la valeur de ce dernier). Néanmoins, le code source bitcoin prévoit une division par deux de la rémunération des mineurs (et donc de l'émission des bitcoins) tous les 210 000 blocs minés, soit approximativement tous les quatre ans :

- de la création du premier bloc jusqu'au 209 999e bloc, créé le 28 novembre 2012, chaque mineur fut récompensé de 50 bitcoins par bloc validé ;
- du bloc 210 000 au bloc 419 999, créé le 9 juillet 2016, la récompense fut de 25 bitcoins ;
- depuis cette date, la récompense n'est plus que de 12,5 bitcoins.

Cette baisse progressive de la rémunération en bitcoins doit être compensée par le développement des frais de transaction, correspondant à une prime pour chaque bloc validé, actuellement trop faible (de dix à quinze centimes d'euros) pour dédommager un mineur du matériel investi et du temps passé.

Il est donc très étonnant que l'on puisse continuer à affirmer que le bitcoin est un système de règlement « gratuit ». C'est **un système spéculatif** – reposant entièrement sur l'attente que le bitcoin s'apprécie – **et non pas gratuit**. **La promesse d'une gestion partagée, sans tiers de confiance, a abouti à mettre en place une gestion incroyablement plus complexe, onéreuse et finalement peu partagée !**

*

Une fois qu'il a trouvé le hash de son block, le mineur communique la solution à tous les nœuds du réseau (si elle est laborieuse à trouver, puisque le nonce est aléatoire, la solution est facile à vérifier une fois le nonce donné). **Les autres nœuds sont censés valider le block, c'est-à-dire les transactions qu'il contient. C'est ici que la procédure est la plus incertaine et que les présentations – même se prétendant les plus techniques – sont en général les plus floues. En quoi consiste exactement cette validation ? Est-elle effectivement réalisée par les différents nœuds ? Qu'est-ce qui en atteste ? Pourquoi, sans perspective de gains en bitcoins, les autres nœuds referaient-ils le travail du mineur qui a trouvé le hash ?** En fait, les autres nœuds « valident » le block dès lors qu'ils le joignent à leur propre version de la blockchain, ou plutôt dès lors qu'une majorité de nœuds choisit de le faire. C'est précisément pourquoi l'on parle de « gestion par consensus ».

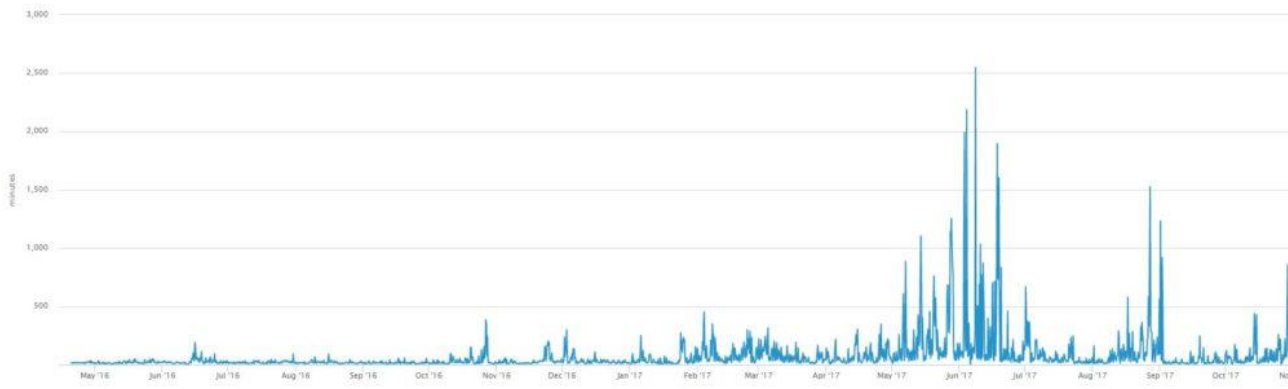
Cela soulève un évident problème : quiconque possède plus de 50% de la puissance du réseau (donc de la puissance de tous les ordinateurs participants) est à même de tourner le consensus en sa faveur. Il maitrise la formation de la blockchain et finalement des transactions qui y sont

enregistrées. **Le système bitcoin, dont on vante l'incomparable sécurité, est en fait assez facile à pirater !** Le coût pour acquérir 51% de la puissance du réseau en l'état actuel des choses a été chiffré. Il ne dépasse pas quelques millions de $, ce qui parait peu face aux possibilités d'enrichissement, dès lors que le cours du bitcoin dépasse les 10 000 $. Face à une telle menace, la réponse consiste généralement à dire qu'une telle prise de contrôle serait vite détectée et provoquerait une fuite des participants. Mais c'est assez discutable. D'abord, la prise de contrôle pourrait être assez discrète – tenant à une entente entre quelques gros participants et se limitant à quelques détournements peu visibles mais fructueux. **Du fait de sa complexité, de sa lourdeur et des moyens importants et coûteux qu'il requiert pour y intervenir, le système bitcoin est à la fois totalement ouvert et complètement opaque**. Il suffit de demander qui serait en mesure, aujourd'hui, de démontrer qu'une telle entente entre certains participants n'existe pas ? Enfin, ceux qui ont investi en bitcoin aux cours qu'il a atteints à partir de l'été 2017 pourraient-ils facilement quitter le système, avec les risques d'effondrement que cela provoquerait ?

Quoi qu'il en soit, une transaction est validée lorsqu'il y a une majorité de nœuds qui l'acceptent. La limite à 1 Mo de chaque bloc a été également introduite pour faciliter ce mécanisme de « consensus », qui est la seule règle ayant été trouvée pour, à partir de multiples interventions sur les différents nœuds du réseau, maintenir une version unique de la chaine. Il peut en effet parfaitement arriver que deux blocks soient validés en même temps. Lequel sera inscrit dans la blockchain ? Une règle a été instaurée : la chaine la plus longue sera validée. En d'autres termes, le premier des deux blocks auquel fera référence un nouveau block créé sera retenu. On dira que chaque transactions du bloc a reçu deux confirmations, puis trois quand un autre bloc sera ajouté aux deux précédents, etc. Et l'on admet qu'une transaction peut être considérée comme définitivement acceptée

lorsqu'elle a reçue 6 confirmations – soit, avec une validation de block toutes les dix minutes dans le système, au bout d'une heure. Contrairement à ce qu'on lit souvent, **les règlements sur le système bitcoin ne sont donc pas instantanés** – mais ils sont plus rapidement validés que sur beaucoup de systèmes classiques de paiements (sauf lorsque les paiements sont assurés ou garantis en deçà d'un certain montant).

Par rapport aux systèmes classiques, une faille apparait néanmoins qui est propre au bitcoin. **Il peut en effet arriver qu'une transaction soit confirmée dans un laps de temps beaucoup plus élevé (une ou deux journées, voire plus d'une semaine) ou ne soit pas validée du tout**. Comme le montre leur historique, les délais moyens de validation des transactions sont susceptibles de beaucoup varier dans le temps :



Récemment, la plateforme de jeux en ligne **Steam** a récemment annoncé qu'elle n'accepterait plus les règlements en bitcoins, notamment à cause de sa forte volatilité mais encore du fait de la lenteur des transactions.

Par ailleurs, des transactions peuvent tout simplement ne pas être retenues par des mineurs pour être incluses dans les blocks qu'ils constituent – dans ce cas, la plupart des portefeuilles finissent par annuler ces transactions (cela peut prendre jusqu'à 15 ou 20 jours). Cela concerne notamment les transactions qui n'offrent pas de frais de transaction ou qui en proposent de faibles.

En principe, dans le système bitcoin, le paiement de frais de transaction est facultatif. Cela a pu laisser croire que l'usage des bitcoins est totalement gratuit. Cependant, les mineurs déterminent l'ordre de traitement des transactions à intégrer dans les nouveaux blocs en fonction des frais de transaction offerts par les utilisateurs. Plus un utilisateur accepte de payer des frais de transaction élevés, plus sa transaction sera traitée rapidement. Pour le moment, ces frais demeurent très faibles. Mais dans un contexte d'engorgement des transactions, l'idée a été émise de les augmenter.

