ADLI TAKKAL BATAILLE
JACQUES FAVIER

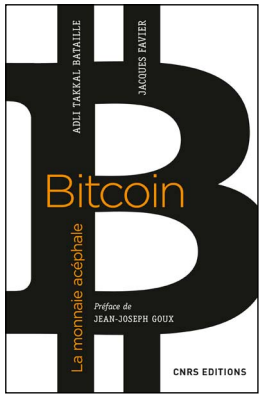
Bitcoin

La monnaie acéphale

Préface de
JEAN-JOSEPH GOUX

CNRS EDITIONS

Présentation de l'éditeur



Voici le guide utile et pratique pour comprendre la méta-monnaie qui pourrait bien redéfinir en profondeur les règles de notre économie globalisée.

Créée en 2009, cette monnaie décrite par les uns comme virtuelle mais considérée par d'autres comme un véritable or numérique s'échange en pair à pair sur Internet en dehors du réseau bancaire traditionnel.

Quelles sont les propriétés spécifiques de cet objet numérique infalsifiable ? Quelles sont les caractéristiques monétaires d'un jeton informatique émis sans autorité centrale, sans banque, sans État ? Que nous dit Bitcoin des nouveaux usages économiques, de la cybercriminalité, de la société de surveillance ainsi que de l'évolution du cyberespace ?

Bitcoin accompagne en effet à la fois Internet dans son évolution et la société dans sa décentralisation, grâce à son architecture et à son registre, la blockchain.

La première grande synthèse en français, claire et accessible, sur la nouvelle monnaie du troisième millénaire.

Jacques Favier, normalien et agrégé d'histoire, a fait carrière dans la banque et l'investissement. Il anime le site « La Voie du Bitcoin ».

Adli Takkal Bataille, diplômé de linguistique, spécialiste du numérique, anime le site « Le Coin Coin. »

ADLI TAKKAL BATAILLE
JACQUES FAVIER

Bitcoin,
la monnaie acéphale

Préface de Jean-Joseph Goux

CNRS ÉDITIONS
15, rue Malebranche – 75005 Paris

ISBN : 978-2-271-11556-0

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.

Introduction

Dans les derniers mois de l'an 2008, le système financier mondial né au début des années 1970 parvenait à retrouver une assise au bord du gouffre par un transfert inouï, vers l'endettement public, des dettes et risques nés de l'activité débridée de la spéculation financière, puis par une politique de création monétaire sans précédent. Le monde reprit sa course effrénée à la croissance, qui malgré les prévisions du Club de Rome et leur bilan accablant quarante ans plus tard, ne cesse d'être prônée par des dirigeants à court d'alternative permettant de conserver leur emprise sur une société sujette à de grandes mutations tout en offrant un monde plus soutenable.

Le 1er novembre 2008, moins de deux mois après la faillite de Lehman Brothers, une note technique décrivait aux quelques centaines d'abonnés d'une obscure publication en ligne consacrée à la cryptographie une invention qu'il n'est pas possible de résumer techniquement en un mot mais qui s'est révélée à maints égards révolutionnaire : un protocole d'échange d'informations sans intermédiaires, un objet numérique non copiable, un livre de compte et d'enregistrement sans fonction centralisatrice et pourtant non-falsifiable, un mécanisme de confiance sans tiers de confiance et sans police, une unité de compte émise indépendamment de toute banque centrale ou commerciale, un possible instrument monétaire sans aucun lien avec une autorité souveraine quelconque.

Cette quasi-simultanéité empêche de considérer le protocole Bitcoin (avec un B majuscule) comme la réponse aux événements. Ceux-ci ont tout au plus précipité la publication de la note signée du nom de Satoshi Nakamoto[1]. Que celui-ci soit un homme ou une femme, américain ou japonais, unique ou collectif, est assez anecdotique. L'essentiel est qu'il avait, en ce 1er novembre, plus d'un coup d'avance sur ce que les événements manifestaient clairement ou suggéraient aux plus critiques des observateurs.

