

## Journée Blockchain/Bitcoin

### Les usages Monétaires : caractéristiques nécessaires d'un étalon.

#### 1. La nécessité d'un étalon

On pourrait très bien admettre que sur une plate-forme d'échange on puisse tout échanger avec des ratios. Le nombre servirait d'étalon car, système de classement, (voir Einstein « Le monde tel que le vois » - « Mein Weltbild ») le ratio qui en résulterait déterminerait une valeur. L'exemple serait qu'on échange une poule contre 40 œufs. Toutefois, on doit admettre que cela supposerait que toutes les plateformes, pour les soldes dégagés, soient reliées avec un ratio d'échange. A défaut, ce solde qui doit être considéré par le titulaire, ne serait pas comme « as good as money ». Il refusera d'opérer la transaction si lorsqu'elle est envisagée elle lui laisse un solde « sans valeur ». Surtout, la question du sort des soldes serait posée si les ratios ne peuvent entraîner une compensation. Pour éviter cette muraille il faudrait qu'une plateforme, telle par exemple celle d'AMAZON, devienne à objet universel. On peut tout y trouver et on peut tout y acheter et échanger. Mais alors on fera face à l'obstacle de la domination du marché par un seul acteur dont on sait par des exemples historiques vers quels errements elle peut conduire.

Le rôle d'intermédiation de la monnaie qui libère son détenteur de choix obligatoires puisqu'il peut aller d'une offre à une autre serait bafoué.

Cette hypothèse se heurte aussi pour le moment à des règles spécifiques à certains types d'échanges comme les acquisitions immobilières. Elle se heurte aussi aux différentes souverainetés monétaires qui veulent que certaines transactions ne puissent être menées que dans la devise de résidence d'une des parties ou des deux. En outre, même en supposant une formule pour arrondir les soldes, le seul ratio ne rend pas compte du temps qui fait que la valeur va varier selon des cycles différents pour les biens ou animaux échangés. La poule durera plus longtemps que les œufs. De fait implicitement, le solde ne sera accepté que s'il lui est attribué une valeur d'échange qui a défaut d'étalon monétaire sera la capacité de la plateforme à établir que le solde sera échangeable dans l'avenir contre d'autres nombres valorisant les biens mis à l'échange. Plus fondamentalement, les cycles d'échange étant différents selon les acteurs un solde est nécessaire. Ainsi, par exemple le constructeur automobile vend les voitures qu'il produit chaque jour tandis que l'acheteur n'en achète que d'une manière discontinue et étalée dans le temps. Il faut donc à ce dernier une capacité de stockage de valeur pour procéder à ce genre d'achat. De la même manière, « la répartition » nécessaire à la vie sociale d'aujourd'hui implique qu'une réserve soit faite au profit des retraités ou au profit des enfants pour leur éducation. S'agissant de droits à satisfaire dans le temps il faut pour en prélever la valeur à certains pour l'attribuer à d'autres ou encore accepter l'épargne de certains, un étalon pouvant permettre de déterminer les pouvoirs associés. A défaut, vous n'accepteriez jamais de cotiser sur votre salaire ou même que votre employeur cotise pour vous afin, de vous servir une retraite dont vous ne sauriez pas quel genre de niveau de vie elle pourra vous permettre le moment venu. L'étalon est donc nécessaire, non seulement pour les besoins de visibilité des droits à répartition, mais aussi pour qu'ils puissent être modulés selon les besoins. Pour assurer ce qui est désigné d'une manière classique comme la fonction de réserve de la monnaie un étalon doit lui être associé pour rendre compte de la dimension « temps »

## **2. Les caractéristiques nécessaires d'un étalon a) La stabilité**

Evidemment, les cycles auxquels sont soumis notre production comme notre consommation et notre mode de vie sont de durée variable comme la vie des biens que nous consommons. Pour cette raison, et pour assurer la transparence nécessaire à la confiance dont une économie a besoin, la l'étalon doit être stable. A cet égard la volatilité de la valeur de l'étalon a un effet distributif car dès qu'il a été associé pour sa mesure à un bien, il en donne une valeur. Toute créance étant aussi une dette pour sa contrepartie. Changer la valeur de l'étalon a pour effet de modifier les droits à terme de chacune des parties, débitrice comme créditrice. En période d'inflation le détenteur de revenus fixes la subit. En revanche, le débiteur profite d'une répartition accrue. L'émetteur de monnaie le sait aussi puisque les émissions changeant les volumes monétaires disponibles vont faire varier la répartition des biens si leur disponibilité n'est pas homothétique.

