LA RÉVOLUTION BLOCKCHAIN

PHILIPPE RODRIGUEZ

LA RÉVOLUTION BLOCKCHAIN

Algorithmes ou institutions,
à qui donnerez-vous votre confiance ?

DUNOD

Mise en page : Belle Page

Dunod, 11 rue Paul Bert, 92240 Malakoff
www.dunod.com

ISBN : 978-2-10-076360-3

Remerciements

Tout d'abord, j'exprime ma reconnaissance à l'intrépide communauté Bitcoin en France qui a partagé sa passion avec moi depuis quelques années. Que soient remerciés Pierre Noizat, Gonzague Grandval, David François, Éric Larchevêque, Thomas France, Thomas Voegtlin, Sébastien Couture, Jacques Favier, Karl Chappe, « Marco », Adrian Sauzade, Adli Takkal Bataille, Jean-Yves Rossi, Hubert de Vauplane.

Un grand merci à l'incroyable équipe d'Avolta Partners qui conjugue au présent intelligence et volonté : Patrick Robin, Arthur Porré, Bruno Vanryb, Ève Baldini, Pascal Farrugia, Baptiste Jacob, Thomas Raygagne, Claire Costes, David Laurent.

Merci aux entrepreneurs et politiques qui m'ont fait progresser dans la compréhension des enjeux de la blockchain : Paul Benoît, Isabelle Moureaux, Julien Bayou, Jean-Paul Delahaye, François Veron, Nicolas Debock, Xavier Faure, Thierry Petit, Laurence Parisot, Laure de La Raudiere, Laurent Grandguillaume, Philippe Marini.

Chez Dunod, j'adresse mes remerciements à Odile Marion pour sa confiance et ses conseils précieux ainsi qu'à Marielle Roubach pour sa relecture attentive.

Mes remerciements sincères à Pierre Manenti qui a collaboré à cet ouvrage en le documentant et l'éditant avec un talent et une passion qui le mèneront loin.

Sommaire

La naissance d'une économie pair-à-pair

« Vous ne changerez jamais les choses en vous battant contre la réalité existante. Pour véritablement changer votre environnement, construisez un nouveau modèle qui rend obsolète le modèle existant. »
Richard Buckminster Fuller, 1982[1]

Novembre 2013, Kiev, Ukraine. Alors que les caméras du monde entier braquent leur regard sur la place Maïdan, lieu de rassemblement de l'opposition ukrainienne, un détail attire mon attention dans la vaste foule des protestants. Un partisan de la rébellion tient dans sa main un panneau sur lequel est imprimé un QR Code et au-dessus duquel on peut lire « *Soutenez la révolution* ». Étrange alchimie que celle de cette masse humaine, force visible à l'œil nu, et de ce carré noir et blanc de pixels, puissance invisible, étonnant porteur d'un message, lui, invisible. Il renvoie vers le portefeuille « bitcoin » du mouvement de contestation nationale, appelant aux dons et aides en tout genre, en ces heures désespérées. Au XXIe siècle, le numérique s'est ainsi imposé comme un instrument de notre quotidien, mais aussi comme un outil de la conquête politique.

Inventé dans les années 1990 par une entreprise japonaise, le QR Code a connu un essor formidable depuis une dizaine d'années

grâce à la popularisation mondiale des téléphones intelligents (smartphones). Ce petit carré de modules noirs sur fond blanc renvoie, une fois « scanné » par un téléphone approprié, à un texte particulier, une animation en ligne ou même un site internet. En 1997, les premières versions de QR Code servaient ainsi de titres de transport aux passagers du rail japonais. Un peu moins de vingt ans plus tard, sur la place Maïdan, en Ukraine, leur plus récente version renvoyait tout simplement à une page de don bancaire et permettait à tout détenteur d'un compte bitcoin de s'associer financièrement au mouvement de protestation populaire.