Quatre jours plus tard, alors qu'elle inaugurait le nouveau bâtiment de la *London School of Economics*, il revint à la reine Elizabeth de poser, avec l'élégance ingénue qui n'appartient qu'à elle, la grande question : pourquoi personne n'avait-il rien vu venir ? Le petit aréopage savant qui entourait Sa Gracieuse Majesté ne put sceller un embarras hébété. En France, le président Sarkozy affirmait que personne ne pouvait voir venir la crise. Bien des gouvernants, bien des financiers répétèrent ce genre d'assertions, qui ne donnaient d'indications que sur le spectre étroit de leurs fréquentations et de leurs lectures. En réalité, il est aisé de retrouver tous les avertissements publiés durant des années, et qui furent loin d'être exclusivement le fait des critiques hétérodoxes. Pourtant, pour l'essentiel, la littérature critique visait à dénoncer les « excès » du système, ou ses « dévoiements » : trop de spéculation et pas assez de contrôle, pour faire simple.

Les critiques les plus hardies pointaient deux limites, l'une écologique, l'autre sociale. Si l'on a simultanément trop de gaspillage de ressources non renouvelables et trop d'inégalités, autant dire que les ressources naturelles ne servent plus qu'à payer les frais financiers. Au-delà de cette critique, il reste le choix de prôner l'austérité ou celui de mettre en cause la nature de la « monnaie-dette » et sa création *ex nihilo* par des banques commerciales. L'essentiel de la critique doit donc être une « méta-critique » : c'est le paradigme actuel dont il faut rechercher les ressorts cachés. Seule une réflexion sur les mécanismes du système eux-mêmes peut amener une remise en cause réelle de celui-ci (et non pas des pratiques exercées en son sein et qui

en découlent) et une ouverture vers de possibles r-évolutions d'ordre systémique, tel que l'est le sujet de ce livre.

Or le sujet de la monnaie, de sa nature et des conditions de sa création, n'avait pas suscité la publication d'une littérature critique comparable, par sa masse ou sa réception publique, à la production des études sur la crise à venir. Cela permet de comprendre la vacuité ou la naïveté des premières réactions quand il apparut que le bitcoin, objet non identifié venu d'ailleurs, pouvait peut-être cumuler plusieurs des attributs d'un instrument monétaire. « Le bitcoin, entendit-on alors répéter en boucle, n'a aucun fondement, n'est basé sur rien, n'est régi par aucune autorité et n'est garanti par personne. » Certaines critiques revêtaient un caractère comique, comme celle déniant au bitcoin une valeur fondamentale et ne lui reconnaissant qu'une simple valeur de marché, comme si le dollar ou l'euro avaient valeur intrinsèque et non l'un au regard de l'autre et chacun par sa capacité d'acquérir des biens sur des marchés. On entendit certains parler de ces devises flottantes comme si elles étaient encore grosses d'or. Aussi imprudentes ou impudiques étaient les critiques reprochant au bitcoin de n'être pas émis par une banque centrale, quand il apparaît que 90 % de la création monétaire est aujourd'hui le fait des banques commerciales, qui créent bel et bien *ex nihilo* la monnaie qu'elles prêtent à leurs clients. La distinction entre ce qui est fiduciaire et ce qui est scriptural passait parfois à la trappe dans les raisonnements. Obscènes enfin, les critiques soulignant l'absence de garantie dont bénéficient les détenteurs de bitcoin quand on songe à la modicité des divers « fonds de garantie » constitués pour garantir un système dans lequel, fondamentalement, l'argent des déposants n'est qu'une écriture au passif des banques, et surtout lorsqu'il est apparu en mars 2013 que l'Union européenne pouvait ponctionner directement les comptes en banque (à Chypre pour commencer) sans autre forme de procès.