Une forte volatilité intrinsèque de l'étalon serait intolérable puisque dès lors qu'il devient vivant par son association à un support, un tel phénomène sans loi, devient redistributif. Cette redistribution essentielle à notre fonctionnement sociétal sans logique et surtout sans contrôle démocratique est à proscrire. Il détruit le fonctionnement de l'économie de marché puisqu'il va agir sur le prix des échanges sans regard direct sur le service ou le bien échangé, son utilité, sa rareté ou son coût. Le retraité devient plus riche ou plus pauvre sans logique comportementale et sans raison susceptible d'emporter son adhésion ou celle des autres agents économiques qui seraient privés de valeurs. C'est aussi le problème des guerres monétaires ou chacun fait baisser sa monnaie pour favoriser sa production intérieure au détriment de ses concurrents. Les mécanismes qui fixent les prix et l'allocation des ressources ne fonctionnent plus. Les marchés sont indument perturbés.

### **b) l'Universalité**

Tout d'abord qu'est-ce qu'ici l'universalité ? Il s'agit non seulement d'une réalité physique de l'étalon mais aussi comme toujours en matière monétaire d'une reconnaissance facile donc partageable par les usagers potentiels

L'étalon a toujours historiquement été de nature physique car en ayant cette caractéristique, il transcende l'être humain. C'est la vitesse de la lumière, c'est la molécule d'or ou d'argent. L'être humain ne peut en violer les caractéristiques et elles servent de repères. Il est neutre par rapport aux acteurs et donc ce sont les prix qui varient et non l'étalon.

La molécule répond au besoin d'universalité aussi nécessaire à un étalon car quel que soit l'observant, elle est unique.

S'agissant d'une molécule, bien tangible d'abord perceptible (on sait reconnaître l'or et nos ancêtres grecs en supposait déjà l'existence) , elle est échangeable en tant que telle par sa définition et son poids, les mêmes pour chaque observateur ou acteur. J'ai coutume de dire que la première union monétaire a été réalisée par l'émission en Lydie de pièces d'or (5<sup>ème</sup> siècle A.C.).

A l'égard d'un cryptogramme, si son universalité peut être assurée, il peut manquer de transparence pour certains. Il s'agit probablement seulement d'une question de générations. A défaut de transparence, des phénomènes de rejet des unes par les autres pourraient se produire. Il y a un sujet éducatif malgré celui de l'émerveillement quant à la praticité qui lui poussera à l'universalité par l'attraction qu'il générera et « l'autorité » que confère l'universalité comme l'autorité que cette dernière confère et qui rapproche du mystique. Nous voyons là encore une fois le rapport des mathématiques avec le social et ses frontières indéceses. Il implique études et flexibilité au contexte des sociétés

### **c) La Praticité et l'inviolabilité**

Evidemment, si du fait de sa disponibilité de sa rareté, et de sa faible corrosion l'or est à la fois un étalon et un support idéal. Il peut exister encore mieux comme étalon au plan de son transport et de sa comptabilisation c'est-à-dire de son stockage.

Le mieux c'est le cryptogramme. Bien sûr, le cryptogramme, n'a pas de poids et est digital. Il a toutefois aussi besoin d'être aussi inviolable que la définition d'une molécule. Quel cryptogramme aura cette caractéristique et comment l'assurer. Est-ce le cas des monnaies digitales actuelles qui sont à la fois support et étalon ? Probablement pas en tant que tel mais je ne peux pas répondre à la question, surtout en présence de grands spécialistes des cryptages, des monnaies digitales et de leur opérabilité.

C'est ce souci qui a probablement amené les concepteurs du bitcoin et d'autres à envisager la blockchain.