*

Une fois les blocs validés et chainés, par ordre chronologique et chacun étant lié au précédent et au suivant (selon un procédé dénommé CBC, *cipher block system*, développé par IBM et la NSA dans les années 70), la blockchain est constituée. Elle conserve et permet la consultation de toutes les transactions depuis le démarrage du système. Le hashage des blocs garantit qu'ils n'ont pas été modifiés. Si quelqu'un modifiait dans le bloc 1 la somme en bitcoins qu'il détenait alors, cela ne coïnciderait plus avec le hash du bloc 1 qui est contenu dans le bloc 2 et celui-ci dans le bloc 3, etc. La blockchain est ainsi infalsifiable. Sauf à décider qu'il n'en est rien ! Mais qui, en l'occurrence, pourrait exactement en décider ? **Sur un système décentralisé, il ne peut y avoir de gouvernance que par consensus. C'est à la fois une protection (le système ne peut être unilatéralement modifié) et une faiblesse : il est difficile de le faire évoluer**. En 2017, la problématique a été particulièrement rencontrée.

Comme il a été vu ci-dessus, en effet, chaque bloc est limité en taille à 1 Mo. Or, cette disposition pose un problème dit de « scalabilité » : elle restreint à sept le nombre de transactions traitables par seconde, ce qui parait une limite bien trop étroite. La changer, néanmoins, a suscité des débats houleux et épineux au sein de la communauté bitcoin. Il a

notamment été suggéré de développer une solution dite « Segwit » (*segregated witness*) consistant à ne pas augmenter la limite de taille des blocs mais à partitionner différemment les signatures numériques des transactions en "blocs d'extension". Cette solution a néanmoins fait l'objet de critiques la jugeant insuffisante et un compromis a été formulé, appelé « Segwit2x », qui combine la proposition « Segwit » avec une augmentation de taille des blocs à 2 Mo. Cette proposition a été implémentée le 1er août 2017 au bloc 494,784. Elle constitue la première évolution majeure du système Bitcoin depuis sa création. Toutefois, un groupe dissident souhaitant voir passer la taille des blocs à 8 Mo, tout en rejetant la proposition Segwit, a décidé de créer une nouvelle crypto-monnaie appelée **Bitcoin Cash**, qui autorise le traitement de 56 transactions par seconde.

De fait, **le Bitcoin s'est scindé en différentes sous-espèces** – de sorte qu'il faut à présent nommer « **Bitcoin Core** » le bitcoin historique. Il ne s'est pas agi là du premier démembrement ou *fork* de ce dernier. Le Bitcoin Cash (créé en août 2017) a en fait rejoint le **Bitcoin XT** (créé en août 2015), le **Bitcoin Unlimited** (crée en janvier 2016), le **Bitcoin Classic** (créé en février 2016) et représente avec eux autant de crypto-monnaies alternatives au Bitcoin Core.

*

Une nouvelle monnaie qui n'a tenue aucune de ses promesses !

Au total, comment se présente le bitcoin aujourd'hui ? Comme une crypto-monnaie qui a éclaté en différentes branches. Comme un système de règlement, dont on continue à louer les caractères performants et révolutionnaires et qui n'est en fait qu'**une gigantesque usine à gaz** ! Par rapport au fonctionnement de n'importe quelle banque centrale, **la gestion des transactions en bitcoins est d'une lourdeur et d'une complexité phénoménales !,** dont le fonctionnement requiert, symptomatiquement, une consommation énergétique délirante.

Mais le bitcoin est également une monnaie qui n'a tenue véritablement aucune de ses promesses :

- Un fonctionnement intégralement décentralisé ? Le système bitcoin est incroyablement centralisé au contraire, strictement géré par un registre central exhaustif et contraignant.
- Une gestion complètement décentralisée ? Elle est en fait concentrée entre les acteurs d'une communauté de plus en plus restreinte et conjugue tout à la fois des modes de décisions réservés à des spécialistes et une organisation horizontale qui est source de blocages et qui interdit toute rapide évolution d'importance.
- Une monnaie libre ? Mais en quoi ? La traçabilité de toutes les transactions est par définition totale sur la blockchain et il semble assez illusoire de croire que l'anonymat puisse y être absolument garanti.
- Une monnaie accessible à tous ? Du fait de la complexité du système, l'expertise et les moyens nécessaires limitent considérablement l'accès à la communauté des mineurs. Quant au grand public, combien parmi les simples acheteurs comprennent effectivement son fonctionnement et sont à même d'appréhender ses éventuelles évolutions ? Au total, mille personnes détiendraient 40% des bitcoins existants.
- Une monnaie totalement gratuite et des règlements quasi instantanés ? Disons plutôt des coûts de transaction modiques et des délais de transaction rapides mais non garantis, ce qui pourrait néanmoins être largement remis en cause avec la hausse du nombre de transactions, dès lors que l'ergonomie du système ne permet guère d'y faire face.

- Un système parfaitement sécurisé ? Il a fait l'objet d'importants détournements, mis en lumière notamment avec l'arrestation de Mark Karpelès, qui exploitait la plateforme MtGox (fermée en 2014). Par ailleurs, il faut rappeler que quiconque lance une transaction en bitcoin ne peut être sûr qu'elle sera tout simplement traitée !

Récemment, la Directrice générale du FMI a pu considérer que le bitcoin et les autres crypto-monnaies pourraient à terme destituer les banques centrales, les banques conventionnelles et mettre en question le monopole des monnaies nationales. Un tel discours a de quoi laisser rêveur – non pas seulement parce qu'on peut se demander quel serait alors le rôle du FMI ! Christine Lagarde sait-elle bien de quoi elle parle ? Son discours énumère des conditions susceptibles de rendre les monnaies virtuelles plus stables - elles pourraient être émises sur le principe d'une parité fixe avec le dollar ou un panier stable de devises – mais qui les feraient totalement disparaitre telles qu'elles existent aujourd'hui. Sans le dire explicitement, la Directrice du FMI semble en tous cas se satisfaire de la perspective d'une ou de monnaies privées supplantant les monnaies nationales. Pourquoi pas ? Mais face à une telle perspective, **la gouvernance du système bitcoin parait assez problématique !** Qui est effectivement à même de décider exactement de quoi dans l'évolution de cette monnaie privée dont on ne connait même pas les créateurs ? Tous ceux qui célèbrent le caractère libertaire des crypto-devises et voient en elles autant de pieds-de-nez faits aux banques devraient réaliser que **rien n'empêche d'imaginer que, demain, quelques grandes banques internationales deviennent les principaux mineurs et développent les plus importantes plateformes d'achat/vente de bitcoins, mettant ainsi peu à peu la main sur le réseau.** Et sans doute le bitcoin évoluerait-il alors comme l'envisage la Directrice du FMI…

En fait, l'opacité du système bitcoin est totale et, par bien des côtés, le lancement du bitcoin aura ressemblé à une astucieuse mystification. D'emblée, tous les éléments étaient réunis pour séduire – quitte à exploiter la crédulité de beaucoup, avant de pouvoir se reposer ensuite sur l'appât du gain et la recherche de contournements fiscaux. Une monnaie sans banque centrale et sans autorité de supervision, autorisant des transactions totalement libres, en *peer-to-peer*. Un logiciel passant pour avoir été créé par un maitre japonais, dont le nom n'était pourtant qu'un pseudonyme, ce qui créait suffisamment de mystère. Sans oublier l'indispensable petite touche de soufre : presqu'immédiatement, on fit savoir que des mafias de tous genres s'intéressaient de très près à la solution, ce qui, au fond, n'était pas très crédible. Des organisations criminelles ont certainement utilisé le bitcoin mais sans doute pas à la hauteur de ce qu'on imagine du fait de sa très forte volatilité et des risques de perte auxquels elle expose - tandis qu'il était loisible, pour des criminels, d'utiliser ou de créer une crypto-devise moins exposée. La menace obligeait néanmoins les autorités réglementaires à s'alarmer, assurant à la nouvelle monnaie une publicité extraordinaire ! Dans ces conditions, la fortune des vrais acteurs du système – concepteurs et mineurs les plus importants – était faite.

