Que penser des nouvelles monnaies virtuelles utilisant la technique du blockchain ou du registre distribué ? (Ex : le bitcoin)

Tout le monde a probablement entendu parler d'une nouvelle monnaie virtuelle et largement « hors la loi » nommée « Bitcoin ». Il s'agit effectivement d'une autre race de monnaies parallèles que celle qui éclot dans nos milieux alternatifs populaires. Il ne s'agit pas du fruit d'une problématique de refondation du lien social en commençant par une échelle locale. Il s'agit d'une problématique d'invention de solutions technologiques potentiellement universelles (*utilisant le croisement des technologies les plus avancées dans plusieurs domaines de la numérisation et de la communication*) pour voir à quel point le « lien virtuel de pair à pair » peut produire des solutions lucratives fiables pour beaucoup de problèmes de coordination qui butent encore, d'une part sur l'aveuglement de l'horizon individuel, et d'autre part sur le carcan d'une règlementation publique impossible à universaliser…

Il n'est pas étonnant que cette « double crise » serve de terrain de jeu préféré pour les petits génies de la « silicon valley » toujours à mi-chemin entre l'escroquerie et le renversement du paradigme…

C'est ainsi que le bitcoin est une expérience -et une contr'expérience- monétaire, virtuelle, parallèle, à la fois « réussie » (*à sa façon*), limitée en tant que telle, potentiellement révolutionnaire au niveau de perspectives multiples qu'elle semble ouvrir, potentiellement porteuse de « vraies » et aussi de « fausses » solutions (*voire d'impasses*) en cas de généralisations à très grande échelle…

Pour la décrire en quelques points il faut repartir de la question de base de la monnaie qui est celle du degré de confiance que l'on peut avoir dans les signes de créances que l'on peut accepter en contrepartie d'un bien ou d'un service que l'on fournit à un inconnu. Les monnaies « modernes » *(avant le bitcoin)* mobilisent à la fois une garantie « verticale » (*qui engage la puissance publique*) ou « principe de centralisation » et une garantie horizontale (*qui fait jouer à fond la « libre concurrence » entre agents bien informés des risques relatifs pris par les uns et les autres*) ou « principe de fractionnement ». Hélas, ces deux garanties ont montré leurs limites à l'occasion des multiples crises monétaires et financières, et notamment des dernières… D'où l'idée d'une solution technologique qui puisse, à la fois, assurer la transparence de toutes les opérations, et certifier la valeur en garantissant le plus strict parallélisme entre « flux réels » et « flux d'avoirs en signes monétaires », le tout sans contrôle central mais avec un contrôle partagé de l'historique (*registre*) des échanges dans tous les nœuds du réseau de la communauté des transacteurs-usagers…

Il y a certainement plusieurs façons de concevoir une monnaie sûre sur cette base, selon que l'on pense en termes ouverts ou fermés, intéressés ou désintéressés, strictement privé ou partiellement public, etc., etc. … Le bitcoin a mis le maximum de chance du côté du « bon coup pour ses promoteurs » en choisissant -*dès son lancement*- un système strictement privé, et strictement fermé à terme. Il est conçu pour prendre une ampleur délimitée selon une courbe de croissance qui ne devrait poser aucun problème technologique particulier.

Son idée est donc de partir d'une valeur un peu arbitraire (*ex : 1 bitcoin = 1 dollar au départ*) pour ce nouveau signe monétaire acceptable en paiement d'un produit et donc cumulable sur le compte d'un vendeur de bien ou service. Les premiers titulaires de bitcoins sont les premiers propriétaires du dispositif de gestion en réseau. En effet, ce dispositif technique est la première contrepartie réelle et fondatrice de la valeur du bitcoin, de la même façon que la réserve en or fut la première contrepartie réelle du billet vert par exemple. Au début, le réseau est étroit donc peu de bitcoins sont créés. Ensuite il y a un lien permanent entre la masse de bitcoins en circulation et la taille et performance du réseau des usagers. Cependant si la valeur de chaque bitcoin est appelée à varier, ce n'est pas en fonction de la taille et qualité du réseau puisqu'il n'est pas destiné à être vendu. Le bitcoin a été conçu pour prendre de la valeur en étant de plus en plus demandé pour ce qu'il permet de vendre et d'acheter, alors que son offre est limitée par construction. Ainsi, le pouvoir d'achat de ces avoirs en signes monétaires a été conçu pour avoir plus de chance de progresser que de régresser pendant toute la période de développement (*de zéro à 21 millions*) de cette « masse monétaire » (*total des avoirs détenus en bitcoins par l'ensemble des transacteurs-usagers*)…