Mais le problème est qu'un cryptogramme n'a pas en soit de valeur. Or la fonction de réserve implique une valeur au support monétaire qui lui est donné par ce que nos livres appellent le « stamping » l'estampage » la conjugaison d'un support et de l'étalonnage.

Un nombre est un mode de classement mais ne confère pas de valeur car contrairement à un métal, comme l'or ou l'argent..., il n'a pas de valeur intrinsèque. Un cryptogramme n'a pas plus de valeur. Oui, mais unique et rare il peut toutefois prendre une valeur plus au moins grande selon qu'il est plus au moins inviolable car dès lors il devient utilisable comme l'est une serrure pour protéger son bien, sa réserve. Il est rare car il faut l'élaborer et a le coût de cette élaboration (puissance informatique et électricité impliquée à la mise en œuvre de cette dernière). Qui plus est, comme les pièces d'or de l'Oncle Picsou sur son tas d'or (Disney), il devient susceptible d'accumulation.

Mais pour prendre vie, Il faut donc qu'il soit associé soit à une créance émise qui serait échangeable ou émise indépendamment. Dans un cas comme dans l'autre, même si les statuts légaux et fiscaux sont différents, nous sommes en présence d'unités monétaires. Un nombre d'unités et pas le nombre lui-même est associé à une valeur.

On voit bien ici, le caractère mystique qui peut être attribué à l'unité monétaire dès lors qu'on dispose du pouvoir de la libérer de son abstraction en l'associant à une créance, ce droit d'échange, et que dès lors elle prend une valeur. C'est ce qu'on appelle le privilège de seigneurage dont chacun voudrait disposer, celui de créer de rien de la valeur, transmuter du plomb en or. En raison de la peur de l'avenir, l'être humain raisonnable, pour se protéger, aime à accumuler de la valeur. Nous avons déjà abordé cette question de la valeur d'un cryptogramme qui inviolable, peut devenir rare et répondre aux lois de la demande et de l'offre des marchés mais ainsi affecter la répartition des ressources de nos économies.

### **3. La blockchain une contribution possible à la sécurité du suivi de l'étalon et à son inviolabilité – l'inverse de l'anonymat ?**

Laissez-moi tout d'abord vous donner ma vision de comptable de base sur ce à quoi se relie la « blockchain » dans l'univers des échanges humains.

La blockchain est un dispositif destiné à prouver l'intégrité de l'enregistrement de l'image d'un échange entre des êtres ou machines ayant une autonomie. Elle implique donc un objet et des êtres autonomes. Du fait qu'il sera passé entre au moins deux êtres (humains ou sociétal) l'échange devient lui-même commun mais aussi autonome car il ne peut être modifié dans ses caractéristiques (objet – prix) sans l'accord de l'autre ou plutôt s'il est modifié c'est un autre échange. Ce sera une image, un

contrat, un droit un objet comme un bitcoin. Dans notre univers tout est unique. On peut commencer par l'être humain. M X est unique qu'il soit ou non normalien. Si vous en voyez deux, c'est que vous avez un trouble cérébral ou de vision ou que l'un est un travesti. L'image par différents procédés peut être double ou même représenter une réalité semblable mais la réalité est unique, c'est son image qui peut être multipliée. Evidemment, l'échange et la confiance entre humains impliquent qu'ils voient la même image et veillent à chasser les doublons et les travestis. Pour ce faire, par exemple, au 15<sup>ème</sup> siècle un dominicain, employé dans une banque, à décrit un procédé dit de « la partie double » qui transcrit (dans un ouvrage appelé « La suma ») l'idée que si je prête 100 florins à Monsieur X celui-ci me doit cette même somme. Ainsi, va-t-il écrire dans son livre de compte qu'il a retiré 100 Florins de sa caisse puisqu'il les a remis à Monsieur X et que désormais il dispose d'un prêt à l'encontre du même M X qui le lui dit. Il enregistre une créance de 100 Fl au débit de son livre et une diminution de FL 100 de sa caisse. Evidemment, les livres de M X devraient être réciproques, caisse en augmentation et dette pour ces même FL 100. Cet enregistrement est apparu ultérieurement utile à la démonstration de la preuve de la transaction. Ainsi, les livres comptables sont-ils devenus obligatoires par la loi pour les commerçants (code de commerce article L 12312). Mais comment fait-on pour que le livre comptable devienne une preuve. Le législateur dispose tout d'abord que le livre est coté et paraphé au tribunal de commerce avec une date pour cette opération et qu'il soit relié de sorte qu'on ne puisse pas lui arracher ou ajouter un feuillet numéroté fait en outre d'un papier non altérable (comme le serait le papier d'un billet de banque). Ensuite, il dispose que les écritures soient datées et être passées dans un ordre chronologique, sans rature ou correction lesquelles en conséquence se verraient de tout observateur.