Comme il arrive souvent, l'irruption d'une nouveauté radicale permet un examen critique non moins radical de ce qui, sans solution alternative adéquate, passait aisément pour naturel.

Le bitcoin est loin d'être la première « nouvelle monnaie » apparue dans (ou contre) le « système » des changes flottants, état de fait instauré de façon toute empirique au début des années 1970. On avait vu les monnaies locales ou complémentaires, monnaies-heures, coupons ou « *miles* », monnaies émises par des sociétés, monnaies électroniques des jeux en ligne théoriquement destinées à demeurer dans les univers virtuels de ces jeux. Aucune de ces monnaies n'avait prétendu à l'universalité, aucune ne pouvait assumer toutes les fonctions d'une monnaie, pour tous et partout. Telles étaient en revanche les ambitions des prédécesseurs du bitcoin : l'e-Gold, le Liberty Reserve, le dollar Linden de Second Life, la WebMoney, le b-money, le bitgold, qu'elles aient existé concrètement ou sur le papier. Certaines étaient nées comme des complots dans le milieu de ceux qui s'intitulèrent les *cypherpunks*, mais d'autres projets fort similaires étaient élaborés dans les bureaux de la Citibank. Aucune ne répondait à la totalité des ambitions d'une monnaie universelle, fluide comme le cash, confidentielle mais sûre, indépendante de tout pouvoir, adaptée au nouveau monde d'Internet. Aucune ne représentait une réalisation aussi parfaite que le bitcoin, même si la question de la soutenabilité de son réseau n'est pas encore élucidée et reste sujet à controverse.

L'invention de novembre 2008 n'a d'abord été reçue que par une toute petite communauté, sur une base largement ludique. Le medium Internet étant encore plus mythologique que le medium télévision, l'essor de l'unité de compte bitcoin (avec un b minuscule) comme une « monnaie » mêla des moments épiques. Entre autres, celui de la fameuse pizza représentant la première transaction avec le monde réel. Ou encore des aventures illicites comme celle de la Route de la Soie où l'anonymat de la monnaie nouvelle, un peu vite jugé total, fit croire à certains qu'elle serait l'instrument idéal de transactions inavouables. Enfin, des désastres classiques comme celui de la faillite de MtGox, que les détracteurs du bitcoin évoquent rituellement bien qu'elle n'illustre pas la faiblesse de la nouvelle monnaie, dont chacun peut et doit garder la clef pour soi, sinon

celle du vieux modèle d'établissement qui prétend en prendre soin pour le compte de ses clients.

Soudain, en 2013, la spéculation s'en mêla. On entendit du côté des puissants et des doctes des cris d'orfraie, comme si leur propre système abhorrait la spéculation. Elle retomba. On entendit des prophéties : la farce était jouée. Naturellement, on parla de Ponzi, ce qui, en matière d'argent, est un peu le point Godwin de l'invective. La mort du bitcoin fut annoncée près d'une centaine de fois par diverses autorités, prix Nobel compris, bien sûr.

À l'automne 2015 un nouveau crédo se fit soudain entendre : le bitcoin était une chose sans intérêt que l'on aurait bientôt tué s'il ne mourrait pas tout seul, mais son livre de compte décentralisé, nommée *blockchain*, allait révolutionner la finance. Ce serait bien sûr des blockchains privées, sur lesquelles seules les grandes banques appartenant à un consortium *ad hoc* pourraient échanger leurs monnaies et leurs actifs. D'une chose publique et ouverte (*open source* et *open data*) il suffirait de faire une chose privée et fermée. D'une chose sécurisée par l'intérêt (gagner des bitcoins en entretenant le système) il suffirait de faire un club de connivence pour ôter son venin à l'invention et la rendre bienfaisante, c'est à dire utile au système dont le projet était justement, à l'origine, de se passer. Cette idée enthousiasmait tous les néophytes, rassurés par des analyses de seconde ou troisième main, et qui ne se rendaient pas compte que très peu de développeurs semblaient y accorder la moindre foi.