L'astuce d'un virement direct sur le compte des insurgés répondait, en effet, à une situation depuis vertement dénoncée par les médias. Les principaux intermédiaires bancaires en ligne, tel PayPal, avaient bloqué les transferts financiers vers l'Ukraine, étouffant toute possibilité de soutien monétaire au mouvement d'insurrection. La résistance s'était donc organisée pour remédier à la situation, en mobilisant les nouvelles technologies de don en ligne. Indépendamment de tout parti pris dans le conflit ukrainien, l'interdiction du transfert de valeurs numériques est une idée nouvelle dans les relations internationales et mérite de s'y attarder.

L'anecdote de ce manifestant de la place Maïdan et de son panneau de protestation sert régulièrement d'introduction à mes conférences depuis lors. Il montre, en effet, l'opposition existant entre l'idée d'un réseau internet totalement libre et l'autorité encore exercée par certains « gros porteurs », plaçant l'ensemble des échanges numériques sous le contrôle d'une autorité centrale. Dans ce combat, le QR Code est une arme fantastique pour établir un lien direct entre la population et ses outils de transferts de valeur en ligne. Pour cela, elle suppose le développement d'une technologie de stockage et de transmission d'informations à la fois transparente et sécurisée, la « blockchain », et celui d'une monnaie numérique, le bitcoin.

La naissance du bitcoin, une économie pair-à-pair

2010, Paris, France. Mon métier de banquier d'affaires m'amène à conseiller une jeune société française de Montrouge, particulièrement innovante, Qarnot Computing – un hommage au physicien Sadi Carnot (1796-1832), inventeur de la thermodynamique, dont la première lettre a été remplacée par « Q », symbole scientifique de la chaleur. Spécialisée dans la réutilisation de la chaleur produite par les serveurs d'ordinateurs, portée par l'élan de nos politiques de développement durable, elle cherchait à mener une opération de capital pour développer son marché et acquérir de nouveaux clients. L'idée de créer des bâtiments intelligents, capables de subvenir à leurs besoins énergétiques en termes de chauffage par la seule utilisation d'une chaleur déjà produite et malheureusement gaspillée, est tout simplement brillante !

L'ingénieur en chef de ce projet, le polytechnicien Paul Benoît, a inventé un calculateur nommé Q.rad. Construit en forme de radiateur, ce calculateur génial contient de nombreuses pièces chauffantes. Pendant que la machine réalise par exemple des opérations de calcul de risques de contrats des traders d'une banque d'investissement, elle produit en même temps de la chaleur à l'aide de résistances électriques et diffuse cette chaleur dans l'ensemble du bâtiment, à moindre frais. C'est le principe même de l'économie circulaire, avec laquelle nous démultiplions les effets pratiques de technologies déjà utilisées au quotidien.

Sur le fondement du principe de l'informatique en grille (*computer grid*), un ensemble de calculateurs-radiateurs Q.rad forme un supercalculateur. Le cahier des charges de ce dispositif suppose de pouvoir produire de la chaleur tout en annulant le bruit causé normalement par les ventilateurs intégrés. L'idée du calculateur-radiateur était née, faisant de la faiblesse des anciens

modèles la force de cette technologie nouvelle. Tous ces détails, le talentueux ingénieur me les a expliqués au cours des nombreux voyages en Eurostar que nous avons eu le plaisir de partager, en déplacement entre Paris et Londres.

C'est au cours de l'un d'entre eux qu'il m'a, pour la première fois, parlé du « minage des crypto-monnaies ». D'abord des calculateurs chauffants, bientôt des calculateurs « gueules noires », décidément, la science ne connaît pas de limites. Je lui fais part de mon étonnement, auquel il répond avec un sourire amusé. En réalité, le minage des crypto-monnaies désigne les procédés de vérification des transactions du réseau bitcoin. Le calculateur cherche alors à résoudre une énigme mathématique et, s'il en obtient le résultat, il peut récupérer une partie des unités monétaires circulant dans le réseau sous forme de rétribution.

