PARTIE 1

Monnaie et *bitcoin*

1. De la notion de monnaie

Alors que nous allons parler dans cet ouvrage de crypto-monnaie, il est important de comprendre ce qu'est une monnaie. Celle-ci est multiforme et multifonction, ce qui peut rendre son contrôle difficile, alors même que les banques centrales font de la maîtrise de sa quantité un axe prioritaire de leur politique. La monnaie peut se définir par sa forme et par sa fonction.

Commençons tout d'abord par sa fonction. Sans monnaie, nous serions réduits à une économie de troc. Nous risquerions d'attendre longtemps pour trouver un interlocuteur adéquat. Sur un marché fluide de biens et services, il est envisageable d'échanger un bien ou service contre un autre. Pour parvenir à les échanger rapidement, on utilise un moyen de paiement commun, la monnaie, qui sert ensuite à acheter ce dont on a besoin à d'autres personnes qui acceptent le même moyen de paiement. La monnaie garde longtemps sa valeur, elle peut aisément servir à exprimer les prix et elle est largement acceptée.

Les économistes distinguent trois fonctions :
- une unité de compte servant à exprimer les prix des biens ;
- un moyen d'échange, reconnu par tous, pour effectuer des transactions ;
- une réserve de valeur, une des formes de la richesse, permettant de reporter dans le futur l'acquisition d'un bien ou d'un service.

Quelle forme prend-elle ? Au cours des siècles, la monnaie a pris de nombreuses formes parmi lesquelles les coquillages, l'orge, le poivre et, bien sûr, l'or ou l'argent. La valeur de la monnaie est fondée sur ce que l'on peut en faire et sur le fait qu'elle a un coût de

remplacement. Elle ne doit évidemment pas être périssable. Tel est le cas du coquillage, de l'orge ou du poivre. À l'inverse, ce n'est pas le cas par exemple des fruits. Mais elle doit de plus être divisible. On doit pouvoir diviser cette monnaie et en normaliser chaque unité, ce qui n'est pas facile avec l'orge ou le poivre. Voilà une qualité qu'ont les métaux précieux, qui supportent bien l'épreuve du temps et sont divisibles en pièces normalisées.

Si l'or et l'argent ont été pendant longtemps la principale monnaie, ce sont des métaux lourds et difficiles à transporter pour les échanger contre des biens ou des services. Aussi, il est apparu plus pratique de les déposer dans une banque en échange de billets.

Au bout d'un certain temps, les échanges ont eu lieu uniquement avec des billets et des pièces et la créance de papier a fini par se désolidariser du métal. Ainsi est né ce que l'on appelle la monnaie fiduciaire qui n'a pas de valeur matérielle mais uniquement celle qu'une nation décide collectivement de lui assigner.

La monnaie fonctionne parce que les gens y croient**.** Si un agriculteur n'arrive pas à vendre ses céréales, il peut être obligé d'accepter un moindre montant de pièces et billets en échange de celles-ci. Le prix des céréales baisse parce que la masse de monnaie en circulation est trop restreinte. Cela peut être dû au fait qu'il n'y a pas assez d'or pour frapper de nouvelles pièces. Si les prix baissent, on parle alors de déflation. En revanche, s'il y a plus de monnaie en circulation, mais le même niveau de demande de biens, la valeur de la monnaie chute et on parle alors d'inflation. Il faut en effet payer plus pour obtenir la même quantité de biens ou de services.

La valeur de la monnaie dépend essentiellement de la confiance que les gens mettent en elle. Dans les années 1980, les Argentins ont perdu confiance dans leur monnaie, car l'inflation en rognait rapidement la valeur. Ils ont alors commencé à utiliser une monnaie plus stable, le dollar américain. L'État argentin a perdu son monopole d'émission de monnaie et la dollarisation de l'économie a été très difficile à inverser. Ainsi, pour qu'une monnaie fonctionne bien, il est nécessaire que les gens aient confiance en elle. Notons que le terme de fiduciaire vient du latin signifiant « foi ».

Dans les statistiques officielles, en général, on mesure le montant de monnaie dans un pays par la masse monétaire au sens large, qui comprend tout ce qui représente une réserve de valeur et de liquidité [1].

De nos jours, la masse monétaire consiste principalement en dépôts bancaires et non en monnaie de papier. Cette monnaie fiduciaire est plus commode à utiliser que les métaux précieux. L'ajustement de la masse monétaire ne dépend pas du montant de métaux précieux disponible. Mais cela crée en soi une complication : précisément parce que le montant de métaux précieux est fini, il y a une limite au montant de billets que l'on peut émettre.