Quand on eût bien annoncé que le bitcoin était mort, survinrent des attentats qui permirent de dire qu'il en était la cause, et qu'il fallait en finir avec « l'Internet invisible », les messages codés et les monnaies non régulées, coupables de tant de mal.

E pur, si muove… Des centaines de milliers de gens ont une « adresse Bitcoin » (que l'on peut assimiler à un « compte Bitcoin »), des milliers participent activement, comme développeurs ou entrepreneurs, à cette aventure toute récente mais

déjà grosse de quelques milliards de dollars. Au-delà de cette somme – relativement légère pour un système monétaire d'envergure mondiale, mais non négligeable si on assimilait l'aventure à celle d'une start-up –, il convient de voir que dans toutes les grandes villes du monde, au travers de *meetups*, se réunissent régulièrement des gens, jeunes, moins jeunes, éduqués et actifs, qui explorent ensemble ce que Bitcoin permet ou promet. Si le cours du bitcoin en dollars et en euros reste volatile (mais moins que jadis), la courbe du nombre de transactions quotidiennes monte inexorablement, et sans grands à-coups.

Par où commencer ?

Le bitcoin, sujet aujourd'hui incontournable, reste le plus souvent abordé naïvement et négativement par ceux qui pourraient y perdre, ou de façon à la fois messianique et trop technique par ceux qui développent son environnement. Or tel qui porte sur lui une carte de crédit peut souhaiter réfléchir sur son usage et ce qu'il implique, même s'il ne sait pas expliquer savamment son fonctionnement ou ne peut pas disserter sur la congruence sur les nombres entiers qui sous-tend la cryptographie de type Rivest, Shamir et Adleman. Les aspects très techniques ont été nécessairement simplifiés, et renvoyés aux notes de fin de volume. Toutefois, en ce qui concerne le bitcoin, deux efforts intellectuels s'imposent, tous deux à la portée de chacun.

Il faut d'abord consentir un effort conceptuel. Voltaire fait quelque part la remarque que les gueux reçoivent les signes monétaires comme les sacrements, sans trop d'examen. Keynes écrivait de son côté qu'on adopte plus facilement une nouvelle idée qu'on ne se débarrasse réellement des « idées anciennes qui ont poussé leurs ramifications dans tous les recoins de l'esprit des personnes ayant reçu la même formation que la plupart d'entre nous[2] ». Le bitcoin, pour qui veut dépasser les critiques prudhommesques, exige une capacité réelle d'abstraction mais aussi et surtout de remise en cause. Sur la nature de l'argent – il n'est ni ce morceau de papier dans les portefeuilles, ni conservé au frais dans le sous-sol des banques pas même à Frankfort – mais aussi

la nature de la communauté qui en reconnaît le signe, sur l'espace où il circule, un rhizome géographique et dématérialisé, sur les rapports qu'il entretient avec ce qui tient lieu de souveraineté.

Bitcoin, et derrière lui les crypto-monnaies désormais possibles – puisque tout est en « open source » –, vont changer de manière radicale la nature et la circulation de l'argent, mais aussi multiplier les possibilités, bousculer les contraintes et les mœurs des sociétés. Bitcoin ouvre de nombreuses manières nouvelles d'échanger de l'argent mais également des titres, des contrats, des promesses, des informations…

Quelques considérations sur la monnaie seront aussi inévitables, d'autant plus que l'apparition du bitcoin a considérablement soulevé la poussière autour de l'idole !

Il faut ensuite consentir un effort intellectuel : on ne peut éluder un peu de technique ou de science, sachant toutefois que le bitcoin, chef d'œuvre d'agencement de plusieurs idées, n'est pas proprement dit une révolution scientifique. L'essentiel des mathématiques mises en œuvre date de plusieurs décennies, et ceux qui n'y ont pas accès peuvent en percevoir intuitivement l'effet par quelques analogies poétiques : là où le monde nous abreuve d'informations, nous sommes de plus en plus sujets à des réminiscences proches de celles avancées par Platon. Il n'est pas indispensable d'intimider le lecteur avec les détails de la cryptographie à courbes elliptiques ou avec la recherche du logarithme discret.

