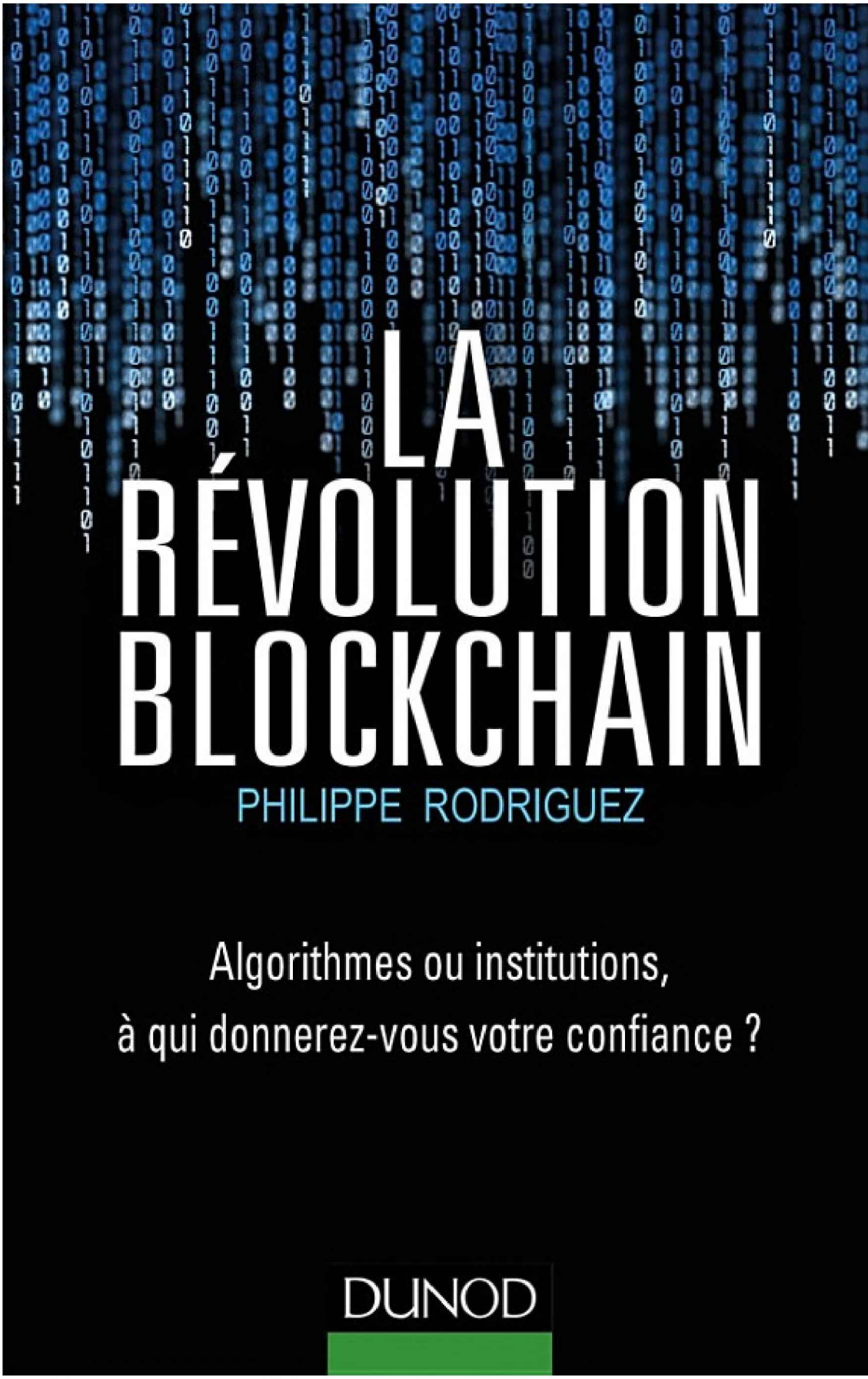

LA
RÉVOLUTION
BLOCKCHAIN
PHILIPPE RODRIGUEZ
Algorithmes ou institutions,
à qui donnerez-vous votre confiance ?
DUNOD

Mise en page : Belle Page
Consultez nos parutions sur www.dunod.com

Dunod, 11 rue Paul Bert, 92240 Malakoff

ISBN 978-2-10-076403-7

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.

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]

N*ovembre 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 XXI^e^ 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. Multitâche, 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.

Pour acquérir ses lettres de noblesse, ses détracteurs voudraient que le bitcoin soit intégré dans un système légal et judiciaire. La Cour de justice de l'Union européenne (CJUE) a donc amorcé ce processus en octobre 2015, en définissant le bitcoin comme une « devise virtuelle ». Aux États-Unis et en Russie, les parlements des deux pays travaillent à la rédaction et au vote d'une loi encadrant l'usage économique et financier du bitcoin, mais les débats traînent en longueur, compte tenu des enjeux présents. Au fond, ce que veulent les banques, c'est que les crypto-monnaies aient leur régulateur, leur police et leurs règles de sanctions. Actuellement, pour l'institution bancaire, le bitcoin n'a pas plus de valeur qu'un billet de Monopoly, un billet certes plus moderne mais un billet de jeu quand même.

En m'intéressant aux monnaies et au cours de mes nombreuses

lectures, j'ai croisé de manière récurrente le terme de « monnaie-fiat », qui désigne une monnaie reconnue par un État comme légale, sans être basée pour autant sur une valeur intrinsèque. Elle doit son nom à l'expression latine « *fiat* », signifiant « qu'il en soit ainsi », car c'est l'État ou la banque centrale qui définit la valeur, la légalité ou encore l'existence de cette monnaie. *Fiat Lux*, pouvait-on lire dans la Bible ; *Fiat Money* pourra-t-on peut-être demain lire au frontispice des banques centrales. Le bitcoin est-il cette monnaie-fiat, n'apparaissant de nulle part, ou sa liberté totale à l'égard des institutions en fait-elle, au contraire, une monnaie individuelle au sens où elle repose sur le consentement de chacun à son développement ?

Alors que la plupart des monnaies ont historiquement été évaluées par rapport au cours de matériaux précieux (or, argent, cuivre), la monnaie-fiat voit son cours imposé par la puissance publique, en échange d'une obligation légale de l'utiliser. Pour l'économiste libéral français Jacques Rueff, ce concept est donc « un néant habillé en monnaie », peu digne de l'intérêt des économistes. Pourtant, appliqué au système bitcoin, ce principe de monnaie-fiat permettrait de légitimer l'émission d'une crypto-monnaie, mais les implications d'une telle décision seraient vastes et agiteraient les statu quo difficilement établis de la finance, de la démocratie, et des transitions écologique, démographique, voire numérique.

À la rescousse du bitcoin, des utilisateurs et de grands économistes

Contre l'armée de ses détracteurs, le bitcoin a aussi ses défenseurs, nombreux et puissamment armés. Dès les années 2000, le fondateur de Microsoft, Bill Gates, a pris fait et cause pour la monnaie numérique. En 2014, l'homme le plus riche du monde a même été plus loin, affirmant que le bitcoin valait plus que les monnaies aujourd'hui en cours de circulation. « *Le bitcoin est une monnaie fantastique*, a-t-il affirmé au journaliste Erik Shatker, *car vous n'avez pas besoin d'être physiquement au même endroit pour réaliser une opération et, pour des opérations d'une certaine taille, la monnaie physique peut être méchamment inconvéniente. C'est un tour de force technologique*[4] *!* »

Aux côtés des personnalités du monde numérique, certains économistes ont également accordé leur soutien au bitcoin. L'économiste libanais Nassim Nicholas Taieb, conseiller spécial auprès du Fonds monétaire international (FMI), fait ainsi partie de ses défenseurs. En 2007, dans son ouvrage *Le Cygne noir*, il développe la thèse de l'épiphénomène de crise, qui ne peut que très rarement se réaliser mais a des conséquences terribles en cas d'application. Reprenant les travaux du mathématicien britannique Bertrand Russell, il explique que notre système économique et financier est comme une dinde, engraissée chaque jour en vue des fêtes de fin d'année, qui pense être traitée royalement chaque jour de sa vie mais qui, sans le savoir, se rapproche inéluctablement de son exécution prévue de longue date.

Face à ce destin fataliste, Taieb veut croire que le bitcoin peut être une solution pour réinventer le système économique et financier. « *Le bitcoin est le début de quelque chose de grandiose*, écrit-il sur son blog, *une monnaie sans gouvernement, quelque chose d'à la fois nécessaire et impératif*. [...] *Néanmoins, nous avons besoin d'un long moment pour établir notre confiance dans cette nouvelle monnaie*[5]. » Il faut donc laisser du temps au temps, ainsi qu'aime le dire Philippe Delmas, retrouver une lenteur que les marchés financiers nous ont fait perdre de vue et reposer à plat ce que nous prenons, parfois naïvement, pour acquis.

Parmi les grands économistes, Milton Friedman (mort en 2006) avait également prédit l'émergence du bitcoin. En 1999, à l'occasion d'une interview donnée à la National Taxpayers Union (NTU) aux États-Unis[6], il avait ainsi affirmé que « *le numérique serait amené à devenir une des forces majeures de l'économie de demain, réduisant le rôle des gouvernements* ». Une seule chose manquait alors, « un cash électronique de confiance ». En septembre 2012, à New York, les créateurs du système bitcoin ont posé les premières pierres de la Fondation Bitcoin, une organisation de relations publiques dédiée à la promotion de la monnaie numérique. C'est notamment elle qui, en 2014, a retrouvé cette interview de Friedman et en a assuré une large audience sur les réseaux sociaux.

La marche inéluctable du système bitcoin

Derrière le système bitcoin, c'est toute une industrie des applications et des protocoles informatiques qui s'est mise en marche. Il sera donc difficile de « désinventer » cette nouvelle monnaie et le monde devra conséquemment s'y adapter. « *Pour que tout reste comme avant, il faut que tout change !* », annonçait laconiquement Tancrède dans le film *Le Guépard* de Luchino Visconti (1963). Les banques centrales n'auront donc pas le choix, elles devront s'adapter, développer des algorithmes pour pouvoir répondre à la nouvelle demande et lutter contre la concurrence des crypto-monnaies.

La technologie blockchain à la base des crypto-monnaies a créé un système dans lequel la valeur du bitcoin dépend pleinement de l'offre et de la demande. Pour les plus optimistes, ce nouveau régime économique de la monnaie pose les bases d'un rapport repensé et entièrement dématérialisé à l'argent, mais, pour les plus pessimistes, il s'apparente à une bulle économique et financière, menaçant d'exploser à tout moment, plongeant alors le monde dans une nouvelle crise d'ampleur mondiale. Une angoisse terrorisante alors que les effets de la crise de 2008-2010 se font encore sentir dans les économies nationales.

Rien ne semble, pour autant, pouvoir stopper le développement de la blockchain, cette technologie porteuse du bitcoin, en constante évolution et régulièrement placée au-devant de l'actualité. Chaque jour, de nouvelles applications voient le jour ; chaque jour, elles démontrent que l'ouverture et la transparence sont des qualificatifs applicables au domaine de l'économie de la finance ; chaque jour, elles touchent de nouveaux utilisateurs et accélèrent la course du développement mondial des technologies numériques. Le vent de l'innovation souffle dans son dos et des milliers de start-up plantent leur graine dans le champ fertile de la blockchain. Elles seront, demain, des entreprises à succès, peuplant le monde des échanges internationaux.

En France et en Europe, le phénomène a aussi donné lieu à l'émergence de quelques centaines de start-up, souvent inspirées par de jeunes créateurs ambitieux. Ancrées dans le monde d'Internet, ces nouvelles entités se développent sur un marché des services dans lequel la confiance entre le prestataire et le client est l'élément

fondamental. Notre pays a, aujourd'hui, la possibilité de développer ce segment de son économie, d'encourager l'émergence de PME et TPE engagées dans ce filon technologique, de se spécialiser et d'acquérir, à moyen terme, une compétitivité hors prix nécessaire à l'avenir de notre croissance.

En janvier 2014, la commission des Finances du Sénat a d'ailleurs organisé une audition sur les enjeux liés au développement des monnaies virtuelles, invitant notamment Gonzague Grandval, président de Paymium, représentant de la communauté blockchain de France. Nos élus ont certes fait preuve d'une écoute attentive et responsable, mais ce genre d'exercice n'est pas suffisant pour rassurer nos entreprises et encourager la réflexion sur ces sujets d'innovations. En mars 2016, encore, la Commission supérieure du service public des Postes et des Communications électroniques de l'Assemblée nationale et du Sénat a organisé un colloque consacré à la technologie blockchain, preuve d'une véritable attention de nos parlementaires sur ces questions de transformation du pays.

Cette grand-messe a ainsi permis de sensibiliser de nombreux parlementaires et hauts fonctionnaires à la technologie blockchain. La machine était lancée et le flot de cette curiosité irriguera, demain, les champs de l'économie, de la finance et de la société civile. Ce colloque a aussi de nouveau mis sur la table la question de l'encadrement juridique des nouvelles technologies, notamment des crypto-monnaies comme le bitcoin. Il s'est donc conclu par une invitation à attirer et retenir en France les meilleurs talents internationaux des technologies blockchain, afin de créer un écosystème favorable au développement de ce segment de l'économie dans notre pays.

Adopter la blockchain, une procédure relativement longue

Parce qu'elle repose, d'abord, sur une relation de confiance entre les prestataires et les clients, la technologie blockchain suppose un temps long d'adoption. Les analystes de cette nouvelle technologie s'accordent à dire que la maturité de la technologie blockchain sera atteinte plus rapidement que celle d'Internet ou du Web. Développé à la

fin des années 1960, Internet n'avait ainsi connu son essor qu'après le développement du protocole TCP/IP en 1977. À l'identique, créé en 1991 avec le protocole HTLM, le Web n'a su s'imposer comme navigateur qu'en 1994. Il aura fallu encore quelques années supplémentaires pour que, sur la base de nombreux protocoles HTML compulsés, le Web soit reconnu comme un navigateur d'ensemble abouti.

À l'époque, le lancement du mail, basé sur un protocole SMTP créé en 1983, avait également dû emprunter de nombreux chemins détournés avant de s'imposer comme messagerie életronique de base au milieu des années 1990. De longues années à patienter, mais un succès fantastique à la clé. La technologie mail a tout simplement remplacé les autres moyens de communication numérique (messageries propriétaires, fax, télex). En 2015, le monde comptait ainsi 4,4 milliards de comptes email, 75 % à usage personnel et 25 % à usage professionnel. Un succès écrasant que la technologie blockchain ambitionne de conquérir aussi.

La maturité de la technologie blockchain, elle, est à attendre à l'horizon 2018-2020, si l'on reprend notre analogie avec l'email et en tenant compte d'une accélération des adoptions. Dans *The Business Blockchain: Promise, Practice and Application of the Next Internet Technology* (2016), William Mougayar estime ainsi que la technologie blockchain connaîtra une « *adoption graduelle, démarrant par les développeurs, puis les entrepreneurs, ensuite les plus technophiles des cadres d'entreprise, pour enfin intéresser les organisations qui verront le changement arriver et la demande de la société pour ces changements se renforcer de jour en jour. Alors, et seulement alors, seront conquises les organisations qui résistent aujourd'hui à ces changements*. »

La révolution blockchain, une matriochka numérique

La révolution blockchain n'est pas un simple épiphénomène technique ou technologique de l'évolution de nos économies et de nos sociétés. Elle s'inscrit, au contraire, dans de grandes révolutions de notre temps,

qui sont autant de défis pour nos modes de consommation et de vie. Le monde change autour de nous et la technologie ne fait que s'adapter aux nouvelles réalités qui nous entourent. Trois transitions s'opèrent aujourd'hui, de manière nécessaire mais aussi délicate : la révolution numérique fondée sur l'émergence de nouvelles technologies, la révolution démographique basée sur l'évolution de la population mondiale et ses effets sur notre consommation des ressources naturelles, et la révolution écologique face à l'épuisement des ressources et aux effets du changement climatique.

La révolution numérique, d'abord, a nourri le développement de nombreuses technologies pour nous rapprocher, nous amener à aller plus vite et plus loin dans nos relations humaines. Cependant, ce modèle n'est pas abouti et atteint aujourd'hui le cœur de nos libertés fondamentales : il viole nos vies privées en diffusant notre intimité sur le Net, il endommage la libre propriété des données, exposées sur des marchés d'achat et de vente, comme n'importe quel autre bien ou service, bref il n'a pas su suffisamment intégrer les considérations humaines dans son raisonnement mécanique.

L'inventeur du protocole HTML, le Britannique Sir Timothy John Berners-Lee, est très critique des récentes évolutions du Web et appelle à un retour aux origines de l'outil numérique. Des valeurs d'indépendance, de neutralité, de sécurité des internautes devraient ainsi se trouver au fondement du pacte numérique entre l'opérateur et l'utilisateur de l'outil numérique. Début juillet 2016, dans une tribune vibrante cosignée avec deux amis, professeurs de droit à Harvard et à Santa Barbara, Berners-Lee a appelé l'Union européenne à consacrer la neutralité du Net et à dénoncer la récente législation européenne en la matière, adoptée en octobre 2015. En conclusion de cet appel, les trois hommes exhortaient leurs lecteurs à faire usage de leur droit d'opposition en ligne. Une nouvelle forme d'acte démocratique en quelque sorte.

La révolution démographique, ensuite, agite tout autant notre monde et notre siècle. Si elle prend des formes différentes dans les pays industrialisés et dans le reste du monde, elle témoigne dans tous les cas d'une urgence à agir pour mieux intégrer l'augmentation de l'espérance de vie en Occident et le rythme des naissances dans les pays en développement. Pour intégrer ces citoyens, il faut fonder un

nouveau contrat social, basé sur de nouvelles règles de solidarité. Le numérique aura son rôle à jouer dans ces révolutions, en analysant davantage les besoins des citoyens et en anticipant leurs demandes, voire en développant des monnaies thématiques, complémentaires à la monnaie d'usage dans chacun des domaines de l'économie nationale.

En Europe, l'émergence d'une économie des personnes âgées et dépendantes (*silver economy*) est ainsi un fait concret depuis plusieurs années. En 2030, un tiers des Français auront plus de 60 ans. Pour accompagner nos seniors, il faudra, demain, savoir mieux surveiller l'évolution de leur santé, mieux accompagner leur maintien à domicile, en d'autres termes mettre en place les outils nécessaires à la prolongation de leur vie économique et sociale. Selon le ministère de l'Économie et des Finances, ce segment de notre économie représentait déjà 92 milliards d'euros par an en 2013 et pourrait même atteindre 130 milliards d'euros en 2020. Le numérique sera donc un véritable atout dans cette transformation de notre économie : objets connectés, outils thérapeutiques, télésurveillance de patients à domicile, téléassistance, domotique, etc.

La révolution écologique, enfin, finit de poser une chape de plomb sur ce début de XXI^{e} siècle. La pollution à outrance de nos sociétés industrielles et les effets des économies émergentes sur l'environnement ont dégradé notre écosystème, au point que nos plus brillants scientifiques anticipent une hausse de +4 °C des températures mondiales à l'horizon 2100. L'Accord de Paris, signé à l'issue de la COP21, en décembre 2015, a certes enrayé ce mouvement et fixé un objectif maximum d'une hausse des températures de +2 °C à l'horizon 2100, mais l'urgence est là. Le niveau des mers monte, l'air devient irrespirable dans les villes, les campagnes s'assèchent. Si nous n'agissons pas, nous sommes à l'aube d'une nouvelle extinction de masse du règne animal et végétal : selon un rapport du World Wide Fund (WWF), 58 % des espèces d'animaux sauvages ont déjà disparu depuis 1970 !

Comme pour la révolution démographique, le numérique sera un instrument majeur de notre action contre le changement climatique. Pour changer, il nous faut d'abord apprendre à mieux et à moins consommer. Les réseaux intelligents (*smart grids*) font partie de cette palette d'outils qui nous accompagneront dans nos changements de

comportement. L'optimisation du chauffage, de l'éclairage ou des transports, les solutions de géolocalisation des transports publics, les systèmes d'annuaires numériques de la biodiversité (comme celui mis en place par la loi Biodiversité de juillet 2016) sont autant de solutions dans lesquelles les technologies vertes (*greentechs*) ont un rôle essentiel. À ce titre, le partage des données publiques (*open data*) sera une règle fondamentale pour mieux apprécier la complexité de notre environnement. Notre méconnaissance d'une partie de la faune et de la flore nous dessert, car la biodiversité est un gisement de ressources pour l'avenir.