On devine au passage que si tous les usagers sont appelés à « y gagner », ceux qui sont partis les premiers dans cette communauté d'échanges devraient être ceux qui y gagne le plus, … *abstraction faite des gains d'usagers mafieux qui se préoccupent moins de gagner sur la valeur des avoirs en bitcoins que de l'opportunité de réaliser des transactions cachées car hors la loi d'une façon ou d'une autre*…

Il faut encore préciser trois points-clés :

- comment marche -dans la durée- la garantie de valeur (*contrepartie*) de chacun des flux et des stocks de bitcoins ? Chaque transaction nouvelle est inscrite en temps réel dans un registre partagé par tous les usagers. Ainsi, il n'existe pas de transaction dont l'équivalence historique n'ait pas été admise et reconnue par les contractants n'ayant aucun intérêt commun à fausser la balance. Au bout du compte la communauté des contractants valide à chaque nouvel achat non seulement la valeur du transfert d'avoir en bitcoins mais aussi la valeur de tout l'historique des transferts réels et monétaire qui ont permis d'en arriver là.

- comment et pour qui crée-t-on de nouveaux bitcoins, et en même temps une extension de la valeur commune réelle du réseau des usagers de bitcoins ? Le réseau s'étend et s'approfondit au fur et à mesure que le registre grossit. Mais pour que ce registre soit indestructible il faut qu'il soit fractionné, dispersé et toujours recomposable car virtuellement stocké dans un grand nombre de nœuds du réseau. Il est stocké et circule en plusieurs blocks (« *blockchains* ») certifiés et vérifiés, au moins six fois chacun, sur six nœuds indépendants. Pour cela, les usagers disposant des plus grosses puissances de calcul peuvent se porter volontaires pour participer à la confection et/ou à la certification d'un nouveau block. Et ce « travail » mérite une rémunération. Il est payé par un tarif en bitcoins, qui est d'ailleurs dégressif pour que cette création s'épuise d'elle-même à l'approche des 21 millions de bitcoins.

Au passage, il est intéressant de noter la poursuite de l'analogie entre le réseau organisé (*nouveau*) et la mine d'or (*antique*) comme fondement historique de la valeur du

signe monétaire. C'est d'ailleurs pour cela qu'on nomme « mining » l'activité de production des blockchains qui étendent à la fois le nombre des bitcoins émis et la capacité de gestion du réseau.
On note aussi que l'activité dite « mining » repose très peu sur le mérite d'un « travail » d'individu mais beaucoup sur la rente de situation des usagers disposant à la fois de l'accès aux bitcoins et de fortes puissances de calculs dédiés, ce qui marche un peu en boucle… Sur ce point aussi, cette forme de monnaie privée s'avèrera probablement très contestable … mais cette caractéristique est amendable…

- est-ce la seule façon de se procurer des bitcoins ? Non, bien sûr, si on n'a pas « gagné » de nouveaux bitcoins par « mining » on peut toujours acheter des bitcoins déjà en circulation en les payant en dollars ou euros, etc. à des titulaires de comptes estimant que c'est une bonne affaire. Cette monnaie est donc spéculative car sa valeur au jour le jour dépend du degré de préférence « des agents » par rapport aux monnaies « concurrentes ». Et d'ailleurs certaines banques participent aux transactions de change de monnaies traditionnelles en bitcoins, voire vice-versa.