Le lecteur ne fera donc pas l'économie d'un peu de technique et de vocabulaire nécessaire. Juste ce qu'il faut pour comprendre avant de réfléchir ou de critiquer. Et seulement après avoir saisi, dans les premiers chapitres, ce qui rend cette chose inconnue tellement désirable à ceux qui l'ont déjà comprise.

Nous avons donc choisi de ne pas présenter ces explications techniques en première partie, comme d'autres auteurs l'ont fait à l'étranger, ou comme les conférenciers le font trop souvent. Rien n'empêche le lecteur technophile de commencer notre

livre par sa deuxième partie, mais le lecteur simplement curieux risquerait, à commencer par la technique, de se décourager faute de saisir les raisons de l'effort intellectuel à consentir. Sans doute nos ancêtres ont-ils été émerveillés de lire l'heure au cadran et de rouler à 100 kilomètres par heure avant (pour certains) de tenter de démonter la montre ou le moteur.

Une fois les bases techniques affermies, le lecteur pourra commencer de se poser de vraies questions financières, et même sociologiques. Le bitcoin est une « monnaie rare », une chose tout à fait opposée aux pratiques actuelles de « Quantitative Easing », mais que ses défenseurs considèrent comme une force. Ont-ils raison de voir dans son extrême divisibilité une réponse suffisante à cette rareté ? Quelle vison du monde reflète ce choix de la rareté monétaire ? Révolution technique et (surtout ?) sociologique, le bitcoin est-il pour autant « révolutionnaire » ? Monnaie potentiellement déflationniste (comme l'or à l'image duquel il a été forgé, conçu pour être rare) le bitcoin est-il pour autant « réactionnaire » ? C'est dans cette alliance de concepts paradoxaux que s'est construit techniquement le bitcoin et qu'il doit être questionné sociologiquement. L'examen de ses paramètres monétaires suggère (comme la mythologie du « minage ») la comparaison avec une sorte d'or numérique, mais cette comparaison classique ne saurait rendre compte du bitcoin dans sa richesse conceptuelle et la multiplicité de ses utilisations possibles.

Or, dans son état actuel, le bitcoin ne pourrait probablement pas se saisir concrètement, dans la « vraie vie », de tous les usages envisageables, et encore moins tous à la fois. Qu'il puisse servir à tout (ce qui est l'objet d'un débat) n'implique pas qu'il puisse trouver sa place comme monnaie universelle bien qu'il ait constitué, avec peut-être plusieurs millions de « bitcoineurs », ce qui est pour l'instant la première communauté monétaire alternative au monde. Plusieurs futurs sont encore possibles.

Nous proposons ensuite, dans notre troisième partie, un parcours de type « historique » traitant, pour commencer, des questions qui se sont posées dans les premières années d'expansion

Table des matières

Préface de Jean-Joseph Goux 7
Introduction 13

I

Sidérant bitcoin

1- Une solution inédite pour un désir ancien 25
2- Un agencement génial,
instrument de véritables exploits 44
3- Une création révolutionnaire
cause d'enthousiasme ou de scandale 65

II

Le bitcoin, sans mystère ni fantasme

1- Esquisse de son ingénieux assemblage 87
2- Croquis des caractéristiques
tant numériques que monétaires du bitcoin 113
3- Ébauche des usages hétéroclites du bitcoin 136

III

Histoire passée et présente d'une monnaie jeune,
féconde et universelle

1- Une enfance difficile, une adolescence turbulente :
le bitcoin dans la zone à risque 165
2- Bitcoin père de toutes les cryptomonnaies 189
3- L'entrée dans la vie active 215

Conclusion 243
Notes 251
Remerciements 269