Le système, cependant, présentait de vrais avantages, comme de s'exonérer de frais bancaires pour des opérations de paiement, ce qui explique que de plus en plus d'entreprises, comme Microsoft, aient accepté d'être réglées en bitcoin. Certes, effectuer des paiements et des virements en bitcoin n'est pas gratuit s'il faut utiliser une plateforme, comme Coinbase ou BitPay (qu'a retenue Microsoft). Mais, pour les commerçants, le coût est bien moindre que pour un paiement par carte et ceci essentiellement à cause de l'interchange. C'est-à-dire de la commission que la banque du vendeur facture à ce dernier et reverse à la banque de l'acheteur, en considérant que celle-ci, en fournissant un moyen de paiement à l'acheteur a permis la vente. Or cela, qui pouvait

effectivement être justifié tant que les règlements supposaient d'avoir recours à des supports bien spécifiques (billets et pièces, TIP, cartes et chèques) disparait dès lors que tout se fait directement sur une plateforme en ligne. Si acheteurs et vendeurs utilisent le bitcoin, ils n'ont plus du tout besoin de banques ! Or ceci leur est favorable, puisque l'interchange est transparent pour les acheteurs mais non pour les vendeurs. La baisse des interchanges qui est intervenue aux USA comme en Europe ne modifie pas essentiellement ce constat. Par rapport aux règlements sur internet, **la fourniture de moyens de paiement introduit un surcoût qui n'a plus lieu d'être**. **C'est finalement ce que soulignent les crypto-devises**. De sorte que l'enjeu est aujourd'hui de ne plus utiliser en ligne de moyens de paiement particuliers (voir Score Advisor *L'avenir des paiements*). En ceci, **le bitcoin a montré qu'un réseau de règlement international privé pouvait se substituer, au moins techniquement, aux monnaies étatiques**. Or ni les crypto-devises, ni la technologie de la blockchain ne se limitent au bitcoin – même s'il faut reconnaitre qu'un brutal effondrement de la valeur de ce dernier condamnerait sans doute en grande partie l'intérêt dont elles font l'objet actuellement. Le **Litecoin**, par exemple, utilise un autre procédé cryptographique que le bitcoin, afin que tous les membres de son réseau puissent miner. Avec le **Nxt**, les mineurs sont tirés au sort. **Dash** distingue des « *Master Nodes* » (qui paient). Avec **BitShare**, les mineurs sont élus (voir ci-après). Apparaissent encore des solutions de *Proof of Transaction* et de *Proof of Block*. En d'autres termes, le bitcoin appelait des corrections et des évolutions, que s'efforcent d'apporter un certain nombre d'initiatives – la plus importante étant la blockchain **Ethereum**.

Ethereum (2013) est une organisation à but non lucratif qui propose une plateforme de programmation pour développer la technologie de la blockchain dans tous les domaines. **R3 CEV**, un consortium de 42 banques (Barclays, Crédit suisse, Comm Bank of Australia, HSBC, Natixis, RBS, TD Bank, UBS, Wells Fargo, etc. mais Santander et Goldman Sachs l'ont quitté, suivies par JP Morgan) y teste notamment les opportunités offertes par cette blockchain *as a service*. Microsoft utilise également Ethereum pour sa propre plateforme Azure.

Ethereum a été créé fin 2013 par Vitalik Buterin, un Canadien d'origine russe de 19 ans. En juillet 2014, il finalise une toute première version du protocole et lève près de 19 millions de dollars pour financer le projet. Un an plus tard sort la version *Frontier*, dédiée aux tests des développeurs, qui constitue la phase 1 du développement d'Ethereum.

Ethereum se définit comme le « *premier véritable ordinateur global* », qui permet de construire sur sa plateforme des applications décentralisées utilisant la technologie de la blockchain, les « Dapps » (*Decentralized Applications*).

Ethereum fonctionne avec une monnaie virtuelle, l'**ether**, dans laquelle sont réalisés tous les paiements sur la plateforme. En valeur de marché, l'ether est devenue l'une des principales crypto-devises, derrière le Bitcoin core et avec le Bitcoin cash et le Dash. Cependant, Ethereum n'a pas du tout été bâtie pour concurrencer le bitcoin : il s'agit plutôt de deux utilisations différentes et complémentaires de la Blockchain, même si l'on

ne peut nier l'existence d'une certaine forme de concurrence et d'idéologie entre les deux communautés qui les entourent.

Par rapport au bitcoin, Ethereum apporte d'importantes modifications. Aucun montant maximal d'ethers en circulation, ainsi, n'a été prédéfini. Les mineurs ayant participé à l'ajout de blocks se partagent tous les ans 15,6 millions de nouveaux éthers créés. Il convient de souligner que l'unité de facturation au sein de la blockchain n'est pas l'ether lui-même mais le **gas**, afin de parer une forte appréciation spéculative de l'ether, qui paralyserait le fonctionnement de la blockchain, rendant nombre de ses fonctions hors de prix (car tout ou presque est payant sur Ethereum !). L'ether permet de payer les gas, selon un cours ajusté à l'activité de la blockchain elle-même et non à la valeur de marché de l'ether.

Le minage en pool y est découragé grâce à un protocole spécifique nommé « Ghost » (*Greedy Heaviest Observed Subtree*). L'algorithme de minage (l'*Ethash*) rend impossible l'utilisation de technologies à base de puces ASIC et reste accessible aux processeurs GPU les plus courants et la *proof of work* est remplacée par une *proof of stake* ou preuve d'enjeu ou de mise : la possibilité de miner (on dit en fait « forger ») un bloc dépend non de sa propre puissance informatique mais du nombre d'ethers que l'on a sur son compte. Dans ces conditions, encore moins que pour le bitcoin, l'organisation du minage sur Ethereum – si elle est beaucoup moins lourde et donc consommatrice d'énergie – n'évite les risques de concentration, d'entente et de détournement.

A la différence du bitcoin, Ethereum propose des comptes individuels, détenus à travers des clés privées, qui retracent les transactions et les avoirs nets de ses membres et qui permettent de stocker des données de tous types (Ethereum est « Turing complet », c'est-à-dire compatible avec tous les langages informatiques). Le coût de stockage est néanmoins très élevé (« quadratique », il augmente avec le carré de la mémoire que l'on utilise).

La principale différence entre les deux blockchains bitcoin et Ethereum concerne le développement des ***smart contracts*** (leur concept est apparu dès 1994). Sur la première, il est en effet possible de définir des petits programmes informatiques permettant de contrôler l'exécution de certains paramètres associés aux transactions de paiement. Ethereum a particulièrement développé l'usage possible de ces programmes, sous la forme de « contrats intelligents ». C'est un changement considérable de la notion de blockchain puisque celle-ci n'est plus alors seulement un grand registre de transactions mais devient comme un ordinateur, doté de fonctions bien précises, programmables et partageables par les utilisateurs – cet « ordinateur global » qu'Ethereum affirme être.