Aujourd'hui le dispositif existe toujours sous une forme renouvelée digitale. C'est le Fichier des écritures comptables « FEC » instauré par le décret du 29 Juillet 2013 qui transpose un texte européen.

La blockchain, ce n'est rien d'autre qu'un dispositif destiné à assurer l'unicité des enregistrements et leur classement chronologique, comme l'assure la numération. Evidemment, plus de papier, plus de ratures visibles, plus de chimie pour effacer l'encre après une erreur... Le dispositif de sécurité n'est pas que les sommes échangées entre prêteur et emprunteur sont réciproques même si elles le sont toujours par définition du droit contractuel. Ce que fait la blockchain, c'est que l'enregistrement étant décentralisé, des copies en sont faites d'une manière continue et que si l'un « corrige » unilatéralement un des exemplaires, les copies du livre ne seront plus conformes. La chronologie est aussi un axiome nécessaire qui n'est pas une nouveauté mais qui est assuré par le « hash » à sens unique des blocs que permet l'ordinateur qui conjugué à l'unicité des faits en assure l'inviolabilité relative. La fraude qui consisterait à modifier une écriture se verrait car ce ne serait pas la même écriture que celle qu'on chercherait à annuler ou neutraliser partiellement. Elle sera de ce fait sera visible et vue.

On notera qu'une seule dissociation serait suffisante pour assurer l'intégrité de la transaction ou plutôt sa surveillance si la copie faite était stockée chez une autorité hiérarchique indépendante qui aurait un pouvoir de surveillance (vision) de l'opérateur, surtout s'il n'était pas réciproque. La blockchain diffère de ce schéma puisque le système est collaboratif tant à l'enregistrement qu'en surveillance. On comprend tout de suite qu'il y a une question qui est de savoir qui dispose des clés d'arbitrage en cas d'anomalie, d'abord d'analyse, puis de solution.

Un schéma est-il supérieur à l'autre ? C'est une question d'abord de coût de traitement et notamment du coût de l'énergie. C'est aussi une question d'organisation sociale. Probablement, l'objet et l'usage sont les facteurs importants de la réponse. Par exemple, pour des usages publics comme la conservation de documents qui par essence sont supposés publics comme un acte notarié de propriété (qui sera stocké au registre des hypothèque) le système a de grandes vertus car de consultable, il devient partagé entre un nombre défini d'opérateurs qui sont par statuts égaux, Notaires en France, avocats d'en beaucoup d'autres pays. Les volumes sont peu importants. Différent, est l'usage monétaire.

#### **4. L'Usage Monétaire : Les caractéristiques nécessaires.**

Il s'agit comme on le sait d'un sujet différent même si par exemple le bitcoin utilise la technique de la blockchain pour garantir l'unicité du support donc prouver l'intégrité des transactions rapportées.

Pour répondre aux besoins monétaires il faut non seulement un étalon, mais aussi que la quantité de monnaie disponible dès lors émise, puisse être ajustée aux besoins afin que sa valeur soit assez stable mais suffisamment flexible pour servir de régulation supérieure en cas de besoin. Il faut à la fois assez de monnaie liquide et d'instruments financiers pour satisfaire aux besoins des agents économiques et de leurs échanges. Il s'agit d'une vaste question car tout instrument de dette est une monnaie virtuelle de liquidité différente et de vitesse de rotation variable comme le sont les besoins d'échange, cela selon le moment (par exemple pour l'agriculteur selon les saisons). C'est une raison de plus pour que l'étalon soit stable et que la quantité de support puisse être ajustée. C'est une des explications que dans un contexte non inflationniste du fait d'un ralentissement des échanges et donc de perte de valeur, avec un étalon – le dollar devenu – autonome il a fallu compenser la perte de valeur des portefeuilles d'instruments par de très lourdes injections monétaires, les QE. On a depuis longtemps (Bodin 15<sup>ème</sup> siècle) démontré l'existence d'un effet à la quantité monétaire.

