Préface

de Jean-Joseph Goux

Dans l'Histoire déjà longue de la monnaie, l'invention du Bitcoin, cette monnaie numérique aujourd'hui encore controversée et expérimentale, apparaîtra très certainement comme un chapitre nouveau à la fois inéluctable, difficile, et chargé de multiples polémiques. Contrairement à la monnaie de compte qui fût sans doute à la base des premières opérations de calcul de type monétaire (pour les impôts par exemple), contrairement à la monnaie métallique circulante, frappée par l'État, dont les Grecs furent les inventeurs – et qui nous a été familière jusqu'à une époque encore très récente – le Bitcoin ou autres monnaies numériques (dites aussi *digitales*, électroniques, cryptographiques, etc.) semblent plus étrangères au sens commun, et en tout cas plus éloignées de l'idée traditionnelle de la « vraie » monnaie qui nous a été léguée jusqu'à ce jour par la culture gréco-romaine. Une véritable rupture, un profond bouleversement, est à l'œuvre, qui nous oblige à une révision complète de nos cadres mentaux. Les résistances à des innovations financières et monétaires ne sont pas nouvelles : la monnaie de papier, le chèque, la carte bancaire, sans parler pour l'instant de l'inconvertibilité des monnaies, ont rencontré de fortes oppositions, suscité des controverses farouches et nourri des angoisses persistantes. Rappelons simplement, parmi mille autres polémiques et réactions négatives, que certains citoyens, aux États-Unis, avaient dénoncé la monnaie de papier comme contraire à la constitution américaine après qu'elle a été perçue, ailleurs, comme un artifice diabolique.

Le Bitcoin ne fait pas exception. D'autant plus que les procédures, les protocoles qui permettent de faire fonctionner cette monnaie décentralisée que certains disent « virtuelle », ne sont pas toujours faciles à saisir du premier coup d'œil et à accepter sans réticences. Cette monnaie récente, qui n'existerait pas sans les possibilités du réseau Internet, ne fonctionne que par une médiation technologique assez complexe qui nous porte bien loin de l'échange direct de pièces de monnaie palpables, ou même de l'écriture bancaire d'un avoir.

Le mérite de l'ouvrage que publient aujourd'hui Jacques Favier et Adli Takkal Bataille est d'être une contribution, claire et détaillée, à une meilleure compréhension de cette monnaie numérique ; une *monnaie acéphale*, insistent les auteurs, car fonctionnant, ce qui n'est pas sa moindre originalité, sur la base d'un réseau sans organe central de contrôle et de gestion, ni la sanction et la garantie d'un tiers de confiance.

Comment cette monnaie, sans autre réalité que celle d'un code numérique chiffrant a-t-elle pu voir le jour ?

On peut dire que l'invention du Bitcoin est le couronnement une évolution historique relativement rapide à l'échelle de l'histoire des monnaies. D'abord, la disparition complète de la matière « précieuse » monétaire circulante au profit du signe monétaire, le billet de banque, qui est censé la représenter ; puis le passage de ce signe monétaire couvert, convertible, à un signe monétaire flottant ou inconvertible. Au lieu d'une conception substantialiste de la chose monétaire (l'or, l'argent), c'est une conception purement sémiotique qui a prévalu. Mais si la monnaie n'est qu'un signe, une sorte de langage, elle peut se communiquer comme un signe, moyennant, bien sûr, un certain nombre de procédures spéciales. Il ne manquait plus que quelques pas pour aboutir à la monnaie numérique. La transmission électronique des signes, par l'invention et la pratique généralisée d'Internet, a été la condition technique ultime qui a rendu possible cette innovation monétaire. À partir de ces deux conditions préalables (inconvertibilité bien acceptée du signe

monétaire et transmission électronique de l'information, partout et instantanément) on a pu assister à une cristallisation rapide, conduisant à l'invention d'un protocole d'usage d'un nouveau type de monnaie, une monnaie numérique, qui répond aux caractéristiques traditionnelles de la chose monétaire tout en permettant des opérations que la monnaie traditionnelle ne permet pas. Le Bitcoin est le résultat à la fois scandaleux et inéluctable de cette évolution. À l'âge d'Internet, la mise en place de ce type surprenant de monnaie n'est pas le moindre bouleversement qu'a apporté, et continue d'apporter, dans tous les domaines des pratiques sociales, ce mode nouveau de communication.