Un *smart contract* est un programme informatique inséré dans un block qui s'exécute de manière conditionnelle (de type « si-alors ») lorsque certaines conditions prédéfinies sont remplies ou lorsque certains événements se produisent – dans ce dernier cas, cela implique que la blockchain soit alimentée par des informations extérieures. Il faut donc définir l'entité ou source, appelée « Oracle », qui fournira l'information et la déposera sur la blockchain à une adresse préétablie. Quelqu'un peut par exemple choisir de donner tant d'ethers à son frère lorsque ce dernier deviendra père. Cette condition étant définie à travers un *smart contract*, ainsi que la source qui attestera de la paternité, le versement sera automatiquement exécuté lorsque cette paternité sera attestée par débit d'un compte individuel (un « compte de contrat » en l'occurrence, rattaché à un *smart contract* et capable d'être mobilisé automatiquement quand, sur Ethereum, les comptes individuels ne peuvent être utilisés que « manuellement », en utilisant une clé privée). Tout le dispositif repose donc, en termes de confiance et de sécurité, sur la fiabilité de l'Oracle, qui est extérieur à la blockchain. Des sociétés, comme **Oraclize** (Londres, 2015) ont été ainsi créées qui proposent de certifier les données transmises par des Oracles. Les données peuvent également être

validées par consensus, l'information requise étant demandée à un grand nombre de participants, lesquels peuvent être incités à répondre par un système de récompense.

Enfin, la mise en place d'une série de *smart contracts* permet de définir de véritables organisations au fonctionnement automatisé (émission d'actions, distribution de dividendes, …), nommées **DAO** (pour organisation décentralisées autonomes).

En l'état actuel, Ethereum présente d'importantes limites en tant que système informatique. Il est lent (du fait d'un fonctionnement séquentiel ne pouvant traiter qu'une transaction à la fois) et cher comparé à n'importe quel ordinateur courant. Pour ses promoteurs, néanmoins, ces deux défauts sont largement compensés par le niveau inégalé de confiance qu'apporte Ethereum. **On retrouve ainsi toujours le même argument voulant qu'il n'est absolument pas possible de faire confiance à de grandes institutions internationales et qu'il est bien préférable de le faire vis-à-vis d'un système totalement opaque quant à savoir qui peut en modifier les règles et qui en assure réellement le contrôle !** De fait, comme l'a montré la DAO de Slock.it, Ethereum est très loin d'être un système inaltérable et inattaquable.
Quoi qu'il en soit, dans le cadre du présent dossier, il convient de revenir au rôle des crypto-devises et à la création de richesse qu'elles permettent.

*

Le bitcoin, une monnaie comme les autres ?

Le bitcoin est-il une monnaie assimilable aux autres ? Plusieurs institutions financières à travers le monde permettent à leurs clients de gérer leurs avoirs en crypto-devises au sein de leur espace personnel en ligne, depuis Standard Bank jusqu'à USAA, en passant par Barclays ou Fidelity. Des plateformes de trading offrent la possibilité d'acheter ou de

vendre à découvert des bitcoins et les contrats à termes, ainsi que des instruments financiers complexes tels que les CFD, se développent.

Il est possible d'utiliser des cartes bancaires en bitcoin (la startup Paymium et l'établissement Aqoba, en France, semblent avoir été les premiers, dès fin 2012, à le proposer). Il existe des distributeurs/échangeurs automatiques de bitcoins. Le premier a été installé à Vancouver en 2013 et il en existerait près de 1 700 dans le monde aujourd'hui. Et, depuis novembre 2016, les chemins de fer fédéraux suisses proposent même, en liaison avec l'entreprise SweePay, l'achat de bitcoins depuis leurs distributeurs de billets de train. En Suisse, encore, la ville de Zoug, une commune de 26 000 habitants qui ambitionne de devenir un centre de développement des technologies de la blockchain et des crypto-monnaies, est devenue la première ville au monde dont les autorités acceptent d'être réglées en bitcoins.

Cependant, travailler en bitcoin oblige à être prêt à modifier souvent ses prix et à ajuster sa comptabilité. **Parce que leur valeur connait une forte volatilité, les crypto-devises restent difficiles à utiliser dans le cadre de contrats commerciaux**. Toutefois, cette volatilité est largement due à la jeunesse de ces monnaies, dont les modes de fonctionnement ne sont pas encore tout à fait fixés, dont la définition légale et le cadre juridiques restent incertains et qui ont subi d'importantes failles de sécurité imprévues. A terme, on peut imaginer que ces monnaies puissent trouver une stabilité beaucoup plus forte (sans renoncer aux principes qui les

fondent, contrairement à ce que souhaite la Directrice générale du FMI). De fait, plusieurs Etats ont désormais décidé de lancer leur propre crypto-monnaie : le Japon avec le **JCoin**, par exemple. A ce stade, ces démarches, encore tout à fait exploratoires, répondent à des objectifs très différents.

- Le Venezuela tente de développer une nouvelle monnaie indexée sur les richesses du pays et bénéficiant du coefficient de confiance qui demeure attaché à la technologie de la blockchain. Pour ce pays, économiquement étranglé entre une monnaie nationale ne lui permettant pas de régler ses importations et le blocus monétaire créé par les sanctions américaines raréfiant ses revenus en devises, il s'agirait ainsi de pouvoir continuer à entretenir ses relations économiques internationales.

  Dans un contexte économique moins « agité », un objectif semblable est poursuivi par la Banque centrale des Etats d'Afrique de l'Ouest, qui a annoncé travailler à la création d'un **e-CFA**.

- En décembre 2017, la Russie a proposé à ses partenaires des BRICS et de l'Union Economique Eurasienne de financer leurs échanges dans une nouvelle crypto-devise. Il s'agit alors tout à la fois de créer une stabilité monétaire, par référence à une unité de compte unique mais non nationale, favorisant le développement des échanges. Une fonction jusqu'ici remplie essentiellement par le dollar, notamment pour le commerce des matières premières et des hydrocarbures, qui pourrait être remise en cause ou au moins réduite si le projet russe aboutissait.

- L'émirat de Dubaï a lancé l'**emCash**, utilisable dans le cadre des achats courants à travers un portefeuille électronique emPay permettant les paiements en ligne ou sans contact dans les magasins. L'emCash permet des règlements instantanés et il s'agit

ainsi d'amorcer un remplacement de la monnaie papier (facilement négociable sur le marché noir), au profit d'une monnaie électronique bénéficiant, encore une fois, du capital de confiance accordé à la technologie de la blockchain – bien qu'on puisse se demander quelle est l'utilité d'avoir en l'occurrence recours à cette dernière, sur laquelle sont également prév la mise en place d'un système de crowdlending et d'un *credit bureau*.

- Enfin, l'Estonie, a annoncé le lancement de l'**estCoin**, poursuivant, non sans contradiction, le double objectif de mise en place d'une monnaie locale associant les citoyens à sa gestion et son utilisation, ainsi que d'une monnaie d'usage international permettant d'ouvrir son économie – un besoin qui parait surprenant de la part d'un pays membre de la zone Euro ! La Banque Centrale Européenne a marqué son refus de voir apparaitre une telle monnaie.

Sur un aspect déterminant, néanmoins, le bitcoin n'est pas assimilable aux monnaies étatiques : il échappe aux mécanismes de la création monétaire. Le nombre de bitcoins émis et en circulation ne dépend pas du fait qu'ils sont utilisés dans le cadre de transactions commerciales mais a été a priori fixé par un algorithme - à ce titre, le bitcoin est également souvent assimilé à une chaine à la Ponzi mais ce qui est vrai dans son cas ne l'est pas de toutes les crypto-devises, notamment l'ether, soumises à d'autres règles de création.