Ce qui est en jeu, c'est l'édifice social et le système politique. Une inflation par exemple, joue comme un impôt. L'impôt selon son usage va avoir des effets différents comme l'émission monétaire. Tout est en jeu, le système de prix, comme par effet induit, le système de répartition et le pouvoir.

Pour cette raison, un système qui aurait pour vertu d'être autonome ne serait pas viable. C'est par exemple démontré par la situation des pays frappés par la malédiction de disposer de matières premières valorisées qui en fait sont sur-financés gratuitement (sans travail).

Une monnaie virtuelle est tout à fait envisageable et même probablement un progrès déjà existant car notre système financier, n'est déjà plus que virtuel.

Il ne peut pas survivre sans régulation de la valeur des supports. Mais aussi, les vitesses de rotation des dispositifs d'échange et de sécurité d'une monnaie cryptographique sont en jeu dans la mesure où certains sont plus rapide que d'autres. A qui la confier le soin d'assurer l'universalité nécessaire du support tout en probablement prévoyant différents dispositifs d'échange pour assurer différentes vitesses, comme comment déterminer les quantités adéquates est un sujet différent de l'étalon que nous n'avons plus autrement que par le dollar (85% des échanges interbancaires et des quantités de devises traitées). En soit, il ne m'apparaît pas que l'anonymat soit intrinsèque aux systèmes collaboratifs autrement que par convention. On sait retrouver les adresses IP, comme par recoupement des observations et suivi des blocs retrouver les identités de celles qui seraient cachées, en soit déjà une source d'identification quand d'autres sont visibles. Par ailleurs, dans le contexte actuel l'attente du public pour des raisons de sécurité l'anonymat comme la protection des données individuelles doivent avoir des limites qui sont dans l'usage fait d'instruments à pouvoir libérateur (drogues, prostitutions, spéculations financières répréhensibles ...etc). la lutte contre le blanchiment implique cette limite. A qui confier ce pouvoir comme comment mettre fin à l'anonymat dans les conditions judiciaires de garantie des droits des individus, reste à établir. En plus du pouvoir judiciaire situé en haut des systèmes constitutionnels démocratiques, des administrations civiles existent déjà avec ces pouvoirs. Reste la difficulté de leur juridiction géographique sur un monde digital dont les frontières n'existent pas encore vraiment. Il est probable que des traités soient nécessaires comme lorsque les droits maritimes et ferroviaires ont été mises en place pour la prospérité de l'humanité grâce aux échanges rendus possibles. Le sens des choses rend la monnaie digitale obligatoire mais ses dispositifs techniques possibles nombreux sans même prendre en compte les progrès incessants des outils. Où et à

quel moment s'arrêter sur une solution universaliste m'apparaît aujourd'hui plus qu'hier, grâce à votre journée et aux brillants exposés qui s'y sont succédés une question qui reste ouverte. Celles qui permettraient la flexibilité tant de l'étalon que des supports et des systèmes d'échange forment sûrement la voie à suivre.

Cela a été un honneur pour moi de venir parler devant vous des contraintes et des espoirs que je voyais.

Les monnaies digitales comme les échanges intellectuels autorisés par cette journée dont je remercie Ricardo Perez Marco et son équipe du Labex de Modélisation Financière d'avoir permis le succès contribuent à l'avancée du sujet. J'ai est vu aussi la force entrepreneuriale qu'il génère et qui lui est associé et qui contribue à cette avancée d'une manière essentielle par le rapport qu'elle crée avec l'utilisateur potentiel. Je les remercie de m'y avoir invité

Le 16 novembre 2016