S'il n'y a pas d'or ou d'argent pour garantir la monnaie, comment les Autorités savent-elles combien de billets imprimer ? Pour gagner en popularité, les Autorités peuvent être tentées d'émettre de la monnaie, mais si elles font trop tourner la planche à billets, les prix vont monter. Et les vendeurs s'attendant à ce que les prix continuent à augmenter vont accroître leurs propres prix encore plus vite. Si le gouvernement ne freine pas de telles anticipations, la confiance dans la monnaie s'émousse et elle risque en définitive de perdre toute valeur. C'est ce qui se produit en période d'hyperinflation.

---

1. Parmi les éléments entrant dans la monnaie au sens large, le Fonds monétaire international (FMI) inclut :
   - La monnaie nationale (généralement émise par la banque centrale).
   - Les dépôts transférables, qui comprennent les dépôts à vue (transférables par chèque ou mandat).
   - Les chèques bancaires (utilisés comme moyen d'échange).
   - Les chèques de voyage (utilisés pour des transactions avec les résidents) et les autres dépôts communément utilisés pour effectuer des paiements (tels que les dépôts en devises).
   - Les autres dépôts, tels que les dépôts d'épargne non transférables.
   - Les dépôts à terme (fonds laissés en dépôt pour une période donnée).
   - Les pensions livrées (par lesquelles une des parties vend un titre et s'engage à le racheter ultérieurement à un prix défini).
   - Les titres autres qu'actions, tels que les certificats de dépôts négociables et les billets de trésorerie (qui sont essentiellement des reconnaissances de dettes émises par des sociétés).

Pour résister à cette tentation d'imprimer de l'argent à tout va, de nos jours, la plupart des pays confient à une banque centrale indépendante le soin de déterminer combien de monnaie imprimer, en fonction d'une analyse des besoins de l'économie, et ils chargent cette banque centrale de ne pas transférer des fonds à l'État pour financer leurs dépenses.

Quel est le lien avec notre sujet sur le *Bitcoin* ? Nous venons de parler de support pour les monnaies fiduciaires, pièces et billets dont l'émission est placée sous le contrôle d'une autorité indépendante : la banque centrale, une autorité indépendante des gouvernements chargée de s'assurer de la connexion entre la valeur de cette monnaie et la réalité économique.
Bien que juridiquement on ne sache pas encore affirmer avec certitude que le *bitcoin* est une monnaie au sens juridique (voir à ce sujet la Partie 4), celui-ci présente des similitudes et des différences [2] avec les monnaies fiduciaires traditionnelles décrites précédemment. Nous allons donc expliquer comment le *bitcoin* fonctionne, en gardant à l'esprit la monnaie traditionnelle telle que nous la connaissons.

2. Introduction au *bitcoin*

Parmi toutes ces nouvelles monnaies numériques qui font l'actualité, le bitcoin *reste de loin la plus célèbre pour le grand public. Pourtant son fonctionnement demeure bien mystérieux et sa réputation*

2. Tout d'abord la monnaie *bitcoin* s'appuie sur des supports électroniques : vous n'aurez jamais la possibilité de voir un « bitcoin ». En ce sens, le *bitcoin* ressemble plus à de la monnaie scripturale détenue sur nos comptes bancaires. Son caractère électronique lui donne la possibilité de s'échanger facilement par un simple clic sur son ordinateur ou son mobile, ce qui n'est pas possible avec les pièces et les billets. Elle ne dépend d'aucune autorité centrale pour garantir son cours et assurer la confiance. Toute la construction de cette monnaie repose en effet sur un vaste réseau de communication planétaire avec ses propres ressources humaines et techniques dont aucune maille du réseau ne peut se prévaloir d'avoir plus de poids qu'une autre. Enfin, une transaction en *bitcoin* est auditable, ce qui n'est pas le cas avec une transaction en monnaie fiduciaire.

controversée. En tout cas, le bitcoin *suscite la curiosité et force est de constater qu'après examen, il mérite cet attrait. Aurait-on enfin trouvé, vingt ans après la naissance du* Web*, la monnaie de l'Internet ?*

Le *bitcoin* a été créé fin 2008 pour réaliser des transferts d'argent entre deux personnes sans faire intervenir une quelconque autorité ou institution financière jouant le rôle de tiers de confiance. La validation de chaque transaction est effectuée par des volontaires qui aspirent à être récompensés en *bitcoins…* Cette communauté de volontaires, qui ne se connaissent pas, joue en quelque sorte le rôle du tiers de confiance.

La régulation de cette monnaie s'appuie sur des preuves de travail (*Proof of work*) et la sécurité du système est une affaire de cryptologie et de puissance de calcul. Tout se passe dans le réseau, le programme tournant depuis sept ans a été pensé pour distribuer 21 millions de *bitcoins* pendant environ 130 ans. Du point de vue de ses créateurs et de ses adeptes, la confiance naît justement de l'absence d'autorité humaine, réputée plus corruptible *a priori* qu'un programme connu et distribué sur le réseau. Ce programme peut être lu par la communauté des informaticiens et les transactions apparaissent en clair dans la mesure où il n'y a pas de chiffrement. Il n'en demeure pas moins que tout ce qui touche au *bitcoi*n nourrit la méfiance, voire le fantasme.