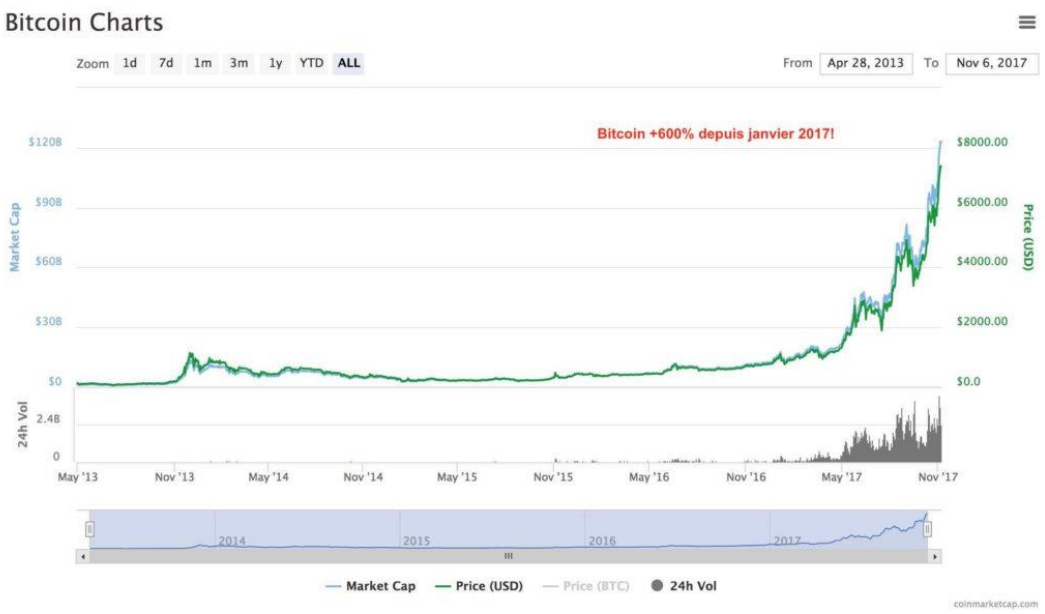
Si les banques accordaient des crédits en bitcoin, au-delà des dépôts en bitcoin qu'elles pourraient recueillir, ces crédits, excédant la masse réelle de bitcoins en circulation, ne seraient pas mobilisables, sans une banque

centrale pour assurer en l'occurrence la liquidité interbancaire en bitcoin. En ceci, le bitcoin ressemble effectivement davantage à un bien qu'à une monnaie : sa valeur est spéculative. C'est une « monnaie-marchandise ». **Il n'acquiert de valeur que par effet de rareté, comme tout bien sur un marché et la création de richesse qu'il permet ne correspond qu'à un effet d'aubaine** – à l'exemple de ce qui est arrivé à la fondation Wikileaks. Les autorités américaines ayant, en 2010, obligé les grandes compagnies de cartes de crédit à refuser toutes les transactions avec elle, la fondation dut se résoudre à accepter les dons en bitcoins pour survivre et à conserver ainsi ses avoirs – ce qui fut pour elle par la suite la source d'un enrichissement, que ses fondateurs étaient bien loin d'avoir imaginé possible !

*

Pour certains observateurs, une défiance croissante vis-à-vis du dollar, du yen ou de l'euro eux-mêmes, liée au fort endettement des Etats, ainsi qu'aux politiques d'assouplissement quantitatif des banques centrales américaines, japonaises et européennes, serait l'une des principales sources des fortes hausses de valeur que le bitcoin a enregistrées ces derniers mois. Comme s'il était devenu une monnaie refuge, au même titre que l'or – dont il a dépassé la valeur de l'once. Après l'annonce du Brexit, le 24 juin 2016, la valeur du bitcoin est montée en flèche, gagnant plus de 9 %, alors que toutes les places financières plongeaient. Le 14 août 2017, le cours du bitcoin dépassait les 4 000 $. Le 12 octobre 2017, son cours atteignait les 5 000 $. Les 6 000 $ étaient franchis dix jours plus tard. En décembre 2017, le bitcoin a, un moment, franchi la barre des 20 000 $. Pour autant, il semble difficile de parler d'un marché élargi au plan mondial. Il concerne prioritairement certains pays. **Près de 80% des transactions sur le bitcoin seraient d'origine chinoise.** A elles seules, les deux principales plateformes chinoises, OkCoin & BTCC, tiendraient

22% du marché. En Corée du Sud, selon une étude récente, 31% des actifs auraient déjà utilisé le bitcoin ou d'autres crypto-devises.



Qu'est-ce qui pourrait menacer cette envolée ? Les observateurs s'accordent à pointer les évolutions réglementaires et fiscales que les Etats pourraient décider. En mars 2014, ainsi, le fisc américain a déclaré que le bitcoin ne pouvait pas être considéré comme une monnaie mais comme un bien, dont les transactions sont soumises à la fiscalité sur les plus-values.

Selon la Banque centrale européenne, la réglementation bancaire et financière qui s'impose aux Etats membres de l'UE ne concerne pas le bitcoin. L'autorité bancaire européenne a ainsi simplement mis en garde les consommateurs contre les risques liés au bitcoin (13 décembre 2013). Elle a également recommandé le 4 juillet 2014 aux institutions bancaires et financières européennes de ne pas utiliser le bitcoin, ni de proposer des services autour de ce dernier. Aux USA, Jamie Dimon, le Président de JP Morgan Chase, a qualifié le bitcoin de « fraude » et a annoncé que si des traders de JP Morgan échangeaient de la crypto-monnaie, « *je les*

licencierais dans la seconde, et ce pour deux raisons : c'est contraire à nos règles et ils sont stupides. Dans les deux cas, c'est dangereux ».

Le 22 octobre 2015, la Cour de justice de l'Union européenne a confirmé que les opérations d'échange de bitcoins contre des devises traditionnelles étaient exonérées de TVA, considérant le bitcoin comme une « devise virtuelle » et non comme un bien ou un service. Mais la France n'a pas encore fixé avec clarté la nature ni le régime juridique du bitcoin. Pour la Direction générale des finances publiques, le bitcoin est considéré comme un bien meuble, la valeur à l'achat ou à la vente et sa valeur en fin d'année fiscale faisant sa valeur légale. Aucun texte n'écarte les transactions en bitcoins des obligations fiscales en vigueur, en particulier en matière d'imposition des bénéfices ou de collecte de la TVA. Cette situation a été rappelée par l'administration fiscale, le 11 juillet 2014. Celle-ci considère que l'acquisition et la cession de bitcoins constituent une activité spéculative soumise à l'impôt sur le revenu, cette activité pouvant être occasionnelle ou régulière. Dans le premier cas, le détenteur de bitcoins est soumis au régime fiscal des bénéfices non-commerciaux (BNC), dans le second au régime fiscal des bénéfices industriels et commerciaux (BIC). Les bitcoins n'étant pas considérés comme des valeurs mobilières, les gains constatés lors de leur cession ne peuvent pas bénéficier des abattements en fonction de la durée de détention. Ils ne pourront pas non plus bénéficier de la «flat tax» à 30 % à partir du 1er janvier 2018.

*

Il reste que **pour tous ceux qui le possédaient sans avoir eu à l'acheter, comme les mineurs, le bitcoin a permis une création de richesse pure** (et non seulement liée à un effet spéculatif de marché comme pour tous ceux qui ont acheté des bitcoins), puisqu'au départ les bitcoins ne valaient rien et ne représentaient qu'une ligne de code informatique.

Certes, tout cela a reposé sur un effet spéculatif, adroitement organisé : il fallait que cette nouvelle monnaie se fasse remarquer, intrigue et séduise, pour qu'on veuille la posséder, en pariant sur sa valorisation future. Et à cet égard, le bitcoin fut une incontestable réussite, surtout si l'on considère qu'il n'a tenu aucune de ses promesses ! Il n'y avait rien de nouveau dans la recherche d'un tel effet spéculatif, sauf qu'il concernait une nouvelle monnaie créée de rien.