Pour répondre à ces défis de taille, deux transitions sociétales doivent être accomplies à court terme : la transition monétaire et la transition démocratique. En effet la multiplication des crises bancaires et monétaires a non seulement montré l'essoufflement de notre modèle économique général, mais elle a aussi interrogé la véritable souveraineté des États et de nos gouvernements face aux pouvoirs de l'argent et de la finance. Au fond, sur le modèle de la théorie du cygne noir de Nassim Taieb, ces crises à répétition nous ont fait considérer l'idée que notre modèle économique pouvait avoir une fin en soi et qu'il fallait, en conséquence, savoir réfléchir à sa mutation à moyen terme.

Afin de mener à bien la transition monétaire et d'envisager une évolution de la dette mondiale, il faudra consacrer les transferts de fonds entre les migrants et leurs familles restées dans les pays en développement, voire accompagner l'effacement progressif des dettes publiques des pays pauvres. L'annulation de dette n'est pas une idée nouvelle, elle remonte en effet à la Bible chrétienne, mais l'accroissement rapide des dettes publiques de certains pays (parfois au-delà de 100 % du produit intérieur brut [PIB] annuel) pose la question de leur annulation. En 1998, à l'occasion du G8 de Birmingham, la question de l'effacement des dettes publiques a été posée sur la table des négociations internationales à la suite de manifestations publiques.

Différentes initiatives d'annulation ou de réduction des dettes publiques ont ponctué les deux décennies suivantes, souvent à l'appui de programmes de la Banque mondiale et du Fonds monétaire international, mais leur efficacité reste discutable. Un rapport du Trésor de mars 2016, consacré à l'Initiative d'effacement des dettes des pays

pauvres très endettés (PPTE) note ainsi que, vingt ans après la mise en place de cette démarche, ces pays se sont pour la plupart ré-endettés faute de mobilisation de l'épargne nationale et d'investissements dans les secteurs stratégiques de leur modernisation. La remise en marche d'une économie nationale n'est donc pas seulement une affaire de dettes, mais aussi de réformes sectorielles et structurelles.

Parallèlement, une étude de la Banque mondiale d'avril 2016 montre que le montant des fonds transférés des migrants vers les pays d'origine a très peu augmenté en 2015, laissant craindre un appauvrissement des ménages des pays en développement et un effondrement économique de ces pays. Cette évolution de l'économie des transferts peut être aussi lue sous le prisme du recours aux nouveaux outils numériques d'échanges monétaires. Des trappes à pauvreté menacent donc ces millions de familles, déjà confrontées à des problèmes de malnutrition ou d'accès limité aux services d'éducation et de santé. Pour toutes ces personnes, il faudra aussi développer l'inclusion financière, c'est-à-dire l'offre de services financiers à faible coût (assurances, épargne, crédit à court et long terme, hypothèques).

Parallèlement, pour lutter contre l'abstention et la désaffection des citoyens à l'égard de l'exercice démocratique, il faudra réinventer notre modèle politique et replacer le pouvoir décisionnel au plus près de l'individu. Contre l'idéal centralisateur de la révolution, notre époque a besoin d'une forme polycentrique de pouvoir politique, dans laquelle chaque individu est un centre de gravité unique de l'action publique – ainsi que les humanistes le souhaitaient, l'homme est pleinement replacé au cœur des questionnements politiques. La construction d'un mille-feuille administratif rend illisible le système politique actuel et nos concitoyens rejettent un ensemble politique dont ils ne comprennent plus le sens de l'action. Il s'agit donc d'améliorer la gouvernance politique en rétablissant quelques lignes directrices claires à l'action publique et en refondant le pacte citoyen autour d'une plus grande participation des électeurs.

Réinventer un nouveau paradigme économique est encore possible !

Le développement de l'économie collaborative et circulaire, l'expansion des licences libres (*open source*), les élans participatifs de la finance, à l'image du financement participatif (*crowdfunding*), sont autant de promesses en l'avenir. Notre société est capable d'évoluer, elle dispose des technologies nécessaires à sa transformation, il lui reste à donner l'impulsion politique vitale. Pour exemple l'impression 3D a ainsi révolutionné notre façon d'appréhender la production industrielle et nous invite à repenser en profondeur notre politique industrielle.

Au sein de la banque d'affaires pour start-up Avolta Partners, avec mes associés fondateurs Patrick Robin et Arthur Porré, nous discutons souvent pour savoir quelles sont ces nouvelles « meta-innovations » qui ont la puissance de produire un grand nombre d'innovations. En premier lieu, nous sommes persuadés que nous tournons la page du capitalisme de propriété, de centralisation pour aller ou revenir à l'idée de « communs », un concept à la fois germinal et prometteur que l'on retrouve dans un grand nombre d'innovations majeures : logiciels en *open source*, intelligence collective, sites communautaires, et même publicité par les réseaux sociaux.

C'est un bon économique de près de dix siècles en arrière que nos sociétés opèrent : nous revenons à l'idée des champs pastoraux « communautaires », dans lesquels chacun pouvait emmener paître ses bêtes à l'époque médiévale. Loin d'être une régression, ce changement de paradigme nous rappelle ce que l'humanité a de collectif, ce qu'elle ne peut pas marchander et ce qu'elle doit, tout au contraire, librement partager : l'air, l'eau, les espaces sociaux, les savoirs, bref, la vie. Une transition réussie de notre économie et de notre société passera donc par une re-sacralisation des communs, ces richesses inscrites au patrimoine de l'humanité. C'est une nouvelle philosophie de vie qu'il nous faut, tous ensemble, adopter !

Pour initier ce mouvement, en 2014, plusieurs personnalités de l'écosystème de bitcoin, se sont réunies dans le sous-sol voûté de l'incubateur qui accueillait la start-up Paymium pour lancer l'organisation Bitcoin France qui aiderait les entrepreneurs souhaitant défendre et faire connaître la technologie blockchain.

Les acteurs économiques commencent à s'y prêter – les organisations privées non marchandes ont fait un premier pas en actant une plus grande décentralisation de leur gouvernance. Ce sera, demain, le tour

des entreprises privées, puis des organisations publiques, voire régaliennes, d'amorcer ce virage vers une plus grande participation des citoyens dans le cadre d'un modèle davantage décentralisé. Une économie du partage, de la participation, de la collaboration pourra alors émerger, fondée sur une gouvernance de l'ensemble des participants et sur une infrastructure à la fois numérique et technologique. La blockchain sera le rouage essentiel de cette nouvelle économie.

Cet essai ambitionne de tracer la route à cette transformation de nos sociétés. Développer la blockchain sera une grande aventure humaine, à laquelle les hommes et les femmes du monde entier participeront. Les développeurs, les hackers, les informaticiens, les mathématiciens, mais aussi les économistes, les entrepreneurs et les politiques auront tous un rôle à jouer dans cette évolution de notre communauté, car le pari n'est pas seulement économique et politique, il est aussi technologique et social. Il ne s'agit pas d'imposer un nouveau mode de vie, mais de révolutionner nos pratiques culturelles sur le fondement de l'assentiment de chacun.

D'abord, cette perspective m'amènera à commenter le cours de l'histoire des technologies numériques, de la machine de Turing pendant la Seconde Guerre mondiale, décodant les messages secrets des armées nazies, aux fermes de serveurs chinois au XXI^{e} siècle, résolvant des énigmes mathématiques en échange de crypto-monnaies. Cette transformation de l'outil numérique s'est d'abord réalisée par un acte de confiance : confiance en la machine, confiance en sa capacité à changer notre mode de vie, confiance enfin en sa capacité à changer le monde. C'est sur cette route que nous avons croisé les « cypherpunks », à la frontière de l'informatique et de la révolution politique.

Ensuite, j'analyserai les évolutions économiques liées à ces nouvelles technologies informatiques. Je tâcherai d'expliquer comment un nouveau protocole informatique peut désormais servir de monnaie d'échange ou de moyen de paiement, comment encore la communauté mondiale s'est enthousiasmée de l'émergence des crypto-monnaies et de leur promesse de créer un système monétaire sans autorité centrale. Au-delà des horizons utopiques de la réflexion, je reviendrai sur les théories économiques les plus sérieuses, prédisant l'enracinement des

crypto-monnaies comme monnaie complémentaire de notre système bancaire contemporain.

Comprendre ces adaptations de notre économie, ce sera aussi comprendre comment la technologie blockchain fonctionne. Bien entendu, ce plongeon au cœur des technologies se fera pas à pas, mais il est important pour comprendre la révolution opérée par l'émergence des crypto-monnaies, ses impacts, ses fonctionnalités et ses perspectives d'évolution à moyen et long terme. Pour cela, nous voyagerons à travers l'écosystème des start-up qui, aujourd'hui et partout dans le monde, font vivre la blockchain avec des idées réalistes et une capacité d'exécution forte. Ces révolutions économiques et techniques agissent dès à présent sur la finance, la société de confiance, mais aussi la politique dans son ensemble, comme réponse à la crise démocratique.

Enfin, en termes de conclusion, j'interrogerai notre capacité à épouser ces nouveaux défis et à nous adapter. Nous nous attarderons sur les moteurs et les freins des années à venir. Le Web et les nouvelles technologies numériques ont changé le monde en permettant la diffusion de contenus à un coût marginal faible, voire nul, transformant notre rapport à la propriété. La blockchain interroge donc la conservation et le transfert des valeurs dans leur essence même. C'est à l'issue du panorama de la blockchain seulement que nous pourrons dresser ces conclusions analytiques.

Embarquez, si vous le voulez bien, pour ce fabuleux voyage dans l'univers de la blockchain. Qui que vous soyez, néophyte ou expert, observateur du lancement du Web dans les années 1990 ou jeune curieux des nouveautés numériques, cet essai se promet de vous donner les clés de lecture fondamentales pour la compréhension de la blockchain et de ses ambitions pour notre économie, notre société et notre système politique. Attachez vos ceintures et en route. Même si, comme dirait le Doc Brown dans *Retour vers le futur*, là où nous nous rendons… il n'y a pas de route !

Des maths et des hackers

« *Le bitcoin doit nous permettre d'accéder à une monnaie décentralisée, appartenant pleinement au peuple*. »

GAVIN ANDRESEN, *lead developer* de Bitcoin, 2011

La première application grandeur nature de la technologie blockchain s'est faite avec le développement des crypto-monnaies. En effet, l'idée d'une « chaîne de blocs » – c'est la traduction littérale de blockchain – dotée d'une technologie cryptographique et décentralisée, était une fondation essentielle à l'édiction et au fonctionnement d'une nouvelle monnaie numérique, sans organe de contrôle central. Blockchain et bitcoin sont ainsi deux frères jumeaux, longtemps confondus, aujourd'hui reconnus dans toutes leurs différences.

Les crypto-monnaies ne sont pas nées du jour au lendemain. Elles se sont nourries des rêves et des obsessions de plusieurs centaines de chercheurs, qui ont passé quelques décennies à imaginer, inventer et travailler sur les problèmes majeurs de cette solution innovante. Comme toute monnaie, la principale condition de sa réussite était la confiance de ses utilisateurs en sa fonctionnalité. Il fallait convaincre les entreprises, les ménages et les structures publiques de son sérieux. Le succès des crypto-monnaies s'explique ainsi par la très forte adhésion de la communauté blockchain et par les ambitions altermondialistes de nombreuses populations, et ses limites, par la résistance farouche des milieux bancaires et institutionnels et le manque de confiance en la stabilité de toute nouvelle devise.

Revenons toutefois quelques années en arrière. Trois défis théoriques s'imposaient à l'émergence des crypto-monnaies : la propriété intellectuelle des infrastructures numériques, la protection de notre droit à la vie privée et la gouvernance de cette nouvelle monnaie. Pour y

répondre, la technologie blockchain a mobilisé des apports technologiques : l'*open source*, d'une part, la cryptographie, d'autre part. Les crypto-monnaies se sont ainsi appuyées sur les annuaires et plateformes de partage de données numériques pour mettre en œuvre les fonds baptismaux de l'infrastructure monétaire. Plus qu'un outil, les crypto-monnaies ont ainsi fait appel à une philosophie de vie, sur le plan technologique et sur le plan sociétal.

Elles ont aussi fait un usage régulier de la cryptographie et de ses outils, notamment de l'encodage des messages et des propriétés des utilisateurs, pour créer un système monétaire dans lequel l'identité de chaque acteur est entièrement tenue secrète. J'y reviendrai, plus en détail, plus loin dans notre livre. Dès les années 1980, le mouvement anarchiste cyberpunk/cypherpunk s'est ainsi engagé dans l'activisme en ligne, sous couvert d'anonymat, développant l'usage de la cryptographie numérique. Ses représentants ont largement concouru au développement de technologies d'encryption, de sécurisation des échanges de données, et ont posé les fondements de la cryptographie moderne.

Enfin, dans une logique de rejet du système existant, les crypto-monnaies ont voulu créer une monnaie sans autorité centrale de régulation. Elles ont donc cherché, ainsi que l'entrepreneur français Pierre Noizat l'a noté, à créer « une monnaie libre » de toute forme de contrôle. Libre de toute contrainte administrative ou politique, libre d'établir sa valeur en fonction de la seule relation entre l'offre et la demande, libre encore de toutes les contraintes imposées par un système global de supervision, régulièrement et ouvertement dénoncé. Celui d'une finance mondialisée et mal régulée, soutenant les plus riches et desservant les plus miséreux.

Aux origines de la cryptographie moderne, le mythe Turing

L'analyse des messages cachés, la cryptanalyse, est une science antique, déjà utilisée par les Grecs et les Romains, plusieurs millénaires avant notre ère, comme art de révéler ce qui était caché ou ce qui avait disparu, notamment les messages codés en temps de guerre. Au

XIXe siècle, l'art de cacher des messages, la cryptographie, a changé pour investir le champ du mystère et de la mort, en raison de sa parenté avec le mot « crypte ». Les œuvres littéraires de l'écrivain américain Edgar Allan Poe ont ainsi fait connaître au grand public cette tradition cryptographique et l'auteur a lui-même entretenu des échanges cryptographiques avec ses lecteurs.

Avec les guerres mondiales du XXe siècle, la cryptographie connaît un essor formidable en s'appliquant à de nouveaux formats. Pendant la Première Guerre mondiale, les Allemands cryptent de nombreux télégrammes destinés à leurs forces armées et les puissances alliées déploient plusieurs équipes polyglottes de cryptanalyse des messages codés arrachés à l'ennemi. L'affaire du télégramme Zimmermann de janvier 1917 témoigne, d'ailleurs, de l'importance fondamentale de ces discussions codées dans le cours de la guerre. Bien que souvent efficaces, elles souffraient néanmoins d'une lenteur du processus d'analyse, long de plusieurs heures, alors que la transmission du message était, elle, devenue quasi instantanée avec les nouvelles technologies.

En 1919, l'ingénieur néerlandais Hugo Alexander Koch dépose un brevet de machine à chiffrage électromécanique, la machine Enigma. Bien que la société de production de la machine ait fait faillite, elle est immédiatement rachetée par le renseignement allemand pour encrypter ses télégrammes militaires. Dans la seconde moitié des années 1930, les services secrets français et polonais travaillent ensemble à décrypter les messages codés de l'Enigma, utilisée par l'Allemagne nazie, mais en vain. Avec le début de la Seconde Guerre mondiale, l'ensemble des alliés s'attachent donc à faire une priorité de la cryptanalyse des messages allemands afin d'anticiper les mouvements de l'ennemi.

En août 1939, à peine un mois avant le début de la guerre, l'École gouvernementale britannique du chiffre et du code (Government Code and Cypher School, GCCS) crée une base secrète à Bletchley Park, dans le Buckinghamshire, pour réunir les plus brillants cerveaux de la Couronne et déchiffrer les messages ennemis. Sous le nom de code de « Club de golf, de fromage et d'échecs » (Golf, Cheese and Chess Society), reprenant l'acronyme anglais GCCS, cette équipe d'analystes travaille sans relâche à écouter les transmissions allemandes et à les

déchiffrer. Armé des informations de l'ancien bureau du renseignement polonais et d'une machine dérobée à l'ennemi en 1939, le mathématicien britannique Alan Mathison Turing parvient finalement à casser le fameux code en 1941.

Pour cela, il construit une machine électromécanique de décryptage des messages obtenus, essayant aléatoirement plusieurs ensembles de clés potentielles de lecture et écartant toute clé en cas de contradiction logique. Une aventure brillamment racontée dans le film *Imitation Game* (2014) de Morten Tyldum, dans lequel l'acteur Benedict Cumberbatch prête ses traits au mathématicien anglais. Le premier outil de cryptanalyse automatique est né et baptisé « bombe de Turing, Welchman et Pendered », du nom de ses trois inventeurs. En 1942, Turing se rend aux États-Unis pour collaborer avec l'armée américaine à la construction de nouvelles « bombes » de cryptanalyse. Ces machines ont un rôle décisif dans la victoire des alliés pendant la Seconde Guerre mondiale.

Turing et les premiers ordinateurs

Au lendemain de la Seconde Guerre mondiale, Turing décide de poursuivre ses travaux sur les machines de cryptanalyse, au sein de l'équipe qu'il dirige alors au Laboratoire national de physique de Teddington, au Royaume-Uni. L'odyssée de la bombe de Turing, Welchman et Pendered a en effet fait naître de nombreuses vocations au sein de la communauté scientifique internationale. En juin 1945, le mathématicien américano-hongrois John von Neumann publie ainsi un rapport sur les calculateurs à programme, intégrant une mémoire de conservation des instructions et des données. Ce schéma de décomposition de la machine, l'architecture de von Neumann, pose les bases de l'informatique moderne et inspira à Turing une nouvelle réflexion sur ses travaux.

À l'automne 1945, Turing repart donc des travaux de von Neumann pour rédiger le projet d'un prototype de calculateur, l'*Automatic Computing Engine* (ACE). Pour des raisons personnelles, le mathématicien britannique abandonne néanmoins son ambition pour se consacrer à l'étude de la biologie. Toutefois, en 1948, à l'invitation d'un

ancien collègue du GCCS, il participe de nouveau au développement d'un des premiers ordinateurs au monde, doté d'une mémoire électronique, le *Manchester Automatic Digital Machine* (MADM), aussi connu sous le nom de Mark I, présenté au grand public en avril 1949. Produit en série par l'entreprise Ferranti, Mark I devient le premier ordinateur généraliste commercialisé au monde en février 1951.

Condamné dans une affaire de mœurs en 1952, à cause de son homosexualité, et soumis à un traitement de castration chimique, Alan Turing se voit retirer la direction de la programmation de Mark I. Mis à l'écart du grand projet de sa vie, il sombre dans une profonde dépression. De dépit, il finit par se suicider en juin 1954, croquant dans une pomme empoisonnée au cyanure. Son engagement et ses idées ont pourtant nourri les rêves d'une génération de scientifiques : du mathématicien britannique James G. Wilkinson, qui réalisa le prototype ACE de Turing, à l'entrepreneur américain Steve Jobs, qui fit, selon la légende urbaine, de cette fatale pomme au cyanure, le logo de la marque Apple. Finalement, en 2009, le gouvernement britannique de Gordon Brown reconnaît officiellement le traitement injuste du héros de guerre de la Couronne.

Si le mythe Turing porte encore son ombre sur l'informatique moderne, c'est surtout parce que le jeune mathématicien a participé au développement des technologies numériques contemporaines en posant les bases des théories sur l'intelligence artificielle. Avec son article « Computing Machinery and Intelligence » (publié en octobre 1950), il définit une épreuve, le « test de Turing », permettant de qualifier une machine de suffisamment intelligente pour tromper un groupe d'humain, encore utilisé de nos jours. En effet, si la technologie blockchain permet de stocker et d'échanger d'énormes volumes de données, l'analyse de ces données est le prochain paradigme technologique à atteindre et permettra de véritablement mettre en place un système de gestion autonome d'une crypto-monnaie.