J'imagine cette énorme machine, creusant la terre à la recherche de métal brillant ou analysant l'eau d'une rivière. Un peu comme le chercheur d'or du XIX^e^ siècle passant au tamis le lit de sa rivière à la recherche de pépites minuscules. Le caractère aléatoire de ces trouvailles fait tout le charme de ces opérations mais agite aussi ma vision technique de l'informatique. Multi-tâche, producteur de chaleur, le calculateur m'apparaît soudain comme une machine désormais douée de conscience, échangeant un salaire en crypto-monnaie contre la réalisation d'opérations mathématiques de haut vol. Entrerions-nous déjà dans l'ère des robots conscients que, depuis des décennies, la science-fiction prophétise ? L'existence d'une monnaie en ligne, visible des seuls supercalculateurs, m'intrigue.

De retour à Paris, le récit de cette machine chercheuse d'or occupe toutes mes pensées. J'imagine un géant de fer articulé, empreint de mes lectures et de mes séries, une machine animée et engagée dans la résolution de son objectif suprême : créer de la valeur par sa seule activité informatique. Je m'empresse de lire

tout ce qui me passe sous la main au sujet de ces crypto-monnaies : littérature business et scientifique, articles de presse spécialisée ou généraliste, etc. Ma première impression est décevante. Le commentaire d'ensemble est souvent négatif, voire ouvertement critique. Les spécialistes ne semblent pas croire au développement massif de cette monnaie en ligne et prédisent l'essoufflement de l'engouement pour cette nouveauté.

Dans *Atlantico*, journal pourtant d'orientation libérale, le blogueur Jean-Pierre Chevallier présage même la mort prochaine du bitcoin, condamné à périr sous les coups des banques centrales et des champions bancaires nationaux. Depuis plusieurs siècles, les économistes du libertarianisme ont pourtant soutenu le développement des monnaies privées afin de limiter l'influence de la puissance publique dans l'économie monétaire, mais la crise économique et financière de 2008-2010 a étouffé l'enthousiasme initial face à l'émergence de la monnaie numérique. Désormais, les États et les banques centrales forment un front unique pour la défense d'un univers bancaire à la fois contrôlé et régulé. La place d'une monnaie privée s'en est donc trouvée fortement réduite.

L'idée de la désintermédiation bancaire, c'est-à-dire la fin des banques et le développement d'un échange direct entre deux acteurs du marché, n'est pourtant pas nouvelle. Le développement d'une économie pair-à-pair (*peer-to-peer* ou P2P en anglais) trouve ses racines dans la création de l'application américaine Napster, en 1999, qui permettait de partager librement de la musique en ligne entre des dizaines de millions d'utilisateurs connectés, sans l'intermédiation d'une plateforme d'achat et de vente de titres musicaux. Dès 1998, pourtant, dans un article scientifique, l'ingénieur chinois Wei Dai avait proposé de développer une crypto-monnaie en ligne, la *b-money*, « *un système de distribution anonyme et électronique* [permettant d'établir] *un schéma groupé d'utilisateurs digitaux sous pseudonymes se*

payant entre eux avec de la monnaie numérique et se liant par des contrats sans aucune aide extérieure[2] ».

Dix ans plus tard, en 2009, naissait le premier système de crypto-monnaie décentralisée et numérique, le bitcoin, prouvant toute l'actualité des théories économiques de Friedrich Hayek sur la privatisation de la monnaie. Le rêve de toute une génération était enfin achevé et une nouvelle monnaie était battue, sous les coups de claviers, au cœur des processeurs. Son inventeur, un développeur caché sous le pseudonyme Satoshi Nakamoto, a depuis contribué à l'amélioration de la crypto-monnaie avant de passer la main à d'autres développeurs du système au milieu de l'année 2010.

Portée et limites de la crypto-monnaie, l'offensive des banques

Outre le ton très critique d'*Atlantico*, la presse française s'est montrée très prudente, voire sceptique, à l'égard du phénomène des crypto-monnaies. Dans *Marianne*, les journalistes Alexandre Coste et Hervé Nathan évoquaient ainsi une « *arnaque géante sur internet* », reprenant pêle-mêle les commentaires narquois des administrateurs des banques centrales. Un responsable de la Banque centrale européenne (BCE), cité dans l'article, dénonçait ainsi le manque de stabilité de cette nouvelle monnaie : « *La monnaie doit permettre d'acquérir n'importe quel bien et service, aujourd'hui et dans l'avenir* […] Il *faut donc qu'elle soit stable. Mieux vaut pour cela avoir des euros ou des dollars régulés par une banque centrale, que ces machins*[3]*…* » !