Normalement, la valeur d'une monnaie est liée à son usage, donc à la demande dont elle fait l'objet :

Usage = demande = valeur

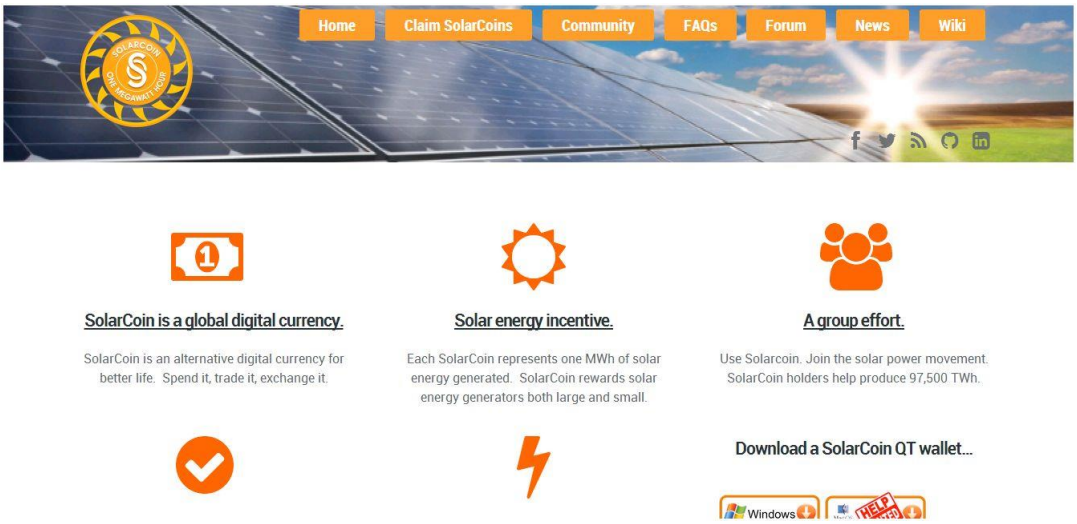
Fondé sur une pure spéculation dès le départ, le bitcoin a bouleversé ce schéma :

Valeur anticipée = demande = usage

Aujourd'hui, les ICO tentent de reproduire ce schéma – très classique – de spéculation pour en tirer profit (et ils y parviennent assez bien). Mais une autre variante du premier schéma peut être imaginée, en partant du fait que puisque la nouvelle monnaie ne vaut rien au départ, on peut largement la distribuer. On n'attend pas qu'une demande se forme ainsi mais l'on compte que l'effet spéculatif va naitre de ce que beaucoup de détenteurs de la nouvelle monnaie vont vouloir qu'elle valle quelque chose pour pouvoir l'utiliser :

Possession = valeur anticipée = usage

Ce nouveau schéma a notamment été élaboré dans le cadre du projet **SolarCoin**, lancé en 2014. Alors que la spéculation demeure le plus souvent vue comme un phénomène irrationnel, comme un dérèglement de marché, **SolarCoin intègre ouvertement une dimension spéculative dans son fonctionnement et l'organise… pour servir le développement durable !**



Pour encourager le développement de l'énergie solaire, la fondation américaine SolarCoin propose en effet de délivrer des SolarCoins par mégawatt-heure produit sous forme photovoltaïque (et faisant l'objet d'une certification). C'est là une réponse originale à un constat simple : si l'on veut encourager l'adoption de certains comportements, il faut distribuer des récompenses, des *rewards*. Seulement cela, qui est assimilable à une subvention ou à une promotion, coûte cher ; très cher si l'on veut promouvoir des comportements à une échelle globale. Mais, si l'on crée une monnaie particulière pour le faire, cela ne coûte rien ! Mieux même, celui qui crée cette monnaie peut même parier qu'en partant de rien il finira par être à même de distribuer des encouragements valant effectivement quelque chose. Le pari peut paraitre insensé. Mais il est également très réfléchi.

Pour me récompenser d'avoir produit de l'énergie solaire, je reçois quelque chose qui, au départ, ne vaut rien. Mais non pas rien du tout, parce que je ne vais pas être le seul à la recevoir. Or, dès lors que nous serons plusieurs à le détenir, nous aurons tous intérêt à ce que ce rien devienne quelque chose que nous serons invités à acquérir et à conserver parce que nous spéculons sur sa valeur future. Le SolarCoin se fonde ainsi sur une production réelle d'énergie et sa valeur sera d'autant

plus forte que plus de personnes, entreprises et particuliers qui produisent de l'énergie, en posséderont. Le SolarCoin ne vaut rien mais en créer ne coûte pratiquement rien non plus, tandis qu'on peut imaginer qu'il acquiert une valeur réelle au cours du temps, ce qui pousse à le conserver et à en obtenir davantage – sur le site de la fondation, des formules sont ainsi déjà proposées pour accepter des dons ou des règlements en SolarCoins.

La Fondation SolarCoin, elle, a décidé qu'elle voulait susciter la production de 97,5 Térawatt-heure d'énergie solaire. Avec 1 mégawatt-heure = 1 SolarCoin, cela correspond donc à 97,5 milliards de SolarCoins ; soit actuellement à 0$ et l'enjeu est de faire que les 97,5 milliards de SolarCoins représentent entre 2 925 et 3 900 milliards de $ d'ici cinq ans. Il s'agit donc d'acquérir 4 000 milliards de $ à partir de rien ! Et pour cela, il suffit d'organiser une spéculation autour du SolarCoin.

Plus de SolarCoins seront en circulation, jusqu'à 97,5 milliards, plus la Fondation réalisera son objectif. Et pour que les SolarCoin soient demandés, il faut qu'ils acquièrent un cours de marché par rapport aux monnaies réelles. Pour cela, il faut donc organiser leur marché et, pour accélérer la création de ce dernier et l'animer au démarrage, il faut organiser une spéculation pure en permettant que des SolarCoins, pour une petite partie, soient acquis sans même que de l'énergie soit produite : 500 millions seront ainsi distribués librement aux fondateurs et promoteurs du projet, tandis que n'importe qui pourra « miner », c'est-à-dire créer des SolarCoins, sur la base d'algorithmes (exactement comme pour les Bitcoins), jusqu'à un total de 105 millions jusqu'en 2040 – mais 95% devront être « minés » les 4 premières années, afin d'accélérer la spéculation. Après, il restera la possibilité d'acheter ou de vendre des SolarCoins à travers une bourse, ainsi que via Twitter. Le but est d'atteindre en cinq ans un cours relativement stable du SolarCoin entre 30 et 40 $. Alors, les SolarCoins récompenseront *véritablement* les producteurs d'énergie solaire, à la hauteur de leur production. Ils pourront

directement financer des échanges et devenir une monnaie. Pour la Fondation, tout cela ne coûtera toujours rien !

En somme, on veut valoriser un comportement et, pour cela 1) on le monétise sous la forme originale d'une nouvelle « monnaie » à laquelle 2) on tente de donner une valeur à travers une spéculation, comme s'il s'agissait d'un phénomène normal, souhaitable. Pour une fondation poursuivant un but d'intérêt général, la démarche est stupéfiante, tant par son ambition et la hauteur des chiffres visés que par l'originalité des moyens mis en œuvre. Alors qu'en France la plupart des projets de monnaies locales sont encore tout empreints d'une idéologie digne des utopies socialistes du début du XIX° siècle (recréer un monde sans argent, sans banques, sans spéculation), la Fondation écologiste SolarCoin n'hésite pas à s'inscrire sous une logique résolument spéculative pour atteindre ses buts.

Certes, les risques de non aboutissement d'un tel projet sont élevés : risques que la formule ne prenne pas, n'intéresse pas ou risques, au contraire, qu'une spéculation débridée, se traduisant par une très forte volatilité, ne l'étouffe. Le SolarCoin n'aura été alors qu'un objet monétaire non identifié, un composé hybride et non viable. La démarche n'en reste pas moins digne d'être signalée car, si elle réussit, elle représentera une innovation monétaire majeure, aux prolongements potentiels vertigineux. Une innovation qui, dès aujourd'hui, montre sous quel angle les crypto-monnaies pourraient peut-être acquérir une dimension économique déterminante. Soit en acquérant une valeur par elles-mêmes, comme c'est le cas du bitcoin, soit en devenant des monnaies complémentaires, c'est-à-dire en créant un surplus de richesse monétaire en valorisant une activité qui n'en génère pas en elle-même directement. C'est par exemple le cas, avec le Compte CO2.