La naissance de l'Internet distribué

En 1996, alors qu'Internet s'impose progressivement comme un outil grand public, un groupe de mathématiciens et d'informaticiens piloté par

les chercheurs américains George Woltman et Scott Kurowski lance le projet *Great Internet Mersenne Prime Search* (GIMPS). L'idée est de mettre l'informatique au service de la recherche mathématique, en mobilisant la capacité de traitement d'un réseau distribué d'ordinateurs, répartis dans divers endroits géographiques, dans le but de la résolution d'une immense énigme mathématique : la recherche des nombres premiers de Mersenne.

Un nombre premier de Mersenne est en effet un nombre qui est à la fois un nombre de Mersenne, c'est-à-dire le résultat de l'équation 2n-1, et un nombre premier, c'est-à-dire un nombre qui est divisible par 1 et par lui-même. En mathématiques, ces nombres premiers de Mersenne servent à compléter une séquence dite de Lucas, du nom d'un mathématicien français du XIX^{e} siècle, comme la suite de Fibonacci ou encore la suite de Jacobsthal. Un premier nombre premier de Mersenne est découvert le 13 novembre 1996 par ce procédé. En janvier 2016, 15 nombres premiers de Mersenne sont découverts et le logiciel continue de fonctionner.

Trois ans plus tard, en 1999, l'université américaine de Californie à Berkeley se lance dans un projet analogue : SETI@home (« SETI at home » : *Search for Extra-Terrestrial Intelligence*, Recherche d'une intelligence extra-terrestre) avec une fonction de recherche distribuée à la recherche de vie intelligente extra-terrestre. Aux frontières de la science-fiction, SETI@home ne découvre pas de signe de vie extra-terrestre mais enregistre un signal intéressant en septembre 2004, faisant dire à l'astronome américain Frank D. Drake qu'un signal concluant devrait être observé entre 2020 et 2025.

Fierté toute personnelle, j'ai modestement participé aux aventures de GIMPS, au début des années 2000, en faisant tourner plusieurs ordinateurs au sein de ce grand réseau international au service de la science. C'est finalement un ordinateur français, intégré au service support d'une entreprise d'informatique tricolore mais détourné par ses utilisateurs, enthousiasmés par ce défi mathématique et numérique, qui a réalisé la découverte pionnière de novembre 1996. Dans le monde entier, des utilisateurs comme ce Français ont participé à des initiatives dépassant leur capacité individuelle : cet état d'esprit marque l'avènement du protocole blockchain.

En 2002, une initiative identique est lancée par l'université de

Californie à Berkeley et l'Institut Max Planck de physique gravitationnelle à Hanovre. Ce projet, intitulé Einstein@Home, étudie les ondes gravitationnelles dans une visée scientifique, mais il démontre aussi l'immense capacité de calcul des ordinateurs combinés dans une logique d'Internet distribué. En 2007, enfin, l'université de Californie à Berkeley a inauguré un troisième et dernier projet d'informatique distribuée, MilkyWay@home, réunissant 38 000 ordinateurs, mis à disposition volontairement, dans le but de générer des modèles tridimensionnels de dynamique stellaire. Ces recherches scientifiques ont ainsi posé l'un des piliers de la technologie blockchain, celui de l'informatique massivement distribuée.

La naissance du bitcoin, de Wei Dai au BitGold

Après l'article fondateur de l'ingénieur Wei Dai sur la *b-money* (1998), l'idée d'une crypto-monnaie a lentement fait son chemin, à la fois parmi les économistes et les informaticiens. Par le passé, la mise en œuvre d'une monnaie électronique centralisée a déjà fait l'objet d'un « essai clinique », en 1990, sous l'impulsion du mathématicien américain David Chaum. La plateforme DigiCash Inc. permet de mener des transactions monétaires en ligne, de manière anonyme, grâce à un système d'encryptement très avancé. Toutefois, elle doit reconnaître sa banqueroute en 1998, en raison d'une intégration encore minime de l'e-commerce dans l'univers d'Internet. En 1995, deux jeunes pousses ont certes fait leur apparition, eBay et Amazon, mais elles n'ont pas encore eu le temps de pleinement déployer leurs ailes.

En juin 1996, la National Security Administration (NSA), l'agence américaine du renseignement, s'est penchée sur le sujet de la monnaie électronique, non sans une certaine inquiétude, dans un rapport aujourd'hui encore peu connu. Ce document, sobrement intitulé « Comment s'enrichir : la cryptographie de l'argent anonyme et électronique » (« How to Make a Mint: The Cryptography of Anonymous Electronic Cash »), s'intéresse aux problèmes liés à la cryptographie des transactions numériques, soulignant que les « clés cryptographiques », ces codes permettant le déblocage d'un virement,

ont la valeur juridique d'une signature mais qu'il est extrêmement difficile de vérifier si l'utilisateur d'une telle clé, humain ou informatique, est véritablement le client du compte en banque.

En 1997, le cryptographe britannique Adam Back développe donc un système de « preuve de travail » (*proof of work*) appelé Hashcash. Grâce à cette avancée technologique, les systèmes de paiement en ligne peuvent progressivement s'assurer que l'utilisateur des « clés cryptographiques » est véritablement humain à partir de la mesure des ressources informatiques utilisées par l'ordinateur employé pour signer numériquement l'autorisation de virement. Sur la base de ces réflexions, en 1998, le cryptographe américain Nick Szabo se donne pour mission de réaliser le rêve formulé par Wei Dai, la création d'une monnaie numérique décentralisée, le BitGold. Le Britannique Adam Back est depuis le CEO de Blockstream, l'une des entreprises les plus prometteuses dans le domaine de blockchain.

Dans son article fondateur, Wei Dai établit deux principes fondamentaux du développement d'une monnaie numérique : le premier, une base de données globale enregistrant la valeur en termes d'argent détenu par chacun des utilisateurs, et le second, un système d'enregistrement de l'argent mis en ligne sur l'ensemble du réseau. Le besoin de vérification du stockage d'argent en ligne est ainsi l'une des pierres angulaires des crypto-monnaies et le développement de Hashcash, par Adam Back, a permis de résoudre technologiquement ce besoin technique.

Professeur à l'école de droit de l'université George Washington, aux États-Unis, Nick Szabo s'intéresse d'abord aux contrats numériques (*smart contracts*). Il a longuement étudié l'algorithme *Elliptic Curve Digital Signature Algorithm* (ECDSA), inventé par Scott Vanstone en 1992 et utilisé pour permettre des opérations de signature et de chiffrement en ligne. En effet, dès 1994, Szabo commence à développer la théorie des contrats numériques, consacrés comme des protocoles de transactions informatiques avec la valeur juridique d'un contrat papier. L'informatique ne peut souffrir d'une impunité juridique et il faut donc lui transposer les règles du droit.

Entre 1998 et 2005, Szabo passe sept longues années à mettre en œuvre un projet de monnaie numérique en ligne, basé sur des chaînes infalsifiables par des preuves de travail de type Hashcash et agrémenté

de nombreux outils de travail, comme l'horodatage des transferts, les signatures numériques par des paires de clés cryptographiques, etc. À l'issue de ses travaux, Szabo publie une imposante étude en ligne pour prolonger l'aventure BitGold, mais le manque de sécurité de l'infrastructure monétaire minimise fortement l'importance des avancées conduites. Ses détracteurs condamnent ainsi la reproduction aisée des codes de création de valeur, permettant à chaque utilisateur de s'inventer des crédits supplémentaires en cas de faillite.

Le projet BitGold de Szabo a aussi souffert de la publicité offerte à Rippleplay, un système de règlement brut en temps réel utilisé sur le marché des changes et rendu public en 2004. Son développeur, l'ingénieur canadien Ryan Fugger, a, lui aussi, lu l'article de Wei Dai de 1998 et veut mettre en place une monnaie virtuelle mondiale décentralisée. À ses origines, Ripplepay est d'abord un service financier de paiement sécurisé en ligne, mais doublé de l'existence d'une communauté en ligne, réunie au sein d'un réseau mondial. Face au vide des réseaux sociaux numériques d'alors, Rippleplay a damé le pion à BitGold et l'aventure bitcoin s'arrête subitement pour quelques années.

Le tournant de 2008, l'ère Satoshi

En octobre 2008, un internaute anonyme, connu sous le psedonyme de Satoshi Nakamoto, propose le lancement d'une nouvelle monnaie numérique dans un papier scientifique intitulé « Bitcoin: A Peer-to-Peer Electronic Cash System ». En janvier 2009, après plusieurs années de travail secret, il rend public son logiciel Bitcoin-QT, créant les premières unités de monnaie numérique sur lesquelles il dit avoir travaillé pendant deux ans. Les premières transactions en bitcoins ont des usages aussi divers que variés – ainsi un achat de pizzas réalisé par Hal Finney en mai 2010 resté célèbre pour avoir coûté près de 10 000 unités bitcoins (BTC), soit 5 millions de dollars au cours actuel du bitcoin ! En octobre 2009, le premier taux de change du BTC en dollar américain est édicté – 1 BTC valait alors 0,001 USD.

En août 2010, cependant, le réseau Bitcoin-QT connaît une première brèche de sécurité. Deux internautes ont contourné le système de sécurité pour s'attribuer plusieurs centaines de millions d'unités de

bitcoins. La faille est rapidement repérée et la transaction effacée, mais le mal est fait : la confiance des utilisateurs est branlante. Aucune autre faille de sécurité d'une ampleur égale n'a jamais été enregistrée depuis cette fausse transaction, mais les détracteurs de la monnaie numérique se réfèrent systématiquement à cet incident pour en condamner l'usage. En décembre 2010, Satoshi quitte définitivement Bitcoin-QT et passe la main à un autre internaute présent aux origines, Gavin Andresen, pour se consacrer à divers projets personnels.

Diplômé de l'université de Princeton à la fin des années 1980, Andresen a commencé sa carrière comme ingénieur en logiciels de graphiques 3D chez Silicon Graphics Computer System. Cofondateur d'une société de jeux multi-joueurs en ligne pour aveugles (avec un dispositif de lecture des textes par l'ordinateur), il a publié plusieurs manuels de référence dans les années 1990 sur les évolutions à venir de l'informatique. Bien connu au sein de la communauté bitcoin, le legs de Satoshi en fait un personnage incontournable, aujourd'hui directeur scientifique de la Fondation Bitcoin. Je l'ai rencontré, en 2014, à Amsterdam, alors qu'il prenait la parole sur le sujet de la crypto-monnaie : c'est un homme visionnaire qui a bien compris que la révolution blockchain passerait d'abord par une petite communauté avant de devenir un phénomène mondial.

C'est, d'ailleurs, à l'occasion du lancement programmé de Bitcoin-QT, en novembre 2008, que le mot « blockchain » est utilisé pour la première fois, dans un échange public entre Satoshi et Finney, plus tard destiné à prendre sa succession, après le départ d'Andresen. Bitcoin-QT et le bitcoin de manière générale ont en effet survécu à plusieurs passations de pouvoir, se développant et se transformant sous la main de plusieurs architectes. En réalité, l'apparition et la disparition de Satoshi, le fondateur de ce nouveau système de crypto-monnaie, reste encore un mystère pour les observateurs et la presse. La véritable identité de cet internaute a ainsi donné lieu à de très nombreux débats.

Les théories les plus étranges ont ainsi fait leur apparition à l'époque de la disparition de Satoshi : Bitcoin-QT serait, en réalité, une opération secrète de la NSA pour développer un nouveau mode de financement (inspiré de son rapport de 1996) ou une entreprise conjointe de Samsung, Toshiba, Nakamichi et Motorola (dont les initiales, mises bout à bout, forment le nom « Satoshi Nakamoto »), etc. En 2014 une

journaliste américaine de *Newsweek* a ainsi révélé avoir découvert l'existence d'un Californien, âgé de 64 ans et d'origine japonaise, Dorian Nakamota, de son vrai nom Satoshi Nakamoto, cryptographe pour le compte de l'armée américaine.

À la suite du buzz médiatique sur la révélation de sa prétendue identité, le célèbre compte de Satoshi, mystérieusement resté sans utilisation pendant quatre ans, apprécié comme une relique semi-mystique par toute la communauté en ligne, publie simplement un bref message : « *Je ne suis pas Dorian Nakamoto* » (*I'm not Dorian Nakamoto*). Ce sont comme les premiers mots d'un revenant, car ce message des plus simplistes a un sens on ne peut plus nietzschéen : Dieu n'est finalement peut-être pas mort…

En 2014, comparant l'étude scientifique de 2009 au style rédactionnel d'une vingtaine de « suspects », une équipe de recherche de linguistique de l'université Aston de Birmingham, au Royaume-Uni, affirme que Nick Szabo, le fondateur de BitGold est le désormais célèbre Satoshi Nakamoto. Un an plus tard, en 2015, une journaliste du *New York Times* arrive aux mêmes conclusions. Le principal intéressé se dit aujourd'hui flatté mais dénie toujours être la personne cachée sous le fameux pseudonyme. À la fin de l'année 2015, enfin, deux journalistes du magazine *Wired* prétendent être sur une nouvelle piste, celle de Craig Steven Wright, un entrepreneur australien né en 1970.

En mai 2016, l'affaire prend un nouveau tournant lorsque Gavin Andresen, auquel Satoshi Nakamoto a confié les rênes du système bitcoin en 2010, affirme qu'il y a de fortes chances pour que Craig Steven Wight soit le fameux fondateur de Bitcoin-QT. À la suite de cette annonce, l'entrepreneur australien publie des documents officiels, témoignant de son implication dans la création de Bitcoin-QT à la fin des années 2000, mais plusieurs chercheurs mettent en doute cette affirmation et parlent d'une escroquerie. Son passé sulfureux, sa condamnation pour faute dans la banqueroute dans son ancienne entreprise, en 2004, et les perquisitions à son domicile, au cours de l'année 2015, dans le cadre d'une fraude aux aides fédérales de recherche participent assurément à ternir la réputation de ce candidat à la postérité numérique. L'affaire reste sans suite après que Wright décide de ne pas avancer de nouvelles preuves de son identité, en dépit du soutien officiel de la Fondation Bitcoin.

« *Nous aimons créer des héros*, expliquait alors Gavin Andresen, *mais il semble que nous aimons aussi les haïr s'ils ne vivent pas dans un idéal inaccessible. Ce serait sans doute mieux si "Satoshi Nakamoto" était le nom de code d'un projet de la NSA, ou d'une intelligence artificielle envoyée du futur pour faire évoluer notre argent primitif. Ce n'est pas le cas, c'est un être humain imparfait étant en tout semblable à nous autres*. » Reste qu'à ce jour, l'enquête se poursuit sur la véritable identité du fondateur du bitcoin, nimbant cette crypto-monnaie d'un parfum de mystère.

Qui se cache vraiment derrière le masque de Satoshi ?

Dans une récente tribune de juillet 2016, Jacques Favier, membre éminent de la communauté française bitcoin et fin connaisseur des monnaies en général, poursuit la métaphore et fait endosser les oripeaux du colonel Chabert, célèbre héros balzacien, à Craig Steven Wright : « *C'est un héros dépossédé, émouvant, mais assez lucide. Un roi goutteux a remplacé son empereur, un aristocrate l'a remplacé dans le lit de sa femme, la société a changé, il ne la reconnaît pas davantage qu'elle ne le reconnaît lui-même. Au terme de ses efforts, il prend, dit Balzac, la résolution de rester mort. Le roman de Balzac nous donne finalement des clés pour tenter de comprendre la situation, que Satoshi soit l'un des prétendants connus, ou bien qu'il soit tout autre et reste caché*. »

Si le fantasme d'un héros mythifié est, certes, plus séduisant que la vérité, l'identité de Satoshi Nakamoto demeure une énigme à résoudre à l'heure actuelle. Au cours des dernières années, je me suis moi-même prêté au jeu de cette enquête, d'abord avec amusement, ensuite avec curiosité et enfin avec passion. Compte tenu de la somme des connaissances techniques nécessaires à l'élaboration d'un tel système numérique, il me paraît improbable que Satoshi Nakamoto ne soit qu'une seule et même personne. J'estime, pour ma part, qu'il s'agit plutôt de l'alias d'un collectif de chercheurs, résolus à exécuter la prophétie de Wei Dai et à développer une crypto-monnaie.

J'ai longtemps trouvé étonnant que les quelques grands chercheurs

capables d'une telle prouesse, à peine une poignée d'individus dans le monde à la fin des années 2000, ne s'inquiètent pas qu'un tiers, à l'identité inconnue selon leurs dires, ait été à l'origine du bitcoin. Comment ne pas lire, en filigrane de leurs déclarations tranquilles, leur maîtrise parfaite du sujet et leur connaissance volontairement tue de l'identité de Satoshi ? Assurément, Satoshi est membre du cénacle de ces inventeurs de génie. Est-il Nick Szabo ? Hal Finney ? Craig Wright ? Wei Dai ? Ou encore, est-il tous ces hommes à la fois ?

Depuis longtemps, les scientifiques se sont réunis au sein de collectifs de recherche, publiant sous un alias unique, pour faire connaître leurs recherches. Nicolas Bourbaki en est un exemple. Paraît-il si absurde que les inventeurs du bitcoin aient fait de même ? Wei Dai, Szabo et Finney auraient ainsi réuni leurs forces au sein d'un groupe de travail. Chacun des trois hommes aurait de fait disposé d'une clé de sécurité à usage individuel et les publications sous pseudonyme commun auraient nécessité trois ou quatre desdites clés de sécurité. La maladie de Charcot, diagnostiquée à Finney en 2009 et qui causa sa mort en 2014, expliquerait que, éloigné de son ordinateur et ne pouvant utiliser sa clé de sécurité, Nakamoto se soit soudain muré dans le silence en 2010.

La réalité, c'est que l'identité de Satoshi Nakamoto est sans importance. Il est certain que ce secret ajoute du mystère et du *storytelling* dans l'univers de la blockchain. Ces éléments ont d'ailleurs concouru à nourrir un intérêt médiatique pour les crypto-monnaies et la technologie blockchain, mais l'anonymat du créateur de cette super-structure monétaire n'est pas un problème en soi. Il rappelle, tout au contraire, que, dans un système monétaire massivement distribué, chacun porte sa part du poids du système. En d'autres mots, dans le protocole blockchain, chaque utilisateur est en quelque sorte un fondateur.

Concentrer l'information et protéger la vie privée

En octobre 2015, *The Economist* consacrent une étude en première page à la technologie blockchain et à l'importance de la mécanique de confiance (*trust machine*) dans le fonctionnement ce nouveau système.

« *Blockchain*, peut-on dire lire dans l'article, *est le dernier exemple des fruits inattendus de la cryptographie.* [...] *C'est une science qui conserve les informations secrètes, ce qui est vital pour le chiffrement des messages, l'e-shopping, l'e-commerce, mais qui est aussi, et de manière paradoxale, un outil rendant les choses et le monde plus transparents*[7]. »

Faut-il alors croire, avec la nouvelle « La lettre volée » d'Edgar Allan Poe (1844), qu'un secret bien gardé est un secret qui n'est pas dissimulé ? L'idée serait séduisante, mais la vérité de la technologie blockchain est tout autre. La cryptographie a croisé l'histoire de l'informatique à de nombreuses reprises au cours du dernier siècle et des deux dernières décennies, des travaux de Turing pendant et après la Seconde Guerre mondiale à ceux de David Chaum et Scott Vanstone dans les années 1990, puis ceux de Nick Szabo sur les contrats numériques.

Dès son étude de 1998, Wei Dai a souligné l'importance grandissante de ces problématiques de vie privée face à la transformation de l'informatique et de l'économie de manière générale : « *Le modèle traditionnel de banque repose sur un haut niveau de discrétion, avec une limitation de l'accès aux informations par les parties contractantes et la tierce partie. La nécessité d'annoncer publiquement toutes les transactions empêche la poursuite de cette méthode, mais la discrétion peut être maintenue en limitant les flux d'information à un autre niveau : en anonymisant les clés publiques. Le public peut voir que quelqu'un envoie de l'argent à quelqu'un d'autre, mais sans information reliant le virement à une personne en particulier. Il s'agit d'un traitement similaire à celui utilisé dans les échanges boursiers, où l'heure et la taille des échanges, dits "tape", sont rendus publiques sans dire qui sont les deux parties à l'achat et à la vente.* »

L'idée de la collecte et de l'analyse d'informations à la base de la technologie blockchain interroge une partie de l'opinion quant à ses conséquences sur la protection de la vie privée dans les sociétés numériques. Non seulement, des organismes extérieurs collectent des données sur nos comportements et nos habitudes, mais nous en sommes venus, nous-mêmes, à générer des données sur nos façons d'agir à travers l'usage des nouvelles technologies. Le lancement de Wikipédia, par exemple, cette encyclopédie universelle en libre accès,

co-construite depuis 2001 par ses utilisateurs, ne relève-t-elle pas de cette nouvelle vision d'Internet : un réseau 2.0 ?