Des rapports des grandes banques centrales ont été remis et n'expriment pas tous la même bienveillance vis-à-vis de ce nouvel arrivant. Les sénateurs canadiens, américains et français par exemple s'y sont penchés et s'y pencheront de nouveau sans doute, concluant qu'il faut continuer à suivre le sujet.

Actuellement, se construisent les outils pour utiliser les *bitcoins* : des *wallets* (portefeuilles numériques) pour acheter ou vendre des *bitcoins* sur des plates-formes d'échange contre des devises classiques. Ou encore des logiciels pour réaliser des transferts d'argent de personne à personne dans la devise *bitcoin*. Il existe des distributeurs de *bitcoins*, des rayons de grand magasin et même des

bars acceptant le *bitcoin* en proximité et, bien sûr, des commerces en ligne qui acceptent cette devise.

Mais le potentiel du *bitcoin* n'est pas encore exploité, loin s'en faut. Derrière le folklore et les péripéties des plates-formes, il existe un « système de paiement » *Bitcoin* (avec un B majuscule, appelé aujourd'hui *Blockchain* pour éviter la confusion), pour ainsi dire un écosystème *Bitcoin-Blockchain*, qui potentiellement peut bouleverser une partie de l'économie de l'Internet et même au-delà, par des innovations pratiquement inscrites dans le système.

Ces innovations trouvent naturellement leur place dans la nouvelle économie de partage, quand il s'agit par exemple d'inventer des solutions de paiement pour des plates-formes collaboratives plus fluides et moins chères que les moyens de paiement actuels qui n'ont pas été créés pour cela.

Toutefois, il reste au *bitcoin* de nombreux défis à surmonter pour exister en tant que monnaie pratique : la volatilité de la devise, la robustesse des plates-formes d'échange, la complexité de sa gestion liée à l'accroissement du nombre de transactions, pour ne citer que ces trois difficultés. Le *bitcoin* intrigue et suscite de nombreuses questions, ce livre va s'attacher à y répondre.

3. Une histoire du *bitcoin*

L'histoire du bitcoin *commence le 1er novembre 2008 avec la publication des spécifications du système* Bitcoin[3] *par un certain Satoshi Nakamoto qui ne se fera jamais connaître. Ces spécifications font quelques pages et, si l'on excepte des calculs mathématiques obscurs pour beaucoup d'entre nous, il reste un énoncé clair des intentions et du fonctionnement du système, clair… autant que faire se peut. Pour les intentions, il s'agit de réaliser des paiements sur*

3. *Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin* : un Système de Monnaie Électronique de Pair à Pair.

Internet sans passer par les tiers de confiance que sont aujourd'hui les institutions financières.

Le 3 janvier 2009 survient la création du premier bloc appelé « block genesis » de 50 *bitcoins*. Le 12 janvier 2009 a lieu la première transaction de pair à pair entre Satoshi Nakamoto et Hal Finney, un cryptologue célèbre qui avait travaillé sur les notions de Preuve de Travail (*Proof of Wo*rk) dont se sert le système *bitcoin* justement pour se réguler (cf. Point 4 : Un exemple de transfert). Le 5 octobre 2009 naît le premier taux de change et le *bitcoin* vaut ainsi 0,0001 $. Le 25 avril 2010 la première cotation voit le jour, le *bitcoin* (BTC) vaut alors 0,0003 $: trois fois rien mais trois fois plus que 6 mois plus tôt. Le 9 février 2011, la parité *bitcoin*-dollar est atteinte, le *buzz* médiatique autour du *bitcoin* peut commencer. Les veilleurs que nous sommes scruteront ses moindres gestes.

Les premiers rapports et notamment celui de la Banque centrale européenne sont produits l'année suivante, en 2012, lorsque la valeur du *bitcoin* est de 15 $ environ ; le rapport est critique vis-à-vis du *bitcoin*. En 2013 et 2014, ont lieu les audiences des sénats américains, canadiens et français à propos du *bitcoin* qui se concluront par une volonté de surveiller le développement sans entraver la capacité d'innovation de cet ovni monétaire. Pendant ce temps, le cours flambe à plus de 1 000 $ le *bitcoin* fin 2013, avant de redescendre tout au long de 2014, pour se retrouver à la moitié de sa valeur au début de l'année 2015.