Il a été créé en 2013 par la startup brestoise 450. L'idée du Compte CO2 est simple. Vous faites une économie en termes de consommation

énergétique. Vous réduisez votre propre émission de gaz à effet de serre. Cette économie est matérialisée sur un compte en ligne dans une unité, les « CO2 », qui sont inscrits sur le compte. Et l'idée est de se servir de ces CO2 comme d'une unité monétaire, pour régler certaines charges ou dépenses, auprès d'acteurs qui les acceptent.

Exemple : vous chauffez votre maison au fioul et vous émettez ainsi 7 000 kg de gaz carbonique par an. Vous passez à une chaudière en bois. Vous inscrivez sur le Compte CO2 l'économie réalisée : + 7 000. Or, pour les commerces qui acceptent d'être payés en CO2, 1 000 CO2 valent 50 €. Vous avez ainsi épargné 7 x 50 € = 350 €. Avec lesquels vous pouvez acheter un billet de train, puisque ID TGV accepte les CO2 (Amzair Industrie, spécialiste des pompes à chaleur, et Europcar les acceptent également).

Sous ces perspectives, l'idée est de rendre accessible à tous le marché des émissions de gaz carbonique, à travers un compte d'épargne que l'on n'alimente pas avec de l'argent mais avec les économies énergétiques que l'on réalise. Et, pour cela, le Crédit Mutuel Arkéa a pris en charge la gestion du Compte CO2, auquel une carte de paiement peut être associée et il a défini, à travers sa filiale de crédit à la consommation Financo, un

prêt finançant l'acquisition d'équipements écoresponsables dont les frais de dossiers peuvent être remboursés en CO2.

Il est intéressant de comparer le Compte CO2 à SolarCoin, strictement similaire dans le principe. Mais dans son principe seulement car, s'inspirant du modèle du bitcoin, SolarCoin joue de manière audacieuse sur un effet de marché et organise délibérément la spéculation autour des unités monétaires qu'elle crée : les SolarCoins. D'inspiration plus française, diront certains, le Compte CO2 a choisi une démarche beaucoup plus… administrative. Au démarrage, il faut réaliser un bilan énergétique de son logement et de ses moyens de transport, avec les justificatifs correspondants. Et il faut renouveler l'évaluation chaque année, sur la base de nouveaux éléments. Cela peut paraitre un peu contraignant, d'autant que les gains – c'est la grande différence avec SolarCoin – paraissent quand même potentiellement assez limités. Chaque Français émet en moyenne neuf tonnes de gaz carbonique par an. Réduire ce volume n'est pas gratuit et cela ne permet de gagner, une seule fois, que 450 € sur un Compte CO2. On pourrait bien entendu augmenter la valeur faciale des CO2 mais c'est le caractère faiblement récurrent des économies que l'on peut réaliser qui parait le plus gênant.

De sorte que, malheureusement, le Compte CO2 n'a rencontré, malgré d'intéressants appuis, qu'un succès d'estime (12 000 ménages l'ont adopté, ainsi qu'une trentaine d'entreprises). Un succès qui n'est certainement pas à la hauteur de l'ambition et de la pertinence de la démarche.

On pourrait considérer en effet que le Compte CO2 puisse être élargi à bien d'autres actions responsables, que sa formule paraît particulièrement intéressante pour responsabiliser les particuliers, qu'il offre à ces derniers une toute autre manière de gérer leur propre mode de vie et qu'il est à même de créer un écosystème vertueux, associant des acteurs très divers. Par ailleurs, initiative tout à fait privée, gérée à une échelle individuelle, le Compte CO2 rencontre les efforts, notamment en termes de défiscalisation, que l'Etat engage en matière de comportements écoresponsables. Pour la puissance publique, il est en fait doublement intéressant : il est incitatif et il décharge en partie l'administration des tâches de gestion. De sorte que l'Etat pourrait très bien accepter que les CO2 puissent être utilisés pour payer ses impôts ! Cela leur donnerait une large assise, ce qui permettrait d'en élargir la formule, laquelle parait aujourd'hui trop limitée.

Mais il y a plus car le compte CO2 s'inscrit dans l'économie des quotas de gaz carbonique échangeables, définie dans le cadre du Protocole de Kyoto. La startup bretonne a d'ailleurs choisi de s'appeler « 450 » en référence à la limite des 450 ppm de CO2 fixée par le GIEC, comme seuil à ne pas dépasser pour limiter le réchauffement climatique à 2° C. Le compte CO2 permet aux particuliers de revendre leurs CO2 à des entreprises qui compenseront ainsi leurs propres émissions. Il s'appuie sur la formation d'un véritable circuit d'échange quand SolarCoin veut organiser une spéculation comme à partir de rien. Certes, le bitcoin y est parvenu mais nimbé de tout un mystère savamment organisé et en

promettant des opportunités toutes nouvelles d'évasion monétaire et fiscale.

Au total, **un schéma de création monétaire se dégage à travers l'invention de monnaies privées, n'ayant pas vocation à remplacer les monnaies existantes mais à accompagner la réalisation de projets ou à défendre un certain type d'engagements : organiser la valorisation d'échanges non monétarisés à travers une monnaie nouvelle dont une certaine dimension spéculative pourrait être délibérément favorisée, pour accélérer la réalisation d'un projet ou renforcer des engagements**.

*

Et demain ? Quelle évolution possible pour les crypto-devises ?

Deux exemples permettent de l'envisager.

Secco (Londres, 2015) n'est pas seulement une néobanque anglaise de plus mais **la plus disruptive des néobanques**. Une banque sans agences – ce qui est désormais banal – mais également sans appli mobile ni même un canal de contact. Une banque qui promet de réinventer la notion même d'argent mais qui en manque visiblement cruellement pour démarrer.

Le concept de Secco reste difficile à décrire précisément. Vous vous promenez avec une application nommée Aura et vous localisez votre avatar sur un plan, ainsi que ceux des autres personnes qui utilisent Aura dans un périmètre de 60 mètres autour de vous. Vous pouvez ainsi voir qui sont ces personnes, ce qu'elles font et de quels « tokens » elles disposent.

Par exemple, une personne porte un blouson Burberry et un token signale que vous pouvez l'acheter. Et Burberry peut intervenir dans la transaction, gratifier le vendeur et l'inviter à faire une réduction à l'acheteur. Dans un cocktail, à travers leurs tokens, vous pouvez savoir qui est qui. Plus besoin de cartes de visite. Tous les tokens et tous les échanges sont stockés et géré à travers une blockchain, nommée « Blocktree ».

Chacun crée donc des tokens le concernant et se valorise ainsi – c'est tout l'enjeu derrière Secco. Car ces tokens peuvent servir de monnaie d'échange et le but est que chacun devienne vendeur de ses propres données, de tout ce qui en lui peut intéresser les autres, en même temps qu'émetteur de monnaie – *the Bank Of Ourselves*. « *Secco wants its users to become 'data brokers' – treating their data as a currency to spend, lend and invest.* » Car on peut s'échanger des tokens – pour remercier d'un geste, d'un moment, exactement comme un *like* sur Facebook. Et ces tokens peuvent servir de coupons valant services ou réductions. Bref, il s'agit là d'une véritable monnaie.

Tout cela ne semble pas très clair mais il est difficile d'en savoir plus. Pour le moment, Secco n'a réalisé qu'une version alpha d'Aura.

Parmi ses fondateurs, il y a Chris Gledhill, souvent cité parmi les principaux influenceurs en matière de fintech. Il n'est donc pas très surprenant de retrouver chez Secco beaucoup de choses qui évoquent tout à la fois Pokemon Go, Facebook, le bitcoin et des crypto-monnaies comme SocialCoin, les développements sur blockchain et des démarches

comme celle de Digi.me, etc. Il ne manque que l'IA mais, à ce compte, il est probable qu'elle apparaitra !