Les dangers auxquels nous expose la collecte de ces données sont alors immenses. Dans le film *Ennemi d'État* (1998) de Tony Scott, une loi accélérant la surveillance des télécommunications est ainsi promulguée afin de surveiller les agissements de tous les citoyens américains, et Gene Hackman, ancien analyste du renseignement accusé de défection, salutairement venu à la rescousse de Will Smith, dresse le constat terrible d'une société entièrement mise sous écoute : « *À Fort Meade, il y a 9 hectares de réseau informatique dans le sous-sol. Si on parle à sa femme, au téléphone, et qu'on dit les mots "bombe", "président" ou "Allah", ou une centaine d'autres mots clés, l'ordinateur les reconnaît, les enregistre, les marque en rouge pour analyse. Et je te parle d'il y a 20 ans déjà ! Pour un Hubble, ils ont plus de cent satellites-espions dans le ciel qui nous observent, nous. Secret défense. Dans le temps, il fallait qu'on branche un fil sur ta ligne téléphonique. Maintenant que les appels rebondissent sur les satellites, on les capte à la volée !* »

En 2014, les révélations de l'ancien analyste de la NSA Edward Snowden ôtent tout parfum de mystère à ces accusations. Elles prouvent que les gouvernements de notre planète opèrent non seulement des écoutes de la population, mais aussi des écoutes des dirigeants de pays étrangers, comme la chancelière allemande Angela Merkel. L'emprise du gouvernement sur les données numériques n'est toutefois pas une chose nouvelle. Dès les années 1970, les agences de renseignement de toute nationalité ont ainsi intégré les révolutions de la cryptographie et le recours aux outils informatiques.

En 1975, la NSA se dote ainsi d'un algorithme de chiffrement secret, le *Data Encryption Standard* (DES). Dès 1971, le cryptographe américain Horst Feistel a mis au point un tel outil pour le compte de la société IBM, sobrement baptisé *Lucifer*, mais l'agence américaine du renseignement souhaitait se munir d'un tel bouclier pour anticiper toute attaque numérique d'envergure. Cette ambition du gouvernement américain de se doter de techniques de cryptographie a nourri l'émergence des « guerres de la cryptographie » (*crypto wars*), au cours desquelles les internautes ont progressivement cherché à assurer leur droit en transformant l'outil informatique en arme de combat.

Les outils cryptographiques à la disposition des entreprises et des citoyens étaient ainsi relativement limités, et les codes de sécurité facilement cassables. L'émergence de l'ordinateur personnel et la naissance d'Internet au début des années 1990 ont, en outre, conduit à doter le grand public des outils d'encryptement jusqu'alors réservées au gouvernement. En 1966, les États-Unis ont inscrit les produits d'encryptement sur la liste des restrictions d'exportations de munitions, dite Catégorie XIII, afin de limiter l'accès à ces technologies. En février 1994, une première réforme est menée afin de libéraliser la commercialisation de ces technologies, dans un effort de démocratisation du numérique.

En 1996, le président Bill Clinton lève définitivement les limitations de certaines exportations dans le domaine des technologies d'encryptement par l'*Executive Order 13026*, mais décide de maintenir une tutelle du bureau de l'Industrie et de la Sécurité du ministère du Commerce sur les sociétés non militaires de cryptographie. Ces mesures d'encadrement ne sont pas exceptionnelles et l'Arrangement de Wassenaar sur la réglementation des exportations d'armes classiques et de biens et technologies à double usage, de mai 1996, montre bien cette volonté de coordonner les efforts internationaux en matière de contrôle de la cryptographie.

De manière plus générale, la question de la gouvernance mondiale du Net a pénétré le champ des relations internationales depuis plusieurs décennies. Il s'agit aujourd'hui d'un enjeu géopolitique majeur, notamment en matière d'adressage et de nommage des adresses IP ou encore de gestion des noms de domaines. Historiquement, depuis la fin des années 1970, le gouvernement américain détient un certain contrôle sur le développement du réseau internet à travers des outils comme l'Internet Configuration Control Board (1979), l'Internet Advisory Board (1986) ou encore l'Internet Architecture Board (1992). Depuis 2016, l'Internet Corporation for Assigned Names and Numbers (ICANN), une société californienne de droit privé, supervise le développement du Net.

Toutefois, à partir de 2003, la question d'un partage des responsabilités dans la gouvernance du Net est mise sur la table des négociations internationales, avec la création des Sommets mondiaux sur la société de l'information. Des initiatives comme la création de la

World Wide Web Foundation de Sir Berners-Lee ont, en outre, accru l'attention médiatique sur ces problématiques de gouvernance démocratique. En 2005, au Sommet de Tunis, les acteurs privés, les entreprises et la société civile sont ainsi reconnus comme des acteurs à part entière de la régulation du Net. En mai 2014, face à l'échec des discussions autour d'une gouvernance partagée, les gouvernements américains et brésiliens organisent l'initiative NETmundial, visant à créer un conseil international de 25 pays chargés de la gouvernance mondiale du Net. Un nouvel échec, malheureusement, après que l'annonce de trois sièges à vie pour les États organisateurs est rendue publique.

Un mouvement de rébellion, les cypherpunks anonymes

Contre la captation des informations et la mise sur écoute des populations, le mouvement des cypherpunks s'est érigé en rempart de la vie privée. Parce que le Web relie des personnes de pays et de régions différents, il a (en quelque sorte) fondé une communauté à part entière, une sorte de société des internautes, au sein de laquelle un esprit collectif a su se développer. La mouvance cypherpunk s'inscrit dans cette conception large des réalités numériques, sous la forme d'un réseau d'informaticiens, ou plus simplement d'utilisateurs du Web, dialoguant *via* une liste de diffusion mondiale, échangeant des informations et pistant les usages de la machinerie numérique pour les révéler au grand jour. Elle s'est nourrie du mouvement littéraire cyberpunk, apparu dans les années 1970-1980, mêlant science-fiction et numérique.

Neal Stephenson, l'une des grandes figures de ce mouvement littéraire, est d'ailleurs un natif de Fort Meade, aux États-Unis, et a nourri ses œuvres de cette paranoïa d'un gouvernement tout-puissant (*Le Samouraï virtuel*, 1992, *L'Âge de diamant*, 1995). Ses nombreux ouvrages mélangent des angoisses bien connues, matérialisées dès le *1984* de George Orwell (1948), et des considérations passionnantes sur les nouveaux enjeux de la modernité, comme la naissance de communautés numériques, les virus informatiques ou encore

l'impression 3D. Le mouvement littéraire cyberpunk flotte aussi à moitié dans une nostalgie de l'époque victorienne, mélangeant style démodé et nouvelles technologies, dans un sous-genre littéraire dit *steampunk* et souvent représenté à l'appui de machines à vapeur volantes.

À ses côtés, quelques années auparavant, un autre auteur américain de cyberpunk, William Gibson, a aussi contribué à façonner l'univers du mouvement cypherpunk. Passionné de cybernétique et de réalité virtuelle, l'auteur du *Neuromancien* (1984), première source d'inspiration de la saga de films *Matrix* des frères Wachowski (1999-2003), fait ainsi figure d'autorité tutélaire, voire de père spirituel au sein de la communauté cypherpunk. L'idée de connecter son cerveau à une matrice numérique pour se promener dans le réseau numérique mondial est née avec ses romans : le cyberespace est devenu un espace concret où les internautes, pirates du Net, construisent une nouvelle société à l'image de leur volonté. « *Le cyberespace*, note ainsi Gibson, *est une hallucination consensuelle, que des milliards d'opérateurs légitimes font chaque jour, dans chaque pays, à travers les enfants auxquels on apprend des concepts mathématiques. C'est une représentation graphique des données issues des banques de chaque ordinateur du système humain. Des lignes parfaitement alignées de non-espace de l'esprit, des nœuds et des constellations de données. Comme une cité de lumière !* »

En 1992, un important contributeur de la liste de diffusion cypherpunk, Tim May, rédige un essai historique consacré aux possibilités offertes par les nouvelles technologies aux anarchistes, *The Cyphernomicon: True Nyms and Crypto-Anarchy*. Ce texte fait l'apologie de l'anonymat offert par l'informatique grâce à l'intraçabilité des interactions entre utilisateurs et au re-routage intensif des paquets encryptés. Si l'auteur évoque les craintes de l'État à l'égard de ce nouveau segment du partage des informations, il en reconnaît aussi les effets néfastes : « *Le crypto-anarchisme permettra la vente libre de secrets nationaux et de biens illicites ou volés. Un marché électronique anonyme pourrait même rendre possibles de détestables foires aux assassinats et aux extorsions* ».

Deux histoires croisées animent ainsi cet essai : la première, celle des cryptographes alliés de la Seconde Guerre mondiale, cassant les codes secrets employés par les armées de l'Axe ; la seconde, celle des

crypto-anarchistes modernes, eux aussi en guerre contre l'autoritarisme et le totalitarisme des nouveaux gouvernements. En racontant la vie imaginaire de Lawrence Pritchard Waterhouse, un brillant scientifique ayant collaboré avec Turing, et celle de son petit-fils Randy Waterhouse, cryptographe des années 1990, Tim May tisse une toile associant le mouvement cypherpunk à la grande histoire de la cryptographie. Les nouveaux pirates du Net s'inscrivent ainsi dans un héritage intellectuel et scientifique, à même de défendre la justesse de leur cause.

Commentant l'essai cypherpunk de Tim May, l'ingénieur Wei Dai, père philosophique du bitcoin moderne, affirme toute sa sympathie à l'égard de ce mouvement : « *Je suis fasciné par la crypto-anarchie de Tim May. À l'encontre des communautés traditionnellement associées au mot "anarchie", la crypto-anarchie ne veut pas détruire le gouvernement temporairement, mais elle veut qu'il soit oublié et rendu inutile* (unnecessary) *de manière permanente. C'est une communauté où la menace de violence est inutile* (impotent) *parce que la violence est impossible, cela car les participants ne peuvent pas être reliés à leurs vrais noms ou à leur localisation géographique*. »

« *Les cypherpunks estiment que la vie privée est une bonne chose*, écrit encore Tim May, *et souhaitent qu'il y en ait davantage. Ils reconnaissent que ceux qui veulent une vie privée doivent s'en donner les moyens et ne pas simplement attendre des gouvernements, des entreprises, ou d'autres organisations immenses et sans visage, qu'ils leur accordent une vie privée par bienveillance. Les cypherpunks savent que les peuples ont dû se créer leur propre vie privée pendant des siècles, avec des murmures, des enveloppes, des portes fermées et des courriers secrets*[8]. »

L'essai de Tim May nourrit durablement l'esprit de la communauté cypherpunk qui se met, après sa publication, à se réunir physiquement, de manière régulière, dans la baie de San Francisco, aux États-Unis, puis partout dans le monde. Un an plus tard, en 1993, Eric Hugues, l'un des membres du petit groupe désormais baptisé cypherpunk, publie un manifeste crypto-anarchiste, « A Cypherpunk Manifesto ». Il y reprend, à son tour, l'idée que la vie privée doit être préservée des possibles dérives du Net et que le système d'échanges anonymes doit être généralisé. Il y appelle ainsi tous les cypherpunks à écrire des

programmes de chiffrement pour se prémunir des écoutes opérées illégalement par les gouvernements ou les entreprises. « *La vie privée est nécessaire dans une société ouverte à l'âge électronique*, écrivait-il de manière prophétique. *La vie privée n'est pas toutefois un secret. Une affaire privée est quelque chose dont on ne souhaite pas que tout le monde soit au courant, alors qu'une affaire secrète est quelque chose dont personne ne doit être au courant. La vie privée est donc le pouvoir de sélectionner ceux auxquels le monde sera révélé*. »

La même année, commentant ces deux manifestes de la cause cypherpunk, le développeur Hal Finney, parmi les premiers utilisateurs du bitcoin, écrit ainsi : « *Nous anticipons que les réseaux informatiques joueront un rôle de plus en plus important dans nos vies. Toutefois, cette informatisation accélérée apportera des dangers de plus en plus grands en matière de protection de la vie privée. Les cypherpunks veulent donc chercher à mettre en place des structures qui autoriseront les individus à préserver leur vie privée, s'ils le souhaitent. Personne ne peut forcer quelqu'un à utiliser un pseudonyme ou à écrire de manière anonyme. Cependant, la question de la quantité d'informations que chaque personne accepte de révéler à son propos en communiquant devrait être un problème fondamental. Aujourd'hui, le Net n'offre pas ce choix. Nous essayons en conséquence d'offrir ce pouvoir aux gens*[9]. »

En 1997, un représentant éminent de cette communauté, Christian As. Kirtchev, publie également un « Manifeste des cyberpunks », sorte de charte fondamentale des droits et devoirs du Net, réinscrivant le mouvement cypherpunk dans la dynamique de la littérature cyberpunk. Dans ce nouvel essai, les cypher-punks s'affirment comme des « hommes libres » auxquels on aurait dénié « la libre pensée », des combattants « de la liberté d'expression et de la presse ». Au détour d'un article, le Manifeste précise ainsi : « *L'encryption de l'information est notre arme. Ainsi, les mots de la révolution peuvent se propager sans interruption, en laissant les gouvernements seulement deviner*[10] ».

La crypto-anarchie invite donc à se munir des nouveaux outils numériques pour regagner ses droits à la vie privée. Dans son manifeste, Kirtchev souligne cette importance de l'alliance entre l'homme et la machine dans la conquête de nouveaux droits : « *Une cryptographie renforcée permet un encryptement incassable, une signature inoubliable, une messagerie électronique intraçable, et des*

identités pseudonymiques indécodables. Cette méthode assure que toutes les transactions et les communications soient fondées sur une véritable volonté de l'utilisateur. Les forces extérieures, le droit, toute forme de régulation n'ont aucun pouvoir et ne peuvent s'appliquer en ces lieux. C'est l'anarchie, au sens du refus de dirigeant extérieur ou de lois. Des arrangements volontaires, encadrés par des institutions nées de mêmes arrangements volontaires, dits services de séquestre (escrow services) *seront les seules règles applicables.* »

La communauté cypherpunk s'enrichit progressivement de la participation de nombreux membres au cours des deux dernières décennies de son existence, des noms que nous avons déjà croisés et d'autres rendus célèbres par l'actualité récente : Adam Black, le fondateur de Hashcash, Nick Szabo, l'inventeur de BitGold et le possible père du bitcoin, Jacob Appelbaum, l'un des développeurs de Tor et membre du Chaos Computer Club de Berlin, Julian Assange, le rédacteur en chef du site WikiLeaks, ou encore Boris Vitalik, un jeune développeur russe rendu célèbre par ses prouesses informatiques.

Boris Vitalik sous la lumière

Né en 1994, Boris Vitalik est un jeune Russe, émigré au Canada au début des années 2000. Élève de la célèbre Abelard School puis de l'Université de Waterloo, ce génie de l'informatique fait son entrée dans le sérail des crypto-anarchistes en 2012, à l'issue d'un tour du monde en six mois. Développeur de logiciel dès ses 19 ans, il incarne une génération de jeunes « geeks », le teint pâle, la voix fluette, l'air absorbé, à mi-chemin entre la passion et la démence. Il marque aussi un tournant générationnel dans l'univers du bitcoin, jusqu'alors développé par ses penseurs historiques (Wei Dai, Szabo, Satoshi).

En 2013, Vitalik crée Ethereum, une structure globale de portage d'une crypto-économie, à la croisée de la cryptographie, de l'épistémologie, de la théorie informatique, de l'économie et de la politique. Cette nouvelle révolution de la technologie blockchain se fonde sur un approfondissement des mécanismes de protection de la monnaie numérique : dépôts sécurisés, protection des utilisateurs, systèmes de réputation et de prédiction, sécurité à clés multiples, etc.

En mars 2015, le projet réunissait 30 employés à temps plein et Vitalik réussit une levée de fonds de 18 millions de dollars pour financer ses équipes. Le financement des investisseurs en capital risque vient à la rescousse du bitcoin.

Un autre visage de cette période de développement rapide de l'environnement blockchain est celui de Mark Karpelès, un trentenaire français, « baron du bitcoin », aujourd'hui incarcéré au Japon. Développeur de logiciels chez Linux Cyberjoueurs au début des années 2000, il s'installe à Tokyo, en 2009, où il a créé une société spécialisée dans l'hébergement web et dans le développement d'applications numériques, Tibanne. En 2011, il achète 88 % de Mt. Gox, une plateforme d'échanges de bitcoins contre des dollars, créée en 2009. Au moment de son rachat, le site brasse environ 20 millions de dollars de transactions quotidiennes, soit plus des trois quarts des échanges mondiaux de bitcoins.

Néanmoins, à l'été et à l'automne 2013, le site subit plusieurs attaques pirates et près de 750 000 bitcoins sont détournés (grâce à des transactions refusées à tort). Or, entre janvier et décembre 2013, le cours du bitcoin passe de 20 dollars à plus de 1 000 dollars, soit une perte catastrophique pour la plateforme. L'annonce de l'intégration du bitcoin à PayPal, en avril, puis l'installation des premiers distributeurs automatiques de bitcoin au Canada, en octobre, ont en effet contribué à cette ascension vertigineuse, conclue par la reconnaissance du bitcoin comme une « *monnaie légitime* » par la Réserve fédérale américaine (FED), le 19 novembre. La fraude à Mt. Gox se chiffre alors, *in fine*, à plusieurs milliards de dollars.

En décembre 2013, trois annonces finissent de rendre critique la situation du marché mondial du bitcoin : la Banque de France dénonce, dans un rapport du 5 décembre, le caractère « *hautement spéculatif du bitcoin* » et souligne le « *risque juridique important lié à son statut de monnaie non régulée* » ; puis la Banque centrale de Chine fait de même, accusant une monnaie « *qui n'a pas de cours légal* » et qui n'a pas non plus le statut de « *devise authentique* » ; enfin, le 11 décembre, Apple interdit finalement l'utilisation du bitcoin *via* ses applications. En février 2014, de guerre lasse, Karpelès annonce la fermeture de sa plateforme d'échange puis se déclare en faillite.

La notoriété de Vitalik s'inscrit aussi dans un contexte particulier : la

chute de Jita (*Burn Jita*). Historiquement, nous l'avons vu, la science-fiction et le mouvement des cypherpunks se sont nourris l'un l'autre. Les jeux de rôle en ligne massivement multi-joueurs (*massively multiplayer online role-playing game*, MMORPG) sont ainsi un lieu de rendez-vous dématérialisé des cypherpunks depuis près de trente ans. Déjà au milieu des années 1980, le réseau international Bitnet accueillait *Multi Access Dungeon* (MAD), un des premiers jeux de rôle inventé par deux étudiants de l'École des mines de Paris. Les jeux développés par le collectif Mutiny, dans la série américaine *Halt and Catch Fire* (2014-2016), sont ainsi la parfaite représentation de cet esprit : des espaces de détente, dans lesquelles la mise en place d'une plateforme d'échange (*chat*) a soudé la communauté de joueurs.

En 2003, la société islandaise CCP lance *EVE Online*, un MMORPG de science-fiction, dans lequel chaque joueur contrôle un ou plusieurs vaisseaux spatiaux et explore l'univers. Pour développer sa flotte, il peut collecter des ressources naturelles, commercer avec d'autres joueurs, mais aussi nouer des alliances, entrer en guerre avec ses rivaux, voire organiser des actes de contrebande ou de piraterie à l'encontre d'autres joueurs. À l'époque, le jeu connaît un franc succès, car il laisse la détermination des prix d'échange des marchandises au simple marché. Le prix d'un minerai dépend ainsi du point de vente et du poids des différentes corporations de production. La spéculation devient un élément important de l'économie d'*EVE Online* puisque les joueurs sont invités à entretenir une véritable économie capitalistique.