Au passage, on voit que le bitcoin est à la fois une monnaie « plus complète » que nos monnaies « complémentaires » et incomplète cependant.
* plus complète car sa valeur ou son taux de change n'est pas fixe il dépend du marché des monnaies qui mesure les confiances relatives que l'on accorde à chacune pour conserver plus ou moins bien le pouvoir d'achat des agents…
* mais incomplète tant que la création de nouveaux bitcoins ne se fait pas à l'occasion de crédits ou avances monétaires en bitcoins car le système de garantie n'est pas mûr pour aller jusque là…

Cette technologie des blockchains est apparue comme une forme de solution pour créer une monnaie parallèle… mais sans doute pas « la » monnaie de demain. Son utilisation dans l'aventure des bitcoins montre à la fois une avancée et un repoussoir par rapport à ce qu'on pourrait en faire pour remette la monnaie et la finance sous contrôle citoyen. On reste très loin du meilleur qu'on puisse en tirer, et hélas on voit davantage les puissances prédatrices que les activistes humanistes à la manœuvre pour les prochaines aventures dans ce domaine…

Cette technologie des blockchains a, de toute façon, un avenir important dans tous les domaines qui nécessitent une certification des échanges, assez simple et rapide, et qui fasse autorité. Les applications seront multiples…

Cette technologie est donc beaucoup plus qu'une mode et bien moins qu'une panacée. En tous cas c'est un nouvel objet de réflexion et de développements sur lequel les citoyens ne doivent pas prendre un train de retard sur les investisseurs qui sont déjà en train de voir comment « tordre » les algorithmes pour « *replateformiser la déplateformisation d'une économie de partage dévoyée par la première vague de plateformisation qu'on a nommée l'ubérisation* »…
Cette formulation très abstraite et hyper-synthétique nécessitera bien sûr une explication orale en plusieurs étapes…

En tous cas c'est une bataille trop sérieuse pour la laisser sous le contrôle des seuls « investisseurs ». Les citoyens demandeurs de «transition » doivent y faire valoir leurs exigences de contrôle car une économie de partage de communs est plus que jamais accessible. Mais en même temps, la question du contrôle monétaire est en proie à la l'imagination lucrative des puissants, par tous les moyens, qu'ils soient légaux ou seulement impunis…

Le bitcoin, comme moyen et système de transactions privées et sécurisées est un dispositif de monnaie parallèle mais pas le seul possible. Heureusement car il nous inspire bien plus de réticences que d'attraction. Mais cette expérience peut en inspirer d'autres, à vocation plus « révolutionnaire ». Sa conception en a fait, aujourd'hui, une monnaie spéculative qui remplit des fonctions principalement parasites par rapport à ce qui aurait pu être une recherche sérieuse d'alternatives monétaires d'inspiration citoyenne ou d'inspiration publique à un niveau national ou supranational.

Cette expérience est donc soumise à notre observation critique pour éclairer le meilleur ou le pire dans les avenirs possibles des monnaies de demain (*des plus ignobles jusqu'aux plus nobles*). A ce jour, les perspectives les moins vertueuses semblent plus probables. Le chemin est étroit si l'on veut s'en inspirer pour re-stabiliser un système fractal de monnaies imbriquées du local au global …

Au point où nous en sommes de ces expérimentions, une question se pose aux citoyens : « Pouvons-nous n'être que des spectateurs de la bataille des monnaies parallèles virtuelles qui risque de produire plus de changements (*pour le meilleur ou pour le pire*) que nos petites expériences de monnaies complémentaires locales, qui ont bien du mal à accélérer la transition espérée ?

A ce jour, il semble que des généralisations à très grande échelle de cette innovation pourraient se heurter à de graves limites (*vitesse de progression des puissances de calcul et des économies d'énergie pour mettre en œuvre une accélération totalement déraisonnable des consommations de données partagées*)… Mais difficile de dire où peut encore se situer une sorte d'équilibre compatible avec les principes de sobriété énergétique qui devraient aujourd'hui s'imposer en amont de tout projet innovant. Hélas le « principe de précaution » n'est pas celui qui va guider le monde dans cette affaire…

On peut déjà s'inquiéter de voir que les maîtres du crédit, de la monnaie, et de la finance sont les premiers sur les rangs pour « domestiquer » ces innovations. Ils veulent en faire un argument de plus pour se dispenser de la supervision de Etats. Ils veulent s'approprier les clés de systèmes de transactions hors contrôles institutionnels et maîtriser aussi ses failles car le mieux pour les puissants est encore de disposer d'entrées opaques dans un système qui a l'air transparent…