Pourtant, dans les faits, la BCE et ses homologues nationaux n'éprouvent pas que du dédain pour le bitcoin, elles sont aussi très inquiètes de la portée de ses effets réels sur l'économie. En

mars-avril 2013, au moment de la fermeture des banques et frontières chypriotes après l'édiction du plan de sauvetage de la zone euro, l'usage des bitcoins avait progressé de 700 % en une seule semaine et plus de 6 milliards d'euros auraient ainsi quitté la petite île méditerranéenne sous format numérique. La BCE avait alors tiré la sonnette d'alarme auprès de l'ensemble des banques centrales européennes sur l'usage de cette monnaie virtuelle, accusée de profiter de la crise économique et financière locale pour prospérer.

Il faut reconnaître que, depuis sa création en 2009, le bitcoin a su tirer pleinement partie des crises économiques et financières pour se substituer aux monnaies officielles. En mars 2015, l'Argentine et le Venezuela, également soumis à de fortes agitations économiques et financières, enregistraient 12 000 usagers du système bitcoin et des échanges d'environ 1,5 million de dollars par mois. En juin 2015, après l'annonce de la fermeture des banques grecques dans l'attente d'un référendum national sur l'avenir du pays, les échanges locaux en bitcoins avaient augmenté de 300 % et le cours du bitcoin avait bondi de 20 points (de 215 à 235 euros) en une seule semaine.

L'idée de cette monnaie invisible inquiète aussi parce qu'elle rappelle le traumatisme du scandale Madoff aux États-Unis. En juin 2009, le financier Bernard Madoff avait escroqué une vingtaine d'investisseurs de taille internationale à hauteur de plusieurs dizaines de milliards de dollars. L'ancien patron du Nasdaq, le deuxième plus important marché d'actions aux États-Unis, avait mis en place une « pyramide de Ponzi », un système dans lequel il se servait des investissements de ses nouveaux clients pour payer les intérêts des anciens. L'escroquerie n'avait rien de réellement innovant, elle tire d'ailleurs son nom d'un banquier italien établi à Boston dans les années 1920, Charles Ponzi. L'ampleur des sommes concernées devait toutefois faire date.

En 2013, la presse américaine révélait un nouveau « scandale Madoff » après qu'un trader américain, Trendon Shavers aussi connu sous le nom de Pirateat40, a été arrêté pour escroquerie de type pyramide de Ponzi. Shavers avait repris la recette de Madoff, appliquée au système des bitcoins, promettant à ses investisseurs un intéressant taux de rendement journalier de 1 % mais couvrant les intérêts de ses anciens investisseurs par le capital d'investissement de ses nouveaux clients. Après avoir réuni une coquette somme de 5 millions de dollars, le jeune homme avait tout simplement disparu dans la nature. Shavers fut finalement arrêté en 2014 et emprisonné pour six ans à partir de 2015, mais l'affaire avait causé ses torts. Les banques traditionnelles avaient de nouveau des arguments de poids pour critiquer le bitcoin.

Le bitcoin, une nouvelle « monnaie-fiat » ?

Rêve fantasmé d'un argent lavé de tout péché pour les uns, système dangereux et frauduleux pour les autres, le bitcoin révèle toutes les passions sur son passage. En octobre 2013, dans un billet de blog, l'économiste français Paul Jorion estimait que la plupart des promoteurs du système bitcoin sont « *des patrons de boîte de nuit, des joueurs professionnels de poker* [...] *des gamins facétieux* ». Cette accusation simpliste est probablement imputable à la figure d'Éric Larchevêque, ancien joueur de poker professionnel, activité qu'il arrête pour devenir un entrepreneur remarqué dans le secteur bitcoin, avec la Maison du Bitcoin et plus tard Ledger. Dans les faits, le manque de régulation de la monnaie numérique conduit, il faut le reconnaître, à certains excès et le bitcoin est soupçonné d'être présent dans les secteurs du blanchiment de l'argent, de la drogue, voire du financement des activités terroristes.