En 2012, cependant, *EVE Online* connaît une véritable révolution, caractéristique de la mentalité de l'époque. Un groupe de 1 500 joueurs (sur une communauté globale de 400 000 joueurs) décide de s'en prendre au centre économique du jeu. Le groupe anarchiste Goonswarm lance ainsi tous ses vaisseaux sur la planète centrale et le plus grand hub commercial du jeu, Jita, dans l'espoir de déstabiliser l'ensemble de l'économie du jeu. Dans tout autre MMORPG, les développeurs auraient utilisé des fonctions de sécurité pour bloquer cette « révolte numérique » et supprimer les comptes des joueurs, mais les petites mains de CCP décident de laisser libre court à cette attaque pour observer la transformation du jeu par lui-même.

Si l'offensive de Jita est virtuelle, sa reprise par les principaux médias de l'époque témoigne d'un changement de paradigme : l'internaute a

désormais un pouvoir sur l'économie numérique, il peut être un acteur révolutionnaire de la société. Ainsi, l'individu en dehors du système, l'*outsider*, peut agir sur le fonctionnement interne de la société. Les dégâts causés par cette attaque ont été chiffrés à 535 milliards d'ISK, la monnaie du jeu, en quelques jours, soit 83 années d'abonnement en monnaie réelle. Pour les développeurs de CCP, l'attaque-suicide de leurs joueurs était le paroxysme de la liberté qu'ils voulaient insuffler à l'univers du jeu : « *Les flottes de nos joueurs, armées de vaisseaux à forte capacité de tir, ont commencé à détruire des vaisseaux de commerce de haute valeur à l'occasion d'une campagne implacable. En une volée simple mais coordonnée, se sacrifiant par la même occasion en vagues successives, ils ont bouleversé l'économie d'EVE Online. Tout cela a rapidement pris fin, car la "police" in-game du jeu a déchaîné une justice de réprimande quasi immédiate et extrêmement violente, mais, en tant que développeurs, nous avons observé cette bataille à la fois avec effroi et respect, car c'est un événement que nos joueurs ont entièrement amené dans notre univers*[11]. »

Anonymous, une ultime rébellion cypherpunk ?

Avec les principales révolutions du Net du début du XXIe siècle, le mouvement cypherpunk se transforme dans une approche plus activiste. L'hacktivisme, c'est-à-dire la capacité d'infiltrer des réseaux et de mener des opérations coup-de-poing technologiques, est né. En 2003, le réseau Anonymous, désormais célèbre pour l'usage du masque du rebelle britannique Guy Fawkes, est créé dans cet esprit. À partir de 2006-2007, il mène plusieurs assauts numériques contre Habbo, un hôtel virtuel en ligne, puis contre l'Église de scientologie, enfin contre YouTube, qui avait mené une campagne de censure de plusieurs de ses vidéos en ligne.

En 2009, Anonymous se fait connaître sur la scène mondiale en combattant la censure organisée par le gouvernement iranien pendant la période des manifestations postélectorales. En septembre, il annonce officiellement s'engager dans le but de protéger les droits civils des citoyens et adopte son slogan : « *Nous n'oublions jamais, nous ne*

pardonnons jamais » (*We never forget, we never forgive*). En 2010, au nom de l'Internet libre et ouvert à tous réclamé par les cypherpunks, le groupe mène une opération de vaste ampleur, dite *Operation Payback* (opération Représailles), visant les adversaires du piratage sur Internet et les grandes banques en ligne (PayPal, Visa, Mastercard).

Anonymous s'est, très tôt, intéressé aux théories de la blockchain, notamment le système dit de *namecoin*, alliant un nom et un message par paire, afin de remplacer le système DNS (*Domain Name System*, système de noms de domaine) contrôlé par des organisations gouvernementales. Grâce au *namecoin*, le groupe entend « *protéger la libre parole en ligne en rendant le Web plus résistant, créer un nom de domaine .bit dont le contrôle serait totalement décentralisé, mémoriser des informations d'identité comme des adresses email, des clés cryptographiques publiques, etc.* ». La filiation entre cypherpunks et néo-hacktivistes tient donc à cette passion constante pour le secret et la cryptographie.

Faute de chef unique, le groupe semble un temps s'effriter entre une frange extrémiste, engagée dans l'attaque de PlayStation Network en 2011, et une frange plus politique, rangée derrière l'objectif de protéger Julian Assange et le site d'archives WikiLeaks. Créée en 2006 et alimentée de 1,2 million de documents officiels en 2007, cette plateforme en ligne de dissidents internationaux divulgue en effet, de manière anonyme, des documents classés secret défense. En 2010, sous la menace de suppression du domaine du site, WikiLeaks avait supposément accueilli l'aide d'Anonymous dans sa démarche.

L'aventure WikiLeaks, un réseau de lanceurs d'alerte

Si les cypherpunks ont longtemps paru enfermés dans un délire obsidional, bon nombre de leurs prédictions se sont révélées réelles au cours des dernières années. Le site WikiLeaks a ainsi participé à faire connaître du grand public les excès de certains gouvernements, en matière de corruption et de scandales, mais aussi d'espionnage et de violation des droits de l'homme. Dès ses origines, le site regroupe des activistes de toute nationalité : Julian Assange, Wang Dan, Ben Laurie,

Chico Whitaker ou encore Wang Youcai. Toutefois, la notoriété du site a connu un essor incroyable en novembre 2010, à la suite de la révélation de plus de 260 000 télégrammes diplomatiques échangés entre le Département d'État américain et ses ambassades de par le monde.

Entre 2006 et 2009, le site a certes fait parler de lui après quelques révélations sulfureuses : révélation de détournements de fonds par un candidat à l'élection présidentielle au Kenya en 2007, publication de documents de travail relatifs aux négociations sur l'Accord commercial anti-contrefaçon en 2008, mise en ligne de courriers électroniques échangés par les scientifiques du Climatic Research Unit, etc. En avril 2010, WikiLeaks publie même une vidéo de l'armée américaine montrant deux photographes de l'agence de presse Reuters accidentellement tués par un hélicoptère américain lors d'un raid aérien sur Bagdad, en juillet 2007. De nombreux journalistes prennent alors contact avec le site.

En juillet 2010, en coopération avec *The New York Times, The Guardian* et *Der Spiegel*, WikiLeaks publie 91 000 documents militaires américains classés secret défense, notamment sur la guerre d'Afghanistan, incriminant le double jeu joué par le Pakistan. Dans la foulée, en novembre, dans le cadre de l'opération « Cablegate », 250 000 télégrammes diplomatiques américains sont mis en ligne, offrant « *un panorama inédit des négociations d'arrière-salle, telles que les pratiquent les ambassades à travers le monde* ». Le site enchaîne alors les révélations de scandales : publication de 2 000 comptes en banque domiciliés dans des paradis fiscaux et appartenant à des personnalités politiques en janvier 2011, révélation d'une étude de l'Agence internationale de l'énergie atomique sur les réacteurs japonais après les accidents de Fukushima en avril 2011, etc.

En avril 2011, WikiLeaks révèle des informations concernant les 779 détenus du camp américain de Guantanamo, diffusant notamment des photos et des rapports médicaux, témoignant des conditions de vie abominables de ces individus. Le grand public découvre avec horreur la réalité de cette prison, dont Barack Obama avait promis (en vain) la fermeture dès son élection, en 2009. Le 2 septembre 2011, 390 000 documents militaires classés secret défense sont encore mis en ligne, portant cette fois sur la guerre en Irak et l'occupation du pays, puis, en juillet 2012, plusieurs centaines de documents fuitent sur la

Syrie et les politiques de détention aux États-Unis. En quelques années, WikiLeaks s'est imposé comme un lanceur d'alertes incontournable de la Toile.

La poursuite d'Assange ou le succès d'un anonyme

Les origines de l'aventure WikiLeaks se mêlent au parcours de Julian Assange, un cybermilitant australien, récemment interprété à l'écran par Benedict Cumberbatch, dans *Le Cinquième Pouvoir* (2013). À cet effet, l'acteur britannique avait d'ailleurs tenté d'entrer en contact avec Assange, à l'issue d'une correspondance révélée par *The Guardian*. Informaticien auprès de Suburbia Public Access Network, un des premiers fournisseurs d'Internet grand public d'Australie, Assange s'intéresse à la cryptographie dans les années 1990. En 1997, il est l'un des inventeurs de Rubberhose, un progiciel de « déni plausible », permettant à l'utilisateur de prouver qu'il n'a pas fait usage d'un logiciel de création de fichiers.

En 1999, il enregistre le nom de domaine leaks.org mais choisit de ne pas en faire usage immédiatement. Il est alors le gestionnaire d'un forum de sécurité informatique reconnu au niveau national et participe régulièrement aux travaux de la communauté des hackers australiens. Il utilise le pseudonyme « Proff », emprunté au roman cyberpunk *Cryptonomicon* (1999) de Neal Stephenson, ce qui en fait un digne représentant de la communauté cypherpunk. La même année, il dénonce l'acquisition par la NSA du brevet d'un instrument d'écoute et d'enregistrement des appels téléphoniques : « *Ce brevet devrait inquiéter les gens*, écrit-il sur son forum. *Tous les appels téléphoniques dans le monde sont ou pourront bientôt être écoutés, transcrits et archivés dans les boyaux d'une agence d'espionnage étrangère qui ne devra rendre aucun compte*[12]. »

En 2006, au moment du dépôt du nom de domaine du site WikiLeaks, Assange fait partie du conseil de direction de l'organisation et voyage à travers le monde pour en assurer la promotion. En août 2010, quelques mois après les révélations fracassantes de WikiLeaks sur l'armée américaine, une enquête est ouverte contre lui en Suède, pour des viols

qu'il aurait commis lors d'un déplacement professionnel. Assange y voit alors une fausse accusation destinée à nuire à son activité d'hacktiviste. Une partie des charges a finalement été levée en août 2015, la justice suédoise n'ayant pas pu interroger Assange, mais l'enquête préliminaire est toujours ouverte et ne prendra fin qu'en 2020.

En novembre 2010, après la première vague de publication des télégrammes diplomatiques américains, le ministre de la Justice américain a parallèlement ordonné une enquête criminelle sur WikiLeaks. Les comptes en banque d'Assange sont d'abord gelés puis il est arrêté par la police britannique, mais remis en liberté surveillée sous réserve de paiement de sa caution et du port d'un bracelet électronique. L'année suivante, en décembre 2011, Bradley E. Manning, un soldat américain stationné en Irak, est accusé de la fuite des documents américains sur l'Irak et ses juges croient que son interlocuteur a été Julian Assange, désormais directement connecté à cette affaire. En juin 2012, de peur d'être extradé vers les États-Unis et d'encourir la peine de mort, le porte-parole de WikiLeaks choisit de demander l'asile politique à l'Équateur et s'installe à l'ambassade de ce pays à Londres.

Cette réclusion forcée n'est pourtant pas le signe d'une défaite. À Londres, Assange publie d'abord *Cypherpunks: Freedom and the Future of the Internet* (2012), un ouvrage consacré au mouvement crypto-anarchiste. En 2013, il se présente, à distance, aux élections sénatoriales australiennes, mais il finit par y renoncer faute d'emballement médiatique. Dans sa prison dorée, il accueille des dirigeants et des artistes étrangers (Oliver Stone, Lady Gaga, Jean-Luc Mélenchon), participe à des reportages ou des émissions politiques à distance.

À la suite de sa décision, la police britannique reçoit l'ordre de stationner devant l'ambassade d'Équateur et d'arrêter Assange dès que l'occasion se présenterait. Les patrouilles de police ne sont retirées qu'en octobre 2015, pour des raisons de coût (12,6 millions de livres sterling cumulés depuis 2012). À l'été 2015, à la suite des publications sur les écoutes illégales d'officiels allemands et français par le gouvernement américain, Assange publie une lettre ouverte au président de la République François Hollande, demandant l'asile politique en France, mais celui-ci lui est refusé. En février 2016, un

groupe de travail des Nations unies sur la détention arbitraire recommande la fin des poursuites à l'encontre d'Assange, mais le gouvernement britannique rejette immédiatement la décision.

Le choc Snowden : les cypherpunks avaient raison !

Les révélations de WikiLeaks n'ont pas été sans écorner l'éthique des responsables du renseignement américain. Dès 2009, à la suite de l'élection de Barack Obama à la présidence des États-Unis, une enquête interne a interrogé la légalité de certaines pratiques, mais l'Administration américaine a choisi de ne pas y donner suite. Edward Snowden, un jeune employé, d'abord engagé dans les forces spéciales pendant la guerre en Irak, puis informaticien auprès de la CIA (2007-2009) et de la NSA (2009-2012), cherche alors à faire fuiter des informations sensibles. Il prend d'abord contact avec un journaliste du *Guardian*, Glenn Greenwald, sans suite, puis avec la documentariste Laura Poitras. Un contact est finalement établi en mai 2013, à Hong Kong.

Snowden remet alors à ses deux interlocuteurs une clé USB et annonce son départ prochain pour Moscou afin d'échapper à toute tentative de poursuite : « *Je suis prêt à sacrifier toute ma vie, tout ce que j'ai, tout cela parce que je ne peux plus laisser, en mon âme et conscience, le gouvernement américain détruire la vie privée, la liberté d'Internet et les libertés essentielles des gens du monde entier avec ce système énorme de surveillance qu'il est en train de bâtir secrètement*. »

Début juin 2013, Greenwald publie finalement un premier article sur les écoutes téléphoniques opérées par la NSA et sa couverture publique Verizon. Les choses s'enchaînent alors rapidement : grâce à la menace de poursuites juridiques, le gouvernement britannique obtient la destruction des informations confiées par Snowden au *Guardian*, mais rapidement, en septembre puis en octobre, Greenwald est appelé à collaborer avec des équipes de journalistes américaines, brésiliennes et françaises afin d'étudier les documents fournis par l'ancien agent de la NSA.

En février 2014, Greenwald et Poitras annoncent le lancement de *The Intercept*, une plateforme de publication des documents de la NSA révélés par Snowden. À terme, les rédacteurs veulent faire bénéficier les lanceurs d'alerte de toute nationalité d'un support efficace à la publication de leurs informations : « *Notre mission à plus long terme est de mettre en place un journalisme agressif et indépendant sur un grand spectre de sujets*, écrivent-ils sur la page d'annonce de leur site*, de la vie privée, aux affaires criminelles et aux abus de justice ou de libertés fondamentales, aux inégalités sociétales et aux autres formes de corruption financière et politique*. [...] *Nous estimons que la première valeur du journalisme est d'imposer la transparence, et ainsi la responsabilité, de ceux qui détiennent la plus grande part de pouvoir gouvernemental et corporatif. Nos journalistes ne se verront pas seulement permettre, mais bien encouragés, à présenter leurs révélations, sans distinction des personnes qu'elles pourraient gêner*. »

La même année, Laura Poitras consacre son documentaire *Citizenfour* (2014), troisième volet d'une saga consacrée à l'Amérique post-11 Septembre, à l'affaire Snowden. Après avoir dénoncé les excès de la guerre contre le terrorisme dans *My Country, My Country* (2006) et les coulisses de la base de Guantanamo dans *The Oath* (2010), ce nouvel opus revient sur la surveillance mondiale généralisée à travers le parcours d'Edward Snowden. « Citizenfour », c'est en effet le pseudonyme utilisé par Snowden pour communiquer avec la presse en 2013, au moment de ses révélations sur les pratiques de la NSA.

Après avoir fui en Russie, Snowden est au cœur d'une dispute diplomatique entre les deux anciennes puissances de la guerre froide. Début juillet 2013, une rumeur indique que le lanceur d'alerte serait à bord de l'avion du président bolivarien Evo Morales, de retour d'une conférence à Moscou. Immédiatement, la France, l'Italie et l'Espagne annoncent la fermeture de leur espace aérien. L'incident provoque de violentes émeutes à La Paz et, le 5 juillet, le Venezuela et le Nicaragua annoncent leur disposition à accueillir Snowden en exil, au nom de leur ambition de « *le protéger de la persécution de l'empire le plus puissant du monde, qui s'est déchaîné sur lui* ». Deux jours plus tard, le président cubain Raul Castro ajoute sa voix au concert, ouvrant la voie à un exil vers l'Amérique du Sud en passant par La Havane, pour éviter tout contrôle américain.

Mi-juillet 2013, Snowden finit par demander asile au gouvernement russe, avec le soutien du président de la Douma, le Parlement national. Comme les Américains ont annulé son passeport, l'ancien analyste est piégé sur le territoire russe, plus exactement dans l'aéroport de Cheremetievo. Un premier accord d'asile temporaire lui est finalement accordé pour un an, le 31 juillet 2013. Un second accord d'asile de trois ans lui est ensuite délivré, à l'été 2014, avec un droit de voyager librement à l'étranger. Régulièrement invité des médias (à distance), Snowden apporte son témoignage aux députés européens, en mars 2014, dans le cadre du Comité d'enquête sur la surveillance électronique de masse de citoyens de l'Union européenne.

En mai puis juin 2014, le député français Yves Jégo puis les sénatrices françaises Chantal Jouanno et Catherine Morin-Desailly déposent une proposition de résolution pour accorder l'asile à Edward Snowden en France, mais celui qui se dit lui-même « patriote » préférerait rentrer aux États-Unis à moyen terme. En octobre 2016, le réalisateur à succès Oliver Stone met à l'honneur l'histoire de ce héros maudit, dans *Snowden*, un long-métrage où Joseph Gordon-Levitt endosse le rôle de paria et lève le voile sur les activités de renseignement du gouvernement américain.

Internet, lieu de découverte et de création

D'Assange à Snowden, le Net s'est affirmé comme un véritable espace de révélations depuis quelques années. La fluidité du numérique, sa capacité à enregistrer et traiter rapidement des informations à la base des angoisses des cypherpunks a finalement servi leur rêve de transparence et de diffusion des secrets d'État. Elle a aussi généré de véritables menaces sur la sécurité des individus, ainsi celle des agents secrets américains agissant sous couverture dans le nord de l'Afrique, démasqués par la publication des télégrammes diplomatiques de WikiLeaks en 2011. Le tableau n'est donc pas si clair qu'il y paraît.

Au Net, on reconnaît facilement sa capacité à encourager la création : lancement de YouTube en 2005, pour partager ses vidéos ; lancement de Ulule en 2010, plateforme de financement participatif destinée à

l'accompagnement de projets, etc. On oublie parfois que la libre communication des données, notamment le partage des fichiers en P2P, a participé à asphyxier l'industrie de la musique. La prolifération des plateformes d'échange de fichiers audio de musique, telles que Kazaa, Napster ou encore PirateBay, a montré l'importance pour l'économie des données de se transformer, d'adopter de nouveaux supports numériques, bref d'accompagner la révolution numérique.

Une organisation comme Creative Commons, créée en 2001, vise ainsi à libérer les œuvres de leurs droits de propriété intellectuelle. Les nouvelles technologies nous invitent donc à repenser la tragédie des biens communs théorisée par l'économiste Garrett Hardin, à réfléchir à l'inaliénabilité de certains biens publics, essentiels à l'humanité. Le développement de la blockchain est partie prenante de cette réflexion. Elle ne nous interroge pas seulement sur les nouveaux outils du quotidien. Elle pose des questions de fond sur la société de demain : quelle croissance ? Quelle mesure de la réussite d'un pays ? Comment réduire les inégalités et redonner confiance en la démocratie ?

La blockchain, de l'esprit à la main

Au fond, la révolution blockchain a d'abord été une affaire de culture, de littérature et d'esprit avant d'être mise sur pied par des ingénieurs et des techniciens. Le mouvement cyberpunk et la science-fiction ont abondamment nourri tant les rêves des inventeurs que les craintes des internautes. Le mouvement cypherpunk des années 1990, lointain ancêtre d'Anonymous et des lanceurs d'alerte modernes, n'a-t-il d'ailleurs pas emprunté son nom à ce courant littéraire fasciné par la transformation de l'humanité et la crise de la civilisation ? Les récentes études de robotique ne reconnaissent-elles pas, à l'identique, s'être inspirées des ouvrages d'auteurs de science-fiction comme Isaac Asimov ?

Assurément la littérature, le cinéma et aujourd'hui les séries ont contribué à diffuser une certaine culture de l'informatique. Les livres de Dan Brown, *Anges et démons* (2000) et *Da Vinci Code* (2003), ont contribué à cette culture du secret révélé, du complot généralisé contre lequel quelques-uns luttent dans l'ombre et dans l'oubli. Best-sellers

popularisés par des films grand public, ces livres ont aussi nourri un sentiment global d'inquiétude et de paranoïa. Que ne nous dit-on pas ? Le projet Open bitcoin Privacy entend ainsi éduquer à la protection de la vie, en partageant quelques bonnes pratiques des services de bitcoin.