Un point décisif de rupture a donc été l'adoption de l'inconvertibilité du dollar annoncée par Nixon, le 15 août 1971. Il s'agissait de « suspendre temporairement la convertibilité du dollar américain en or », pour mettre fin aux spéculations qui visaient cette monnaie. L'inconvertibilité du dollar devenue permanente, et avec lui de toutes les monnaies, a changé en profondeur l'idée même du signe monétaire. Il fallait accepter l'idée qu'une monnaie peut exister sans être gagée sur quelque chose de « tangible », selon une expression souvent employée. En régime de convertibilité, on pouvait penser que le signe monétaire, le billet de banque, *représentait* une valeur stable, thésaurisée ailleurs, comme l'or, et à laquelle ce signe pouvait toujours renvoyer, tout comme un signe linguistique renvoie à un sens donné et, au-delà de ce sens à une chose stable et bien définie. C'est ce régime ou ce préjugé de la représentation qui est mis en cause par l'inconvertibilité. Ce n'est pas seulement une décision de technique financière et monétaire, mais avec elle un profond bouleversement de la notion de monnaie et de signe. La monnaie numérique naîtra en partie de ce bouleversement, une fois reconnu et bien accepté que la référence à quelque chose de tangible n'est pas nécessaire, ou même davantage encore, n'est qu'une illusion archaïque.

Comment cette acceptation est-elle possible ? Avec la notion d'une monnaie comme signe sans couverture, sans convertibilité, sans gage tangible, s'impose corrélativement l'idée qu'une

convention partagée est la seule base de la valeur monétaire. Là encore l'analogie avec le langage est éclairante. De même que l'accord implicite et unanime des locuteurs, à l'intérieur d'une certaine communauté linguistique *fixe* et stabilise le sens des mots de la langue, de la même façon l'accord implicite des échangistes, partenaires économiques et commerciaux, institue une certaine unité comme monnaie, et tend à fixer sa valeur. Elle n'est qu'un signe, mais un signe reconnu, accepté, pratiqué, même si ce signe monétaire n'est pas gagé par une substance matérielle ou garanti par une instance extérieure. Il suffit de l'accord implicite de tous pour lui donner une valeur.

En ce sens on peut dire qu'une unité monétaire (et le signe qui la représente) a de la valeur parce que tout le monde pense qu'elle a de la valeur. On peut parler, de ce point de vue, d'une sorte de fiction. Mais l'acceptation unanime et mutuelle fait de cette fiction une réalité durable, qui ne manque ni de solidité ni d'usage pratique.

Cependant, à l'évidence, la transmission d'une information linguistique dans un réseau électronique, et la transmission d'une valeur monétaire posent des problèmes assez différents.

L'un des plus importants est la garantie qu'une certaine quantité d'unités monétaires électroniques ne pourra pas servir plusieurs fois. Contrairement au langage qui ne se supprime pas par la transmission, mais peut être répété sans dommages ni pour le destinateur ni pour le destinataire, les unités monétaires électroniques sont des signes ou des signaux que la transmission pour paiement doit épuiser, supprimer, car ils ne doivent pas pouvoir être réemployés. Tandis qu'un mot ne perd pas son sens à être transmis une ou plusieurs fois, un signe monétaire fait passer sa valeur à un nouveau détenteur, et il est perdu pour le premier détenteur. La propriété, l'avoir individuel, est une condition essentielle de la communication monétaire, que ne connaît pas la communication du sens par les mots du langage.

La sauvegarde de l'unicité absolue de l'opération doit donc être rigoureusement garantie. Ce problème majeur de la monnaie électronique a été résolu par le fameux dispositif de la *blockchain* de Bitcoin sur lequel les auteurs reviennent à plusieurs reprises. Les blockchains équivalent à des registres, des livres de compte infalsifiables, qui valident, enregistrent et datent rigoureusement chacune des opérations de transmission de pair-à-pair. Dès qu'un bloc de transaction est validé, il est ajouté au registre, accolé au bloc précédent, formant une chaîne ininterrompue de blocs, mémoire immuable et toujours consultable des opérations engagées.

Sans dissimuler les problèmes que peut poser cette monnaie encore jeune (y compris les risques d'usage criminel), sans rien cacher des controverses qu'elle continue d'alimenter, sans ignorer les hauts et les bas de son cours, Jacques Favier et Adli Takkal Bataille retracent, en un langage accessible, les différents procédures ou protocoles qui ont permis de mettre en place – depuis les idées astucieuses et fondatrices de l'énigmatique Satoshi Nakamoto en 2008, jusqu'au plus récents approfondissements – le système du Bitcoin et d'étendre de plus en plus ses usages. *Blockchains, hachage, minage*, ces procédures fondamentales caractéristiques du fonctionnement du Bitcoin, comme système électronique de paiement comptant entre pairs, sont abordées d'une façon éclairante et vivante, même si, bien entendu, toutes les plus difficiles complexités de ces opérations ne peuvent être développées dans ce livre aux dimensions limitées.

En même temps sont évoqués dans cette présentation dense et documentée du Bitcoin les multiples horizons ouverts, dans une dimension méta-économique, par l'exemple extrêmement prometteur de cet étonnant dispositif en réseau, sans organe central dirigeant, qui, pour ainsi dire, s'auto-administre lui-même.