Il faut dire que la monnaie *bitcoin* subit des secousses : l'affaire dite Silkroad, du nom d'une plate-forme illégale où le *bitcoin* servait de monnaie d'échange pour un trafic de vente de produits illicites sur Internet, a éclaté au grand jour fin 2013, suivie, plusieurs mois après, d'une seconde affaire Silkroad sur le même modèle. Début 2014, est apparue la faillite de la plate-forme d'échange japonaise MtGox dirigée par un Français, sur fond de négligences et de malversations : 744 408 *bitcoins* disparaissent lors de la faillite. Début 2015, ce sont 18 864 *bitcoins* qui sont volés sur une plate-forme slovène.

Pourtant, de plus en plus d'acteurs s'intéressent au *bitcoin*. Tout d'abord à la monnaie *bitcoin* pour de l'acceptation ou de l'échange, voire du transfert de fonds. Puis, progressivement, la tendance est de regarder le protocole, le système *Bitcoin* et notamment la *Blockchain* qui permet de valider et de mémoriser les transactions en *bitcoins*. Sur la monnaie *bitcoin*, les points de vue diffèrent selon les pays. Ainsi en Russie, elle est vue comme une monnaie illégale, alors qu'aux États-Unis elle est considérée comme un actif et non comme une monnaie. En 2015, son cours a été relativement stable, la plupart du temps entre 200 et 250 euros, mais grimpait début 2016 autour des 350 euros. C'est dire que cette monnaie est encore très volatile et continue à attirer les *traders* de tous les continents.

Un entrepreneur et informaticien australien Craig Steven Wright a revendiqué officiellement la paternité du *bitcoin*, début mai 2016, alors qu'il avait jusqu'à présent réussi à garder l'anonymat. Le père de cette monnaie possède un million de *bitcoins* qui valent aujourd'hui environ 450 millions de dollars.

« Satoshi est mort, mais ce n'est que le début », affirme Craig Steven Wright, qui a accordé un entretien à plusieurs médias et apporté sur son blog une preuve technique censée démontrer qu'il est bel et bien le mystérieux Satoshi Nakamoto : un message marqué numériquement qui correspond à la clé de chiffrement privée utilisée pour signer le neuvième bloc de la *Blockchain Bitcoin*. Ce bloc est significatif car il contient une transaction qui transfère les bitcoins de Satoshi Nakamoto à Hal Finney, un cryptographe passionné par la technologie *Blockchain*.

Ses explications ont convaincu deux piliers de la communauté *Bitcoin*, Jon Matonis et Gavin Andresen, qui communiquaient par voie électronique avec Satoshi Nakamoto dans les premiers jours de la création du *Bitcoin* sans jamais connaître sa véritable identité.

Des doutes subsistent encore cependant car si le neuvième bloc dans la *Blockchain* est important pour signifier son lien avec Hal Finney, il n'est pas prouvé que le vrai Satoshi ait possédé les clés privées utilisées pour signer des blocs encore plus tôt dans la *Blockchain Bitcoin*, notamment le tout premier.

4. Un exemple de transfert

Nous allons expliquer un transfert d'argent entre Alice et Bruno qui n'ont pas de compétences particulières en informatique et utiliseront des wallets *à* bitcoins *; toute la suite du transfert se faisant à l'aide de ces* wallets*. Le mot* wallet *représente ici une interface cachant toute la mécanique* bitcoin *derrière des menus simples : acheter ou vendre en* bitcoins*, donner ou recevoir des* bitcoins*, consulter son solde ou son historique de transactions.*

Alice doit 1 *bitcoin* à Bruno. Elle utilisera le service « donner des *bitcoins* » de son *wallet*, saisira l'identifiant du *wallet* de Bruno, le montant à transférer (1 BTC en l'occurrence) et utilisera son mot de passe. Bruno, averti de ce don, ouvrira le service « recevoir des *bitcoins* » et saisira son mot de passe pour bénéficier de ce don. En fait, les *bitcoins* sont logés dans des adresses et le transfert s'exécutera comme un simple changement de propriétaire de l'adresse où se trouve le *bitcoin*. Nous reviendrons sur ce point important par la suite.

Le *wallet* de Bruno demande au réseau une adresse de réception pour le *bitcoin*, adresse qu'il envoie au *wallet* d'Alice. Ce dernier va chercher sur le réseau à libérer 1 *bitcoin* appartenant à Alice en donnant la ou les adresses contenant l'argent, et ajoute l'adresse de réception laissée par Bruno. Le *wallet* d'Alice envoie le tout sous forme de signatures sur le réseau pour validation, la transaction est mélangée à d'autres transactions dans ce qui est appelé un bloc.

4. Le travail de ces volontaires ressemble à celui des mineurs chercheurs d'or dans la mesure où ils extraient de la mine de nouveaux *bitcoins* comme les mineurs trouvent de nouvelles pépites. Au début du *bitcoin*, le minage pouvait être réalisé par un micro-ordinateur un peu gonflé et le mineur était une personne physique. Aujourd'hui, le minage est l'affaire d'un *pool* de minage concentrant des participants et une puissance de calcul très importante.