La série *Halt and Catch Fire* (2014-2016) nous rappelle avec nostalgie les premiers pas de l'informatique et l'esprit de communauté des pionniers de champ de découvertes. La série *Mr Robot* (2015-2016) nous plonge, elle, dans les angoisses de la communauté crypto-anarchiste, dans un univers où la machine contrôle l'homme, prend entièrement possession de lui, y compris dans ses agissements physiques, lui vole ses données, son identité, mais aussi son libre arbitre. C'est, d'ailleurs, le principal discours porté par le film *Nerve* (2016) d'Ariel Schulman et Henry Joost, dans lequel deux jeunes se voient voler leur identité par une société numérique d'anonymes. Le visage fantomatique de Rami Malek n'a donc pas fini de hanter vos nuits à la pensée des sombres tractations d'Evil-Corp.

Que nous apprend l'économie sur la blockchain ?

« Si nous sommes tentés de voir dans la monnaie un élixir qui stimule l'activité du système, rappelons-nous qu'il peut y avoir plusieurs obstacles entre la coupe et les lèvres. »

JOHN M. KEYNES, *Théorie générale de l'emploi, de l'intérêt et de la monnaie*, 1936

Force est de constater que la technologie blockchain nous invite aujourd'hui à repenser notre relation à l'économie et à la monnaie. Que nous apprend cette révolution technologique sur nos usages de l'argent, sur nos relations économiques ou encore sur notre conception de la finance ? Développer le bitcoin, cette quasi-monnaie empruntée au répertoire numérique, c'est en quelque sorte observer notre propre reflet dans un immense miroir, détaillant chaque aspect de notre société. Que nous dit alors la technologie blockchain sur notre économie ? C'est l'objet de ce chapitre, approche synthétique de l'histoire de la monnaie et tentative avouée de dessiner les contours de son avenir proche.

La technologie blockchain, on l'a vu, est en effet le fondement de la crypto-monnaie : autrement dit, elle est l'outil fondamentalement nécessaire au développement d'une nouvelle monnaie numérique, le bitcoin. Elle réunit trois ingrédients utilisés dans la recette de la création d'une crypto-monnaie, à savoir l'*open source*, l'informatique distribuée et la théorie des jeux. Pourquoi vouloir changer la monnaie ? Parce qu'elle est, pour ainsi dire, le pouls d'une économie, le sang coulant dans ses veines et alimentant chacun des organes de la société, et que les récentes crises économiques ont montré que du sang neuf était plus qu'essentiel à la revitalisation du corps sociétal.

Déjà dans *Émile ou de l'éducation* (1762), le philosophe Jean-Jacques Rousseau soulignait, avec justesse, l'importance de la monnaie, « *vrai lien de la société* », chargée d'être une mesure commune des choses pour faciliter les échanges entre les hommes, entre le meunier et le tisserand dans son exemple historique. L'argent ne quantifie cependant pas toutes les choses de la vie et l'auteur du célèbre *Du contrat social* invitait déjà, avec une lucidité frappante, à ne pas mesurer la richesse d'un homme seulement à l'aune de la quantité de monnaie en sa possession : « *Si vous prétendiez expliquer aux enfants comment les signes font négliger les choses, comment de la monnaie sont nées toutes les chimères de l'opinion, comment les pays riches d'argent doivent être pauvres de tout, vous traiteriez ces enfants non seulement en philosophes, mais en hommes sages, et vous prétendriez leur faire entendre ce que peu de philosophes même ont bien conçu*. »

Pour comprendre l'émergence des crypto-monnaies comme le bitcoin et en apprécier toutes les spécificités, il est donc utile de revenir sur la naissance de la monnaie, ses évolutions et ses limites. L'objet de ce chapitre est de dresser une perspective historique du parcours de la monnaie, des pierres de Yap aux flux numériques échangés par les traders des banques de Paris, Londres ou New York. La dématérialisation de la monnaie est ainsi un élément fondamental de notre réflexion, car elle a précédé le développement de la monnaie numérique en tant que tel.

Comme l'établissement du bitcoin au rang de monnaie mondiale semble difficilement réalisable à court et moyen terme, deux autres ambitions pour l'avenir de cette monnaie numérique méritent notre attention : l'usage du bitcoin comme monnaie complémentaire aux systèmes monétaires traditionnels, pour préparer une transition globale de notre économie monétaire à long terme, et le cheminement vers des monnaies disposant de nouvelles formes de gouvernance.

La naissance des monnaies

La monnaie est apparue à l'époque de la révolution néolithique, entre -14 000 et -12 000, en réponse à l'intensification des opérations de troc entre les hommes afin de faciliter ces échanges. Avec le

développement de l'agriculture et la domestication des animaux, les hommes ont en effet voulu échanger davantage et les tribus ont commencé à nouer des relations de commerce durables. La monnaie est donc historiquement apparentée au contrat et aux pratiques sociales de communication entre les hommes, ainsi qu'à l'établissement des premières relations intertribales et internationales sur le long terme.

Aristote, dans *Les Politiques* (IVe siècle avant Jésus-Christ), consacre d'ailleurs quelques lignes à cette théorie de la naissance de la monnaie : « *Quand les habitants d'un pays deviennent plus dépendants d'un autre pays, et qu'ils importent ce dont ils ont besoin et exportent ce qu'ils ont en quantité excédentaire, alors la monnaie entre nécessairement en utilisation.* »

Dans les temps préhistoriques, la monnaie n'était pas forcément un petit objet taillé dans une matière naturelle, ainsi que l'on se le figure aujourd'hui. En Inde, le bétail servait ainsi de valeur d'échange lors d'une négociation, si bien que le mot « bœuf » en sanskrit (*rupa*) sert aujourd'hui encore de dénomination à la monnaie nationale indienne (roupie). Un peu plus tard dans l'histoire de l'humanité, dans les pays celtiques de l'ouest de l'Europe, les armes et les outils ont servi de monnaie d'échange. Les monnaies primitives ne se sont véritablement développées que quelques millénaires plus tard, autour de -10 000 ou -9 000.

Des traces de monnaies à base de coquillages apparaissent ainsi en Amérique du Nord, notamment dans la région de la Californie, autour de -9 000. Ces coquillages servaient à la fois de monnaie d'échange et d'ornementation des maisons ou des sites funéraires, car la monnaie (à l'époque déjà) témoignait de la place de l'individu dans l'ordre sociétal. La valeur de la monnaie dépendait alors de la taille du coquillage et le « ligua », l'unité de compte la plus élevée, mesurait environ 6 pouces de long. De telles pratiques d'utilisation des coquillages ont également été observées en Afrique, dans la région du Congo, jusqu'au milieu du XIXe siècle, et en Asie du Sud-Est ou en Océanie, jusqu'au début du XXe siècle.

Il est d'ailleurs intéressant de noter que Nick Szabo, l'un des pères du bitcoin, a consacré un long essai à la question des monnaies de coquillage, *Shelling Out* (2002), insistant sur l'idée que les monnaies primitives ont participé à créer du dialogue entre les hommes et à initier

une première ère de paix. La valeur du coquillage était alors déterminée dans d'autres unités d'échange, lorsque les peuplades locales ou régionales échangeaient entre elles. En Asie du Sud-Est, par exemple, il fallait 3 840 coquillages de cauris pour acquérir un bœuf, soit une roupie, et 6 400 coquillages pour acquérir un baht, une des 13 unités de pièces d'argent du Siam. C'est la naissance des politiques de change, grâce auxquelles la valeur d'une monnaie est calculée en unités d'une autre monnaie.

L'île de Yap : la monnaie en roue libre

Parmi les plus anciennes monnaies au monde, la roue de pierre de Yap (*rai*) est une monnaie fascinante mais tout aussi étrange. Utilisée dans la Fédération des États de Micronésie, dans la région des Philippines, dès le II^{e} millénaire avant Jésus-Christ, cette monnaie de pierre a la taille d'un imposant disque d'aragonite, percé d'un trou au milieu, avec un diamètre variant de 0,8 à 4 mètres. Taillées dans les carrières de Palaos avec des outils de coquillage, ces imposantes pièces d'une tonne étaient transportées d'un endroit à l'autre à l'aide d'un pilier de bois, coincé dans le trou central et permettant de faire rouler la pierre, puis portées dans les pirogues indigènes.

La valeur de la pierre en question était mesurée à la hauteur de l'effort humain fourni pour l'acquérir : extraction du minerai, taille et ciselage, transport, etc. Ces pierres servaient ainsi au paiement d'achats de terres ou de titres dans cette société clanique, mais aussi à négocier des accords de paix ou de commerce. Par exemple, si le transport en pirogue de la pierre de Yap avait causé la mort d'un homme, sa valeur était conséquemment augmentée. Les pierres étaient ensuite disposées le long des rues, devant les habitations, à la vue de tous, afin de montrer le statut social de leur possesseur. Considérant la taille de la monnaie, le vol était une issue peu envisageable à l'avenir de ces rochers.

Surtout, ce qui est remarquable dans l'utilisation de ces pierres taillées sous forme de grandes meules, c'est la façon dont le consensus s'est créé autour des processus de transactions. Lorsqu'un acheteur A désire acquérir la maison d'un concitoyen B, il va utiliser la pierre comme

forme de monnaie d'échange. A dispose d'une pierre P, dotée d'une valeur reconnue par la communauté. Cette propriété sur la pierre est connue de tous. Au moment où il procède à la transaction, donnant à B la propriété de P, sans avoir même à déplacer la pierre, il est désormais reconnu comme nouveau propriétaire de la maison. La communauté de l'île va ainsi mémoriser que la pierre P appartient désormais à B. La propriété des pierres présente et passée est inscrite dans la mémoire du village. Il n'existe pas de registre centralisé, il s'agit bien d'un registre décentralisé, inscrit dans la mémoire de chacun des membres de la communauté, en quelque sorte identique à celui la blockchain !

Au XIXe siècle, avec l'arrivée des explorateurs occidentaux, l'économie monétaire des archipels changea brutalement. Les goélettes de l'explorateur David O'Keefe permettaient en effet de déplacer plus facilement et plus rapidement les rais que le traditionnel transport en pirogue, diminuant *de facto* leur valeur. En 1931, la dernière roue de pierre de Yap fut taillée, avant que les clans locaux n'adoptent d'autres formes de monnaie. L'usage du *coprah*, une devise en noix de coco, comme monnaie de négoce au transport des rais a, en effet, supplanté l'échange de ces pierres massives.

Toutefois, elles ont su garder un certain cachet car, jusqu'à récemment, la Banque de Hawaï acceptait encore de gager des prêts en dollars sur des pierres de Yap. En Italie, une pratique identique est encore monnaie courante dans la région de l'Émilie-Romagne, où les banques stockent des meubles de parmesan, estimées à environ 300 euros par meule de 40 kilogrammes, avec un intérêt de maturation de 500 euros par meule, en garantie des crédits accordés aux producteurs. En 2016, le Credito Emiliano, la banque de Bologne, envisageait ainsi de stocker environ 500 000 meules pour couvrir des opérations de prêt d'environ 132 millions d'euros.

La monnaie et la comptabilité

Parallèlement au développement des monnaies primitives, les premières nations ont cherché à enregistrer les flux d'entrées et de sorties d'argent au niveau d'une comptabilité nationale. En Mésopotamie, au milieu du IIIe millénaire avant Jésus-Christ, l'empire

Akkad a ainsi été l'un des premiers à développer une unité de compte globale, le *mine*, plus tard utilisé comme unité de masse dans la Grèce antique. La richesse nationale était ainsi inscrite en mines sur des tablettes d'argile, plus tard stockées dans les coffres du palais royal. Le mine servait donc de valeur étalon, c'est-à-dire de valeur universelle dans laquelle toutes les autres valeurs de produits achetés ou vendus étaient converties.

Avec l'intensification des échanges commerciaux autour du bassin méditerranéen, les Égyptiens et les Phéniciens mirent en place une comptabilité plus poussée encore. Dès le IV^e^ siècle avant Jésus-Christ, l'ancienne Égypte disposait d'un système d'audit, afin de vérifier que les commerces sous la tutelle royale ne fraudaient pas dans leurs déclarations d'entrées et de sorties d'argent. Ces mécanismes de surveillance prenaient la forme d'une audience auprès du comptable royal, c'est pourquoi le terme latin *audire* (écouter) a donné le mot moderne « audit ».

À l'époque romaine, sous le règne de l'empereur Auguste, à l'aube du I^er^ millénaire, un système complexe d'inscription des possessions de la cité de Rome fut développé. L'élite gouvernante de la Rome antique souhaitait en effet planifier davantage les recettes et les dépenses impériales et pouvoir prendre des décisions importantes sur le plan financier (comme la construction de temples ou l'organisation de jeux) en toute connaissance de cause. Cet outil de contrôle de la dépense publique fut placé entre les mains d'hommes libres, des esclaves affranchis, tant la tâche répugnait les citoyens romains. Ces informations étaient ensuite inscrites sur des tablettes ou des papyrus et stockées avec le trésor impérial.

Au Moyen-Âge, la transformation de l'économie donna toute son importance à ce régime de comptabilité de la monnaie. D'une part, les marchands étaient désormais capables de mener plusieurs négociations commerciales simultanément grâce à l'internationalisation des échanges, prévoyant une entrée financière d'un côté et une sortie de l'autre. Cette pratique se développa avec la construction de routes commerciales et l'accélération des déplacements des marchands. Le plus vieil exemple de livre de comptes à double entrée est ainsi daté de 1299 ; il appartenait à des marchands florentins, installés à Nîmes.

D'autre part, les crédits bancaires se développèrent sous l'influence

de l'accroissement des dépenses (extension des royaumes, mobilisation d'importantes armées) et la comptabilité fut un instrument incontournable dans l'enregistrement des crédits et débits. Au milieu du XV^e^ siècle, l'économiste italien Benedetto Cotrugli chercha ainsi à définir quelques règles de la comptabilité, dans un ouvrage aujourd'hui encore célèbre au sein de la communauté scientifique, *Della mercatura e del mercante perfetto* (1458). Finalement publié en 1573, imprimé et écrit en italien, le livre connut une très grande diffusion en Europe, assurant une meilleure connaissance de ces mécanismes de comptabilité et accompagnant le développement de la finance médiévale.

La monnaie et l'expérience coloniale

Au XVII^e^ siècle, alors que les colonies européennes étaient en phase d'expansion sur l'ensemble des continents, les Amériques britanniques connurent une pénurie temporaire de monnaie. Depuis le début de la colonisation, les puissances européennes toléraient certes l'usage de monnaies coloniales, comme le dollar espagnol ou le shilling américain, mais les colonies américaines firent l'expérience désagréable d'une pénurie de monnaie classique. La métropole londonienne rechignait en effet à payer les données acheminées vers le Vieux Continent avec de l'or, de l'argent ou du cuivre, et préférait exporter du tabac vers la colonie américaine. L'économie américaine fut donc, dès les origines, forcée de s'adapter à cette situation.

Contrairement à de nombreux stéréotypes, les Amérindiens ne pratiquaient plus le troc à ce moment de l'histoire. Ils utilisaient des coquilles de palourdes (*clams*), qu'ils gardaient attachés autour du cou, sous forme de collier, pour monnayer leurs dépenses. À l'occasion des rituels ou des cérémonies d'échanges entre clans, comme à l'occasion d'un traité de paix ou de commerce, des vêtements du quotidien pouvaient être parés de coquilles de palourdes, comme les ceintures, afin de témoigner de la richesse d'une tribu. Les Narragansetts étaient ainsi connus pour être des spécialistes dans la taille des coquilles de palourdes. De 1637 à 1667, la Nouvelle Angleterre reconnut même cette monnaie comme une valeur d'échange légale au sein de son système monétaire.

En 1652, alors que la Couronne d'Angleterre avait interdit la pratique des monnaies coloniales, le Massachusetts édita une série de pièces en argent, des *shillings* de pin, à cause du pin dessiné au verso de la pièce. Les shillings du Massachusetts furent utilisés dans l'ensemble des colonies du nord de l'Amérique jusqu'en 1682. Toutefois, toutes les pièces utilisées étaient battues à l'année 1652. En effet, à l'époque, Londres était une république et les dirigeants de Boston firent donc de la monnaie un outil de politique, témoignant de leur sympathie pour la république britannique, et un instrument de diffusion de leur message, à l'heure de l'apparition des premiers télégraphes.

L'invention du billet de banque

Avec la recherche d'une simplification des échanges monétaires et la naissance de la comptabilité, plusieurs civilisations ont voulu mettre en œuvre une nouvelle forme de monnaie, plus simple à échanger : le billet de banque. Cette unité d'échange n'était plus, comme les coquillages, les pierres ou les pièces, basée sur sa valeur intrinsèque, mais sur la confiance des consommateurs dans l'organisme émetteur de ces billets. Cette première dématérialisation est une étape fondamentale dans l'histoire de la monnaie, mais elle a nécessité plusieurs siècles d'évolution et de transformation pour être complètement accomplie.

Dès le I^er^ millénaire avant Jésus-Christ, les Chinois de la dynastie Tang, puis ceux de la dynastie Song se prêtèrent au jeu de l'émission de billets de banque (*jiaozi*). À l'origine, ces billets étaient des reçus sous forme de papier, à l'occasion d'échanges commerciaux entre les marchands, fondés sur un système de comptabilité proche de celui développé à l'époque médiévale en Europe. Progressivement, cependant, les marchands se mirent à privilégier cette unité d'échange pour éviter les inconvénients d'échanges en monnaie : poids considérable de la monnaie échangée pour les négociations les plus importantes, difficulté à protéger la monnaie en cas d'attaque ou de vol à l'occasion des déplacements de ces vendeurs nomades, etc.

Échangés dès 960, ces billets de banque chinois furent utilisés parallèlement à la circulation des pièces en métal, mais le gouvernement impérial perçut rapidement les avantages de cette

nouvelle unité d'échange. Parce qu'elle reposait fondamentalement sur la confiance, l'économie du billet invita à de fortes garanties de la part de ses émetteurs. Dans la Chine médiévale, l'empereur décida donc d'imposer un monopole impérial sur la production de billets de banque, en disposant seul des gravures de bois nécessaires à l'impression. Cette décision assura le sérieux de la monnaie, appuyée sur les comptes royaux, mais confia également un rôle politique à l'empereur sur l'économie chinoise. À sa volonté, un certificat de dépôt d'un marchand auprès de ses comptes pouvait être annulé ainsi que, *de facto*, la validité de ses billets. Le succès de ces billets chinois est probant : en 1120, l'équivalent de 26 millions de pièces circulait sous la forme de billets.

Au XIII^e^ siècle, avec les voyages de Marco Polo dans l'Empire mongol et le récit de ses aventures, le billet de banque chinois fut découvert en Europe : « *La monnaie du Grand Khan n'est ni d'or, ni d'argent, ni d'autre métal. On se sert pour la faire de l'écorce intérieure (le liber) de l'arbre qu'on appelle mûrier, qui est celui dont les feuilles sont mangées par les vers qui font la soie. Cette écorce, fine comme papier, étant retirée, on la taille en morceaux de diverses grandeurs, sur lesquels on met la marque du prince, et qui ont diverses valeurs depuis la plus petite somme jusqu'à celle qui correspond à la plus grosse pièce d'or. L'empereur fait battre cette monnaie dans la ville de Cambalu, d'où elle se répand dans tout l'empire : et il est défendu, sous peine de la vie, d'en faire ou d'en exposer d'autre dans le commerce, par tous les royaumes et terres de son obéissance, et même de refuser celle-là*. […] *Le roi commande quelquefois à ceux qui restent à Cambalu qu'ils aient à porter leur or, leur argent et leurs pierres précieuses sans retardement entre les mains de ses officiers, et en recevoir la juste valeur en la monnaie susdite. De là il arrive que les marchands et les habitants n'y perdent rien ; et que par ce moyen le roi tire tout l'or et se fait de grands trésors. L'empereur paye aussi en cette monnaie ses officiers et ses troupes ; et enfin il en paye tout ce qu'il a besoin pour l'entretien de sa maison et de sa cour. De sorte qu'il a fait d'une chose de rien beaucoup d'argent et qu'on peut faire aussi beaucoup d'or et d'argent avec cette misérable monnaie. Ce qui fait qu'il n'y a point de roi au monde plus riche que le Grand Khan, car il amasse des trésors immenses d'or et d'argent, sans dépenser rien pour cela*[13]. »

Rapidement, dans les Flandres médiévales, la solution est adoptée pour se prémunir des attaques de convois de marchands. Au XIVe siècle, les « billets d'or », des documents servant de lettre de change entre un créditeur et son débiteur s'imposèrent comme monnaie courante et, comme les banques étaient principalement la source de ces documents, le billet prit le nom de « billet de banque » (*nota di banco*). Au cours du siècle, l'usage du billet de banque connut alors un essor formidable, du nord au sud de l'Europe : les marchands déposaient leur argent auprès d'une banque et acquéraient un billet valable dans d'autres pays. La dématérialisation de l'argent va ainsi de pair avec la création d'un grand réseau international des banques.