Seulement, Secco n'est pas seulement un patchwork opportuniste. Derrière le projet, l'ambition est énorme. La monnaie ne sert qu'à acheter des biens « réels ». Et si l'on concevait un système d'échange beaucoup plus large, au sein duquel chacun pourrait émettre une sorte d'instrument d'échange fondé sur ce qu'il a à proposer, sur ses qualités propres dans le jeu social et non seulement sur ce qu'il a à vendre ? Sur ce qu'il apprécie et non seulement sur ce qu'il possède ? Alors Secco deviendrait notre premier support de vie sociale. Il ne remplacerait pas tant les échanges et les monnaies qu'il ne les absorberait : « *Secco will operate as an 'underlying' service hidden in all the apps and social platforms we use day-to-day.* » Une idée complètement folle sans doute. Pourtant, s'il ne la rend pas, reconnaissons-le, concrète, Secco fournit comme un premier tremplin pour l'imaginer. Et cela le conduit à adopter un positionnement radicalement décalé par rapport aux banques. Non pas entrer en concurrence avec elles mais s'efforcer d'être autre chose, passer à un concept totalement nouveau pour, à terme, les remplacer.

Sur de telles bases, Secco parviendra-t-il à attirer des investisseurs ? Pourquoi pas ? Certes, à ce stade, son modèle parait encore très incertain. Sur les forums et dans la presse, toutefois, les réactions sont positives (comme à chaque fois qu'on promet un monde sans banques !). Et ce ne serait certainement pas la première fois qu'une invention – nous sommes ici un cran plus loin que l'innovation – serait née d'une approximation.

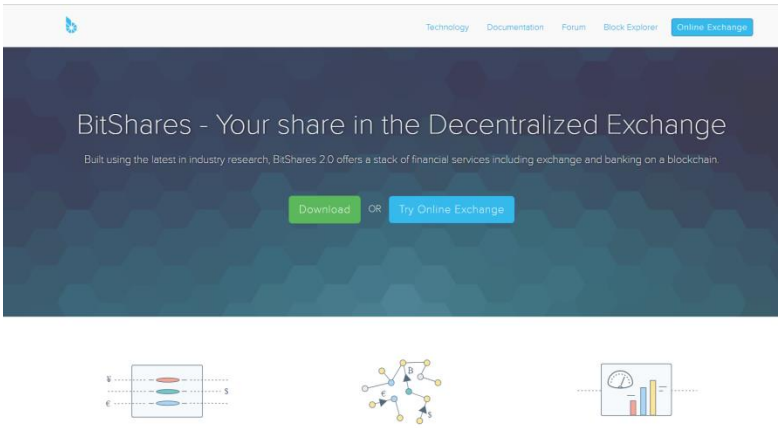
A travers Secco apparait un monde où tout serait échangeable à travers des jetons. Tout, depuis les cartes de visites jusqu'aux biens immobiliers pourrait ainsi passer de mains en mains à travers une appli, une blockchain, donc sans intermédiaire.

Secco apparait ainsi comme une plateforme d'échange globale, utile pour la quasi-totalité des moments de la vie sociale. Mais le modèle parait à ce stade bien trop court et inabouti. Tout d'abord, sous ses configurations existantes, la blockchain ne parait guère adaptée à un système de ce genre, s'il se développait. Ensuite, Secco manque d'une monnaie, c'est-à-dire tout à la fois d'une unité de compte pour que les échanges dépassent, même à travers des tokens numériques, un simple système de troc. Et Secco raisonne en termes trop monétaristes : neutre, la monnaie utilisée sert les échanges, elle n'est pas possédée pour elle-même, pour sa valeur propre. Deux dimensions manquantes qu'introduit en revanche BitShares.

*

Lancé en 2013 à Blacksburg (Virginie), **BitShares** a été créé par Daniel Larimer, un vétéran du bitcoin et Charles Hoskinson, un vétéran d'Ethereum, avec le soutien financier d'un magnat chinois très investi dans les monnaies digitales, Li XIalai.

Bitshares est une plateforme d'échange universelle, capable, est-il affirmé, de traiter 100 000 transactions par seconde (par comparaison, les systèmes de Visa ne dépassent pas les 24 000 transactions par seconde). La plateforme possède sa monnaie propre, les BitShares (BTS) et est gérée à travers un système de *Proof-of-Stake* particulier : 101 mineurs sont élus par les participants (le poids des votes est à proportion du nombre de BTS possédés) et rémunérés en BTS. C'est donc une plateforme d'échange décentralisée, sans intermédiaire et sur laquelle les transactions sont anonymes.



Sur la plateforme, on échange, en BTS, des tokens, comme avec Secco. Ils représentent des parts de société ou des biens et actifs réels. Mais on peut également lier des tokens à des valeurs de marché (*market pegged*

assets). Les tokens se nomment alors des **SmartCoins**. On peut par exemple échanger des SmartCoins valorisés par des dollars ou des actions Apple à un certain cours ou de l'or, etc. On n'échange pas des dollars alors mais des **bit$** dont la contrevaleur est, par exemple, de 1 $. Et les échanges ont lieu en BTS – une sorte de monnaie universelle, en laquelle peuvent être converties toutes les autres, ainsi que la valeur de tous ce qui peut être échangé. Sachant que la plateforme permet de spéculer sur la valeur future des BTS.

Bien entendu, deux obstacles peuvent contrarier le développement d'une plateforme de ce type : que valent exactement les BTS ? Par ailleurs, ne peut-on se retrouver « coller » en achetant des tokens qu'on ne pourra revendre sur la plateforme, si celle-ci rallie peu d'investisseurs ? Les SmartCoins ont précisément été inventés pour assurer les acquéreurs de BTS qu'ils pourront retrouver au moins leur mise de départ, par exemple en $. Le second problème de liquidité est résolu à travers un dispositif particulier. Les SmartCoins se vendent à un certain *price feed* en BTS, déterminé par le consensus des mineurs et à découvert (position *short*) : le vendeur ou « *shorteur* » devra acheter les mêmes SmartCoins avant un certain délai – l'acheteur est ainsi certain qu'il trouvera au moins un acheteur s'il décide de vendre dans ce délai. Par ailleurs, pour être sûr que le shorteur achètera les SmartCoins, il lui est demandé de mettre sous séquestre un collateral en BTS représentant 200% du montant de sa vente, qu'il ne récupérera qu'une fois celle-ci réalisée. Et si, au cours de délai courus, la valeur des BTS se déprécie par rapport à celle de référence (le $ dans cet exemple) en-deçà d'un seuil, la vente sera réalisée immédiatement en mobilisant les BTS mis en garantis. L'acheteur pourra ainsi être remboursé, s'il le souhaite, à une parité de marché BTS/$ qui l'assure de pouvoir au moins retrouver sa mise de départ en $. Par ailleurs, dans ce dispositif, le vendeur parie sur une appréciation des BTS qui lui permettra d'acheter les SmartCoins moins chers qu'il ne les vendu.

Au total, on peut sans risque échanger ce que l'on veut. BitShares est comme **une bourse universelle** – les artistes peuvent à travers elle commercialiser leurs œuvres, par exemple.

Si elle réussit à s'imposer, la plateforme BitShares devra certainement évoluer : assez contraignant, le dispositif de garantie de liquidité qui vient d'être présenté peut intéresser les investisseurs en phase de démarrage. Il n'aurait pas nécessairement vocation à s'imposer de manière générale si la plateforme se développait à une large échelle. Par ailleurs, dans ce dernier cas, le modèle d'une gestion décentralisée deviendrait impossible à suivre du fait de la taille de la base de données que les nœuds devraient stocker sur leurs appareils. Quoi qu'il en soit, BitShares répond assez bien finalement à ce qu'a pu annoncer la Directrice du FMI. **Bitshares représente-t-il dès aujourd'hui ce que deviendra la monnaie demain ?**