La naissance du billet moderne

Au XVIIe siècle, dans le prolongement du succès des billets d'or, les banquiers européens décident d'émettre massivement des billets de banque, sur le modèle de l'empire chinois. En 1661, la Banque de Stockholm saisit l'opportunité d'une crise de la monnaie nationale, soumise aux aléas du commerce international, pour proposer ce papier léger, avec une valeur égale à celle de l'argent. En 1664, toutefois, la banque connaît une sévère banqueroute, en raison de l'artificialisation de la monnaie. Les billets de banque n'étaient pas suffisamment indexés sur une valeur en réserve, une sorte d'étalon monétaire. À la fin du siècle, dans son *Discours sur les échanges* (1690), l'économiste britannique Nicholas Barbon assure ainsi que : « *La monnaie est une valeur imaginaire, édictée par la loi, afin de faciliter les échanges*. »

En 1694, trente ans après la déroute de la Banque de Stockholm, la Banque d'Angleterre renouvela l'expérience des billets de banque, en pleine guerre avec la France de Louis XIV. À l'origine, la valeur des billets pouvait être inscrite manuellement, mais progressivement, pour des raisons de facilité, des chiffres fixes furent inscrits. En 1745, la valeur fixe des billets fut décidée : 20, 50, 100, 1 000 livres sterling. Ces documents comportaient toujours, à l'époque, la signature de l'acquéreur du billet et du banquier. Cette double signature du chèque dut attendre 1855 pour véritablement disparaître.

Des expériences identiques furent conduites en France et aux États-

Unis à la même époque. En 1715, à la mort de Louis XIV, John Law offrit ses services d'économiste au régent du royaume de France, Philippe d'Orléans, proposant notamment de remédier au problème de l'endettement du royaume par la mise en œuvre d'un système de billets de banque. En 1716, Law fut donc autorisé à créer la Banque générale et à émettre un papier-monnaie en échange de stocks d'or dans les banques royales. Afin d'inspirer la confiance dans ce système, Philippe d'Orléans lui-même se prêta au jeu, mais le système s'emballa rapidement, la banque imprimant plus de billets qu'elle ne disposait de stocks d'or.

En 1718, la Banque générale fut renommée Banque royale et le roi en assura dès lors la garantie des chèques distribués. Deux ans plus tard, en 1720, nimbé du succès de son système et de ses ambitions coloniales, Law fut nommé contrôleur général des finances : 1 milliard de billets de banques circulaient alors à travers le royaume de France, gagés sur 322 millions de livres. Jalousé par le duc de Bourbon et le prince de Conti, Law fut victime d'une opération de spéculation sur sa banque. Les grands possesseurs de billets demandèrent ainsi à réaliser leurs avoirs sous forme d'or et d'argent, ce qui ruina la Banque royale et provoqua sa banqueroute, en mars 1720.

La naissance des étalons monétaires

Afin d'assurer la stabilité des billets de banque comme unité monétaire, l'émetteur doit donc s'assurer de disposer d'une valeur détenue, à partir de laquelle il produit des unités d'échange. Cependant, avec l'ébauche de la mondialisation du commerce et la multiplication des conflits, les stocks d'argent et d'or des puissances européennes diminuent et les nations européennes sont invitées à davantage miser sur le billet de banque. En 1774, à l'aube de la guerre d'indépendance des États-Unis, l'Angleterre est ainsi touchée par une crise monétaire mais ne dispose pas des moyens de frapper une nouvelle monnaie.

Pendant les guerres napoléoniennes, soumises à de fortes pressions financières, les banques anglaises suspendent temporairement la conversion des billets de banque. Entre 1816 et 1820, le pays engage une vaste opération de fabrication de monnaie : souverains d'or,

couronnes et demi-couronnes d'argent, *farthings* de cuivre, etc. En 1823, la convertibilité des billets de banque est finalement de nouveau appliquée et les banques régionales émettent des billets de petites dénominations, des « petites coupures ». En 1826, la Banque d'Angleterre rapatrie ces missions d'émission des petites coupures et, en 1833, ses billets sont officiellement reconnus comme la monnaie légale du pays.

En 1844, le gouvernement britannique déclare que tous les billets de la Banque d'Angleterre devront désormais être garantis en or : c'est la naissance de l'étalon-or. En 1848, le gouvernement fédéral des États-Unis édicte un étalon identique en argent et en or, mais le taux de conversion surévaluant l'argent, l'or américain fuit le pays vers les banques britanniques. La ruée vers l'or est alors déclenchée : de partout dans le monde, les hommes et les femmes partent à la conquête de l'Ouest américain, pour acheter une parcelle de terre, creuser, miner et découvrir les pépites tant fantasmées.

En 1853, les États-Unis réduisent progressivement le poids des pièces en argent puis, en 1857, ils suspendent temporairement tout paiement en argent. L'étalon-argent des billets américains est finalement abandonné en 1861. Toutefois, pendant toute la décennie suivante, plusieurs tentatives de résurrection d'un étalon bimétallique (argent et or) voient le jour, au profit des découvertes de filons d'argent dans l'Ouest américain. Avec l'amorce de l'industrialisation, les banques préférèrent néanmoins le choix de la stabilité et l'assurance de fondements solides à leurs futures transactions avec les entreprises. L'or a gagné ce combat de titans.

Cette montée en puissance de l'étalon-or est confirmée, en 1871, par son adoption par l'Allemagne impériale avec la Loi monétaire prussienne, puis par son adoption par l'Union monétaire latine, composée de la Belgique, la France, l'Italie, la Suisse et la Grèce. En France, l'étalon-or est finalement adopté officiellement en 1876, dans les premières années de la Troisième République. Le nouveau système n'est cependant pas unanimement célébré et certains accusent les banquiers de profiter de la rareté de l'or pour créer des crises de crédit et saisir les propriétés des agriculteurs. Pendant la campagne présidentielle américaine de 1896, le candidat démocrate William Jennings Bryan compare même l'étalon-or à la couronne d'épines

portée par le Christ pendant son martyr.

La guerre et la remise en cause de l'étalon-or

En 1914, au début de la Première Guerre mondiale, le Royaume-Uni annonça la fin de la convertibilité-or des billets de la Banque d'Angleterre. Face aux dépenses militaires faramineuses, les principales puissances européennes avaient en effet fait le choix d'imprimer plus de monnaie qu'elles n'en possédaient dans leurs banques. À la fin du conflit mondial, une des conditions de l'armistice fut le paiement de lourdes réparations de guerre par l'Allemagne et l'Autriche-Hongrie sous forme de réserves en or (132 milliards de marks-or), déposées sur les comptes bancaires des puissances alliées. La surveillance du paiement de ces réparations fut confiée à Commission interalliée des réparations.

En 1922, les accords de Gênes marquèrent une nouvelle étape de l'ordre monétaire mondial : la convertibilité-or des monnaies fut fixée comme objectif de court terme des politiques monétaires des puissances signataires, et la livre et le dollar furent désignés comme monnaies de réserve substitutive. Le Royaume-Uni et les États-Unis, vainqueurs de la Première Guerre mondiale, étaient donc avantagés par cette situation puisque leurs monnaies pouvaient servir directement d'étalon à l'émission de billets. La négociation internationale mit surtout en place un nouveau système de convertibilité de la monnaie en or, le *Gold Exchange Standard*.

En 1923, la Commission interalliée des réparations reconnut le défaut de paiement de l'Allemagne de Weimar et autorisa la saisie des mines de charbon de la Ruhr par la France, en compensation immédiate. Après la crise économique et financière de 1929, le Royaume-Uni et les États-Unis décidèrent de dévaluer leurs monnaies pour relancer leurs économies : Londres annonça conséquemment la fin de la convertibilité-or de la livre en 1931, suivie de Washington, pour le dollar, en 1933. Face à la pénurie d'or des banques américaines, le président Franklin Delano Roosevelt déclara « hors la loi » la possession d'or par les Américains dès le mois d'avril 1933.

À la place la convertibilité-or de leurs monnaies, les grandes

puissances des années 1930 mirent en place des zones monétaires, au sein desquelles toutes les monnaies nationales étaient rattachées à une monnaie de référence par un taux de change fixe. En 1931, Londres mit donc en place la Zone livre sterling, aussi appelée Bloc sterling, entre le Royaume-Uni, les pays du Commonwealth (à l'exception temporaire du Canada), les pays scandinaves et le Portugal. Régulée par les accords de Bâle de 1968, cette zone monétaire prit effectivement fin en 1979, soit près de quarante ans après son lancement.

En Europe continentale, la France, la Belgique, les Pays-Bas, l'Italie, la Suisse et la Pologne s'unirent au sein du Bloc or lors de la conférence de Londres de juillet 1933. Cette union monétaire était fondée sur une entente commune au maintien de l'étalon-or et à une coordination accrue entre les banques d'émission des pays signataires. Cette démarche de lutte contre la dévaluation des monnaies permettait notamment de conserver de l'or dans certaines caves des banques d'émission, tout en autorisant d'autres banques d'émission du même réseau à mener des opérations monétaires fondées sur ces stocks à l'étranger. Cette pratique appelée « *earmarked* » diminuait ainsi les risques liés au transport matériel de l'or d'une banque à l'autre.

En 1934, l'Italie viola les règles du Bloc or, suivie de la Belgique en 1935 et de la Pologne en 1936, forcées de dévaluer leurs monnaies. En France, l'évasion de l'or détenu par les banques fut un phénomène avéré entre 1933 et 1936 : les stocks de la Banque de France passèrent ainsi de 4 914 tonnes au moment de la conférence de Londres en 1933 à 2 964 tonnes en octobre 1936. Une partie de cet or fut thésaurisé par les ménages français, tandis que l'autre fut déposée dans des banques étrangères, notamment à Londres, déjà reconnue comme une grande place bancaire internationale. En 1936, la dévaluation du franc mena à une certaine instabilité du pays et, au début de l'année 1937, il fut rattaché à la livre sterling britannique.

Le système de Bretton Woods

Au cours de la Seconde Guerre mondiale, anticipant les négociations de paix, les économistes américains analysèrent l'échec de l'accord de Versailles de 1919 et de l'accord de Gênes de 1922. Pour Henry

Morgenthau, secrétaire au Trésor de l'Administration Roosevelt, le nouvel ordre mondial dépendrait à la fois de mesures collectives de sauvegarde des peuples du monde et d'une coopération économique entre les nations, prévenant tout désajustement économique ou financier. La révision du *Gold Exchange Standard* paraissait donc un point important des discussions entre les alliés.

À la conférence de Bretton Woods, en juillet 1944, les Américains rejetèrent l'idée d'un retour au système de l'étalon-or, soulignèrent la faillite d'un système de change-or multipolaire, comme celui établi par les accords de Gênes de 1922, et proposèrent en conséquence un nouveau système de change-or fondé sur une seule monnaie, le dollar américain. Toutes les monnaies seraient ainsi définies en dollar et seul celui-ci serait défini en or, avec un encadrement de la conversion en dollar entre un taux de change plancher et un taux de change plafond, et une marge de dépassement maximum de 2 %.

Pour assurer l'application de ces nouvelles règles, les accords de Bretton Woods, instituent deux organisations internationales : le Fonds monétaire international (FMI), chargé de surveiller les politiques monétaires nationales et d'accompagner toute éventualité de crise, et la Banque internationale pour la reconstruction et le développement (BIRD), aujourd'hui devenue une institution de la Banque mondiale, chargée d'accompagner la relance de l'économie puis d'accomplir les objectifs économiques et sociaux définis par l'Organisation des Nations unies. Ces nouvelles règles de l'ordre monétaire international déterminent aussi le cadre du commerce international, défini par l'Accord général sur les tarifs douaniers et le commerce (General Agreement on Tariffs and Trade, GATT), en 1947, modifié depuis par des cycles de négociations successifs.

En 1958, la Banque d'Angleterre, banque centrale du Royaume-Uni, met en place l'*Euromarket*, un système d'approvisionnement en dollars des investisseurs européens, exclu de tout contrôle américain. Comme le monde est alors en pleine guerre froide, le système connaît un certain succès, car les Soviétiques y voient l'opportunité de détenir des dollars en dehors de Washington et d'éviter une saisie de l'intégralité de leurs actifs financiers en cas de guerre réelle entre les deux puissances. En 1963, le président John F. Kennedy instaura une taxe sur les intérêts des investissements étrangers afin de décourager cette

pratique mais l'*Euromarket* était devenu une bulle énorme : 3 milliards de dollars circulaient à travers ce système au début des années 1960, près de 46 milliards en 1970 !

La quantité de dollars en circulation dans le monde s'est alors mise à dépasser la taille des réserves totales mondiales de devises. Avec la guerre du Vietnam et la course à l'espace, les États-Unis exportent de plus en plus de dollars à travers le monde, nourrissant une inflation inquiétante. Dès 1970, la République fédérale d'Allemagne demande à ce que ses dollars soient remboursés en or, dévalisant les réserves américaines. Pour stopper l'hémorragie de ses réserves en or, le président Richard M. Nixon annonce la fin de la convertibilité-or du dollar en août 1971 et le régime des changes flottants, c'est-à-dire des changes établis en fonction des forces du marché, est instauré en mars 1973. En 1976, les accords de la Jamaïque confirment l'abandon définitif du système de Bretton Woods.

Hayek et la dépolitisation de la monnaie

Au début des années 1970, après la fin de la convertibilité-or du dollar, l'économiste Friedrich Hayek interrogea le poids de la géopolitique et de la politique sur la valeur des monnaies. Prix Nobel en 1974, ses travaux condamnent avec une grande fermeté le laxisme des politiques monétaires post-Seconde Guerre mondiale. Avec les monétaristes, il regrette en effet que les politiques budgétaires imaginées par Keynes dans la première moitié du siècle, la fameuse relance par la consommation, ne soient qu'une vision de court terme et qu'à long terme, ces dépenses publiques déraisonnées ne conduisent qu'à une inflation. Pour Milton Friedman, la croissance économique des pays doit être accompagnée d'une hausse progressive de la masse monétaire en circulation, afin de financer la multiplication des transactions économiques et financières du pays.

En France, ces théories sont véhiculées par Jacques Rueff, un économiste au service du général de Gaulle et de Georges Pompidou. Défenseur de l'étalon-or, le haut fonctionnaire proposait de revenir sur les accords de Bretton Woods de 1944, pour retrouver une comparaison des monnaies directement à la quantité d'or détenue par

l'État. Pour Hayek, la pratique moderne des politiques monétaires conduit le système bancaire à faire crédit à partir d'une simple création monétaire, c'est ce qu'il appelle « l'expansion forcée du crédit » : les entreprises empruntent de manière inconsidérée sans tenir compte de la demande réelle des consommateurs. Hier, les banques proposaient de la monnaie en échange de stocks d'or ou d'argent mais, aujourd'hui, la mise en place des banques centrales avec leur monopole de production de monnaie impose l'usage d'une monnaie au cours forcé.

Hayek dénonce ainsi cette suprématie des banques centrales, capables d'utiliser de manière discrétionnaire l'instrument de la dévaluation. Dans *Denationalisation of Money: The Argument Refined* (1976), l'un des derniers ouvrages publiés de son vivant, il appelle une nouvelle concurrence libre entre les monnaies. Le bitcoin s'inscrit pleinement dans cette dénonciation des systèmes monétaires centralisés. Pour Jon Matonis, président de la Fondation Bitcoin : « *Le bitcoin porte le fier héritage de Menger, Mises et Hayek, et de la théorie des cycles économiques de l'école autrichienne*. [...] *Il supporte en effet l'idée que la dénationalisation des monnaies ne recherche aucune autorité pour continuer son existence, sans reconnaître aucune frontière politique à sa circulation*. [...] *Le bitcoin est donc un bon point de départ pour mettre fin au monopole des banques centrales dans l'émission de monnaie*[14]. »

L'œuvre même de Hayek porte des conclusions identiques sur la nécessaire dénationalisation de la monnaie : « *Le fait intéressant est ce que j'ai appelé le monopole du gouvernement d'émission de la monnaie, qui nous a non seulement privés de beaucoup d'argent mais qui nous prive aussi du seul processus par lequel nous pouvons trouver ce qui serait beaucoup d'argent. Nous ne savons pas encore tout à fait quelles qualités exactes nous souhaitons pour la monnaie idéale, car au cours des deux mille dernières années où nous avons utilisé des pièces de monnaie, nous n'avons jamais été autorisés à mener d'expérimentations. Nous n'avons jamais eu la chance de déterminer quel serait le meilleur type de monnaie*.

« *Je pense que nous devrions commencer ces réflexions rapidement et que nous devons espérer que certains des financiers les plus entreprenants et les plus intelligents vont bientôt commencer à expérimenter de nouvelles monnaies. Le grand obstacle à cette*

réalisation, ce sont les grands changements qu'elle portera aux structures du monde financier et, je dis cela de l'expérience de nombreuses discussions, aucun banquier expérimenté ne comprend vraiment le système bancaire actuel, ne peut vraiment imaginer comment un nouveau système fonctionnerait et n'oserait prendre le risque de mener une expérimentation de nouvelle monnaie. Je pense que nous devrons compter sur quelques cerveaux plus jeunes et plus agiles pour démarrer cette révolution et réaliser que de telles choses sont possibles[15]. »

Quelques décennies plus tard, le rêve de Hayek semble avoir été accompli à travers l'expérience du bitcoin. Semblait-il pourtant si difficile de faire l'expérience de nouvelles monnaies alors que les crises se répètent depuis plusieurs décennies ? Le statisme de l'institution financière semble prouver les craintes de Hayek. L'irruption du numérique dans le champ de la monnaie invite à une véritable révolution des esprits. Pour l'avocat français Hubert de Vauplane, la définition du bitcoin répond en effet à ces aspirations de dénationalisation de la monnaie : « *Qu'est-ce que le bitcoin ? Techniquement, c'est un protocole technique. C'est un réseau de transactions sur Internet complètement décentralisé, pair-à-pair (peer-to-peer) et open source. C'est également une unité de compte qui circule sur ce réseau. Le système lui-même n'appartient à personne d'autre qu'à ses utilisateurs et l'usage qu'ils font de ce réseau. Si le bitcoin n'est ni une monnaie, ni un instrument de paiement. Comment le droit appréhende-t-il les bitcoins ? Tout comme le pensaient de la Nature les philosophes de l'Antiquité, le droit a horreur du vide. Il n'est donc, en principe, pas de domaine qui puisse lui échapper. Et pourtant, le bitcoin est un OVNI juridique et fiscal*[16]. »

Bitcoin au pays des entrepreneurs

En 2014, j'ai eu l'honneur d'être invité à participer au *Spring Campus* de Croissance Plus, une conférence internationale réunissant plus de 400 dirigeants français et étrangers autour d'ateliers interactifs et de rencontres informelles. Frédéric Bedin, l'organisateur du campus, m'avait demandé de parler des crypto-monnaies et plus

particulièrement du bitcoin. Dans ce temple de l'entreprenariat, placé sous les auspices de la thématique « L'entrepreneur, un aventurier du XXIe siècle », je me suis mis en tête de démontrer que la création d'une nouvelle monnaie se devait d'être le trophée convoité par tout Indiana Jones des temps modernes.

Croissance Plus, co-fondée puis présidée par mon associé Bruno Vanryb, n'est pas à son coup d'essai dans sa réflexion sur la disruption numérique. Mon exposé intervenait en effet dans une réflexion générale sur le monde nouveau que la transition numérique offre à notre économie et notre société. Dans cet univers, le principe d'autorité centrale ou de tiers de confiance n'a plus forcément de place et un échange de valeur peut pleinement reposer sur un algorithme mathématique ou un consensus de milliers d'ordinateurs épars. La confiance y règne comme principe directeur, un concept nouveau et parfois dérangeant.

La veille de mon intervention, pris à part par plusieurs participants pour connaître mon opinion en *off*, loin des micros et des projecteurs, je réalisai toute la méfiance générée autour du bitcoin. « Je n'ai toujours rien compris à ton bitcoin ! », « C'est une arnaque, non ? », « Un repère de dealers où s'échangent des billets de Monopoly et de l'argent sale ». Mon auditoire ne serait, *a priori*, pas facile à convaincre et reposer les fondamentaux du sujet, donner à chacun les clés de compréhension essentielles, me semblait la première étape de l'ouverture du dialogue avec ces professionnels. Sauf exception, la classe politique française partage les mêmes craintes : les députés Laure de La Raudière et Laurent Grandguillaume m'ont fait part de leurs sentiments à ce propos, se montrant des observateurs prudents mais aussi passionnés des révolutions de la blockchain. Dans ma conclusion, après un quart d'heure d'exposé, il m'est laissé quelques minutes pour fixer trois horizons de transformation.

Le premier, c'est l'application de la technologie blockchain du champ restreint de la monnaie à l'ensemble de l'économie : assurance, actionnariat, contrats intelligents, financement participatif, etc. J'y reviendrai, d'ailleurs, plus longuement. Le deuxième, c'est la mobilisation de cette technologie dans une atmosphère générale de défiance à l'égard des institutions bancaires et de recherche de services financiers à moindre coût. Le troisième, enfin, l'argument le plus

important d'un certain point de vue, c'est l'accès aux services numériques de 3,5 milliards d'êtres humains aujourd'hui sans banque et pourtant en demande de services bancaires et financiers. La technologie blockchain peut nous permettre de relever ce défi et d'accompagner ces individus.

Cette introduction à la technologie blockchain, trop brève tant le sujet est complexe, a donné lieu à plus d'une heure de questions : de l'activité de minage à la conversion en devise courante, en passant par l'usage des ordinateurs privés. Mes auditeurs hier inquiets se montraient aujourd'hui intrigués, voire, mieux, passionnés ! J'avoue avoir été parfois, moi-même, à court de réponses, me limitant alors à donner quelques principaux points de repère. Une heure d'échange trop courte mais une heure d'échange et d'invitation à l'aventure de ces entrepreneurs, économistes ou encore chercheurs, à la recherche d'un nouveau modèle d'échange entre les hommes. Car les crises économiques et financières des trois dernières décennies nous l'ont montré avec une certaine violence : nous devons changer ou disparaître.

Les crises monétaires des années 1990

À partir des années 1980, les crises monétaires se succèdent à un rythme de plus en plus rapide. En 1985, sujette à un problème informatique, la Banque de New York est ainsi forcée d'immobiliser son système de règlement-livraison et accuse une perte de 20 milliards de dollars. En 1989, le marché américain est de nouveau agité par une crise spéculative sur les « *junk bonds* » (obligations pourries, en français), des obligations à haut risque soudainement dévaluées, puis le Japon est à son tour perturbé par une bulle spéculative autour de l'immobilier national. Quant à l'actualité internationale de cette fin de guerre froide, elle pèse aussi sur les grands équilibres monétaires et financiers de la planète.

En 1990, l'invasion du Koweït par l'Irak déclenche une panique boursière à cause de l'évolution rapide du prix du pétrole. En 1992, le Système monétaire européen est percuté de plein fouet par l'annonce du traité de Maastricht. Les grands fonds d'investissement parviennent

alors à extraire la livre sterling du marché de change mais échouent à faire de même avec le franc français. En 1993, une nouvelle opération vise la parité entre le deutschemark et le franc français, créant une nouvelle panique boursière en Europe. À la suite de ces errements européens, trois crises incarnent la rupture monétaire des années 1990.

En 1994, d'abord, la crise économique mexicaine, rebaptisée « crise tequila », met fin à un système de garantie du peso mexicain sur le dollar. Le haut niveau d'inflation national ne permet en effet plus de garder une relation de garantie de change entre les deux monnaies. En réponse, plus de 90 milliards de dollars de liquidités étrangères sont insufflés dans le système, conduisant à une hausse des crédits bancaires de 25 % par an, mais l'inflation continue et le manque de compétitivité font que le pays rate le coche. La croissance ne redémarre pas et les investisseurs étrangers retirent leurs capitaux. En décembre 1994, le président américain Bill Clinton annonce donc un prêt historique de 50 milliards de dollars pour sauver son voisin de la crise de ses taux d'intérêt.

En 1997, trois années plus tard, une crise identique survient en Asie – le baht thaïlandais, que l'on a présenté plus haut comme l'une des plus vieilles monnaies au monde, n'est plus capable d'assurer sa conversion en dollar américain, ce qui donne lieu à plusieurs vagues de spéculation étrangère dans le pays. Les banques asiatiques empruntent à court terme des dollars américains pour prêter à long terme en monnaie locale, assurant la garantie de leurs prêts sur l'immobilier. Au terme de ce cycle, les investisseurs étrangers cessent brutalement leur politique d'investissement mais l'immobilier local ayant été surévalué, les banques ne sont pas capables d'effacer l'ardoise et le pays sombre dans une crise financière et monétaire en juillet.

En 1998, l'année suivante, c'est le géant de la guerre froide, la Russie postsoviétique, qui enregistre une crise comparable. En effet, après la crise asiatique de 1997, la Russie a enregistré une perte au niveau de ses échanges commerciaux de pétrole et de métaux avec les pays asiatiques et, soumise à une inflation de 84 %, elle a été obligée de dévaluer sa monnaie nationale, le rouble. Le pays est alors dans une phase de forte instabilité politique et sociale, la valse des ministres répondant aux grèves à répétition des mineurs et des ouvriers. Heureusement, cette dévaluation du rouble redonne des arguments à la

compétitivité internationale de la Russie, ce qui la sauve de l'explosion économique et politique, mais la modernité des crises monétaires n'est plus à prouver.

Dans *The Future of Money* (2001), l'économiste et universitaire belge Bernard A. Lietaer, ancien haut fonctionnaire à la Banque centrale de Belgique, aujourd'hui défenseur des monnaies complémentaires et régionales, écrit ainsi : « *Les crises monétaires mondiales des années 1990 (Russie, Mexique, Asie et Brésil) ont prouvé que notre système monétaire était malade, et que cette maladie affectait tout le monde. Après tout, la monnaie joue le rôle de système d'information central dans notre société moderne, une sorte de système nerveux de nos propres corps. Afin de prévenir un effondrement mondial de la monnaie, une vision unique d'abondance durable et des mécanismes afférents doivent donc être pensés.* »

Les banques centrales nationales et européenne

La mise en place d'une monnaie commune européenne, l'*European Currency Unit* (ECU) dès 1979 puis l'euro à partir de 1999, change la règle monétaire internationale et impose un nouvel environnement aux politiques monétaires. La Banque centrale européenne (BCE), établie en juin 1998, est ainsi chargée de battre monnaie et d'en fixer les taux, avec un objectif final de maintien du pouvoir d'achat dans l'ensemble des pays d'usage de la monnaie, la « zone euro ». Son capital est détenu par les banques centrales nationales de la zone et, de façon minoritaire, par les banques centrales des pays de l'Union européenne hors zone euro.

La banque centrale dispose d'une gouvernance indépendante à l'égard des États, avec un directoire composé du président, Mario Draghi depuis janvier 2013, du vice-président et de quatre membres choisis pour leur haute expérience en matière monétaire. Le poids de la nationalité d'appartenance dans la nomination de ces membres reflète, aujourd'hui, celui de certaines économies dans la zone euro : les quatre membres sont en effet un Français, un Allemand, un Belge et un Luxembourgeois. En outre, depuis 1997, les représentants politiques de la zone euro se réunissent au sein de l'Eurogroupe, une formation du

Conseil européen officiellement reconnue en 2008. Le nouveau rôle des banques centrales nationales est donc largement restreint et, somme toute, confiné à servir d'administration et de réglementation dans chacun des pays.

Le poids de la BCE, superstructure technocratique au sommet des institutions européennes, est donc un élément à même d'être interrogé. Participe-t-il au déficit démocratique de l'Union européenne ? Quels sont ses plans à moyen terme ? Aide-t-elle simplement à la création d'une union bancaire, monétaire, économique, et finalement politique, en Europe ? Réalise-t-elle vraiment ses objectifs en accord avec le Parlement européen et les parlements nationaux ? Si les intentions de la BCE sont louables, le manque d'implication des citoyens européens dans sa gouvernance est un point d'achoppement. La relance d'un processus de contrôle budgétaire des États sur les mécaniques européennes reste un fantasme distant, la création d'un Comité budgétaire européen consultatif, n'étant ainsi prévue que pour 2025…

La dette publique, une longue histoire

La situation des pays au lendemain de la guerre froide est d'autant plus délicate que beaucoup d'entre eux ont atteint un niveau critique de dette publique. Dès le Moyen-Âge, au XII^e^ siècle, les cités européennes ont eu recours à des emprunts à court terme mais à taux élevé pour sauver l'équilibre de leurs finances publiques. À Florence, en Italie, la dette de la cité était même gérée par un établissement public créé spécialement pour suivre ce dossier, le Monte. De nombreuses cités s'enfermaient alors dans le piège des « emprunts perpétuels », empruntant de nouveau pour rembourser un emprunt passé arrivé à échéance. Ce système permettait de ne payer que des intérêts modérés en continu, alors que les grands États de l'époque étaient parfois soumis à des remboursements très élevés.

Au XVI^e^ siècle, la monarchie française accroît considérablement sa dette afin de répondre à ses nouvelles ambitions militaires et, au XVII^e^ siècle, elle met en place le système de la vente des offices vénaux, duplication de ce système de dette au niveau national grâce auquel elle vend des titres de noblesse et des responsabilités à titre provisoire

contre monnaie sonnante et trébuchante. La crise financière du royaume de France devient cependant de plus en plus insoutenable, à mesure que les dépenses s'accroissent et que les recettes faiblissent. Elle sera la cause de la Révolution française de 1789. En Angleterre, entre 1688 et 1702, la dette est ainsi passée de 1 à 16,48 millions de livres, puis 133 millions de livres en 1766.

Au XIX^e^ siècle, les États s'engagèrent à lutter plus efficacement contre la banqueroute – la dernière banqueroute française datait alors de 1796. Au XX^e^ siècle, alors que les Première et Seconde Guerres mondiales appelaient à davantage de dépenses publiques, les États s'endettèrent considérablement : en France, en 1921, la dette publique rapportée au PIB s'élevait à 270 %, puis 100 % en 1929, au moment de la grande crise économique et financière. La forte croissance économique des Trente Glorieuses permit néanmoins d'assumer le coût de cet endettement public : à la fin des années 1970, la dette publique s'était ainsi stabilisée autour de 21 %. Avec les deux chocs pétroliers des années 1970, les gouvernements choisirent néanmoins de laisser filer la dette pour relancer l'économie par la croissance, tout en restant relativement prudents.

Les choses s'emballent néanmoins de nouveau dans les années 1990 : 35,4 % en 1990, 40 % en 1992, 49,6 % en 1994, 59,7 % en 1996, 61 % en 1998, avant de retomber à 58,7 % en 2000, après de courageux efforts de l'administration des finances publiques. Le repos n'est cependant que de courte durée, car la dette remonte à 64 % en 2007, puis 79 % en 2009, après la crise économique et financière de 2008, 85,2 % en 2011, 92,4 % en 2013 et finalement 96,2 % en 2016, en dépit de tous les objectifs européens et nationaux de réduction de la dette. Il faut reconnaître que l'actualité se prête difficilement aux réductions de dépense publique, alors que le contexte d'insécurité invite au contraire à davantage d'action publique, ce qui a amené le président François Hollande à affirmer devant le Parlement, en novembre 2015, que « *le pacte de sécurité* [devait] *l'emporter sur le pacte de stabilité* [des finances publiques] ».

La théorie des jeux, une explication scientifique

Ces phénomènes d'échange de monnaie ou d'endettement des États ont été longuement étudiés par les économistes au cours des siècles passés. La théorie des jeux, inventée par Ernst Zermelo, Émile Borel et John von Neumann dans les années 1920, tâche de comprendre ces mécanismes à la fois économiques et psychologiques. Comment les acteurs de la vie économique prennent-ils une décision rationnelle ? Sur le fondement de quels arguments ? Comment l'interaction entre deux agents d'un même univers économique joue-t-elle sur les décisions prises ? Quelle stratégie optimale pour maximiser le profit de deux agents engagés dans une seule et même négociation équilibrée ? Bref, quel équilibre entre les intérêts de chacun ?

La théorie des jeux pose le postulat de base suivant : il existe des acteurs économiques non coopératifs, avec des buts opposés, et des acteurs économiques coopératifs, pouvant établir un juste milieu entre leurs intérêts distincts. En 1950, l'économiste américain John F. Nash pose ainsi les bases de la théorie dite du dilemme du prisonnier. Deux hommes y sont arrêtés par la police à l'issue d'un braquage de banque, avec deux issues possibles à leur interrogatoire par les forces de l'ordre, soit la coopération avec leur complice (C), c'est-à-dire le silence complet avec une peine d'un an de prison pour chacun, soit la dénonciation de leur complice (D), en échange d'une remise en liberté négociée pour celui dénonçant son complice en premier.

Ce tableau donne donc lieu à quatre hypothèses conclusives : les deux prisonniers peuvent s'entraider et refuser de coopérer (C/C), subissant donc chacun une peine d'un an de prison ; ils peuvent également se dénoncer mutuellement pour espérer une remise de peine (D/D), subissant tous les deux une peine de dix ans de prison puisque s'étant mutuellement trahis ; enfin le premier prisonnier peut coopérer et le second le dénonce (C/D), subissant seul une peine de vingt ans de prison alors que son complice est libéré, ou *vice versa* (D/C). Dans les deux situations où les prisonniers adoptent des comportements différents (C/D et D/C), l'intérêt de l'un est préféré à celui de l'autre, mais dans les deux situations où les prisonniers adoptent des comportements identiques (C/C et D/D), une sorte d'équilibre est obtenue.

Nash s'attache alors à évaluer l'optimum de cette négociation, dans lequel tous les acteurs économiques maximisent leurs gains : l'équilibre

est obtenu en situation C/C puisque les deux braqueurs ne sont condamnés qu'à une année de détention. Cette situation est obtenue par une confiance réciproque entre les deux hommes. Révolutionnaire dans le champ de l'économie, cette théorie nourrit aujourd'hui le courant de la neuroscience, qui étudie nos stimulations neuronales face à une situation de décision économique. Quant à Nash, le réalisateur Ron Howard lui a consacré un film bouleversant, *Un Homme d'exception* (2001), dans lequel il est incarné par Russell Crowe à l'écran, dans un jeu à la fois grave et drôle.

La théorie de jeux met finalement en exergue l'importance de l'information dans une négociation économique et commerciale. Dans des cellules séparées, les deux malfaiteurs doivent faire confiance à leur complice sans connaître le comportement adopté par celui-ci : si le complice est honnête et s'en tient au silence, ils ne feront tous les deux qu'une peine d'un an de prison, mais si le complice entend maximiser son profit, en d'autres termes obtenir sa liberté immédiate, il pourra être poussé à la trahison. L'économie repose donc, avant toute chose, sur la notion de confiance entre les acteurs d'un même système économique. On verra, plus tard, que le problème de l'attaque des généraux byzantins répond sensiblement aux mêmes règles.

La naissance de la monnaie s'inscrit ainsi dans cette démarche théorique. L'utilisation des pièces ou des billets repose sur la confiance des acteurs économiques en la valeur de ces unités d'échange. Lorsque les acteurs n'ont plus confiance en leur monnaie, au sens large du terme, ils reviennent à des unités auxquelles ils font davantage confiance : c'est l'explication des banqueroutes bancaires et financières causées par la demande d'échange des billets contre de l'or au cours des derniers siècles. Pour soutenir la monnaie, l'économie a donc besoin d'institutions de confiance.

La crise de 2008-2010, ultime érosion de la confiance

Après les crises monétaires des années 1990, le monde a retenu son souffle, l'espace de quelques années, avant de replonger dans une terrible crise économique et financière, à l'automne 2008. La désormais

célèbre crise des *subprimes* de 2006-2007 avait en effet encouragé les banques à prêter massivement aux ménages, en indexant les prêts bancaires sur la valeur des hypothèques immobilières. Le dégonflement de la bulle immobilière américaine, c'est-à-dire la prise de conscience de la surévaluation du patrimoine immobilier des ménages américains endettés, a placé les banques dans une situation critique de remise en question de l'équilibre de leurs finances.

Cette perte de confiance a engendré une évaporation rapide des liquidités : devant l'hypothèse d'une faillite bancaire, crainte nourrie par les médias de l'époque, les ménages ont massivement retiré leurs économies des banques, aggravant la situation en l'état. En septembre 2008, incapable de solder ses crédits immobiliers à risque et en proie à une chute continue de sa capitalisation boursière, la banque américaine Lehman Brothers se déclare en faillite, créant un vent de panique sur les marchés boursiers. Les États engagent en conséquence une politique de recapitalisation massive des banques, à l'appui des banques centrales et de vastes plans de sauvetage.

En 2009, la Banque centrale américaine annonce ainsi avoir injecté 9 000 milliards de dollars de liquidités dans le système bancaire. La politique de soutien public des banques aggrave alors considérablement l'état de la dette publique des États concernés. En un an, la dette nette des États-Unis passe ainsi de 10 600 à 11 300 milliards de dollars. En France, le coût de la première opération de sauvetage public des banques s'élève à 360 milliards d'euros, suivie d'un second plan, en janvier 2009, de 10 milliards d'euros supplémentaires.

En Grèce, la convergence de la crise économique et financière de 2008 et d'un fort niveau d'endettement public conduit à une situation exceptionnelle : en avril 2010, le pays est finalement obligé de demander une aide exceptionnelle au Fonds monétaire international et à l'Union européenne, faute de quoi le règlement de sa dette serait placé en défaut de paiement, c'est-à-dire en incapacité de remboursement. Un premier accord est ainsi négocié en mai 2010, en échange d'un engagement du pays à mener des mesures structurelles de réforme (consolidation du système d'impôt, restructuration du régime des retraites), mais l'aide internationale s'avère rapidement insuffisante.

En mai 2011, la Grèce se trouve de nouveau au bord du gouffre

financier et les pays européens hésitent à mettre en œuvre une nouvelle aide exceptionnelle, dénonçant le comportement déraisonné de certaines banques depuis le printemps 2010. Les banques locales ferment donc boutique, les distributeurs automatiques sont fermés, les pensions de retraite gelées puis brutalement baissées. La pression de la rue s'accroît chaque jour, les manifestations publiques se multiplient et, le 21 juin, l'Organisation des Nations unies accuse une situation de baisse des finances publiques, néfaste à l'emploi et aux dépenses sociales. Un second plan de sauvetage du pays est mis sur pied en juillet 2011, 109 milliards de dollars du Fonds européen de stabilité financière et du Fonds monétaire international sont dirigés vers la Grèce.

Le renouveau de la régulation bancaire

Dès octobre 2008, dans une tribune au *Monde*, les économistes français Christian de Boissieu et Jean-Hervé Lorenzi appellent à une « refondation du système bancaire et financier international », en clair à un Bretton Woods II. Le G20 de Washington, en novembre 2008, est une première étape dans la mise en œuvre de nouvelles règles de l'architecture financière internationale : amélioration de la transparence des systèmes comptables des banques, renforcement du contrôle prudentiel avec une révision des normes régissant les agences de notation, amélioration de la régulation financière internationale, renforcement de la capacité des institutions financières internationales à aider les économiques en difficulté, etc.

Lors des accords de Bâle III, en décembre 2010, un nouveau chapitre de la régulation bancaire internationale est amorcé : les banques sont désormais sommées de garantir un niveau minimum de capitaux propres afin d'éviter la crise de banques illiquides survenue en 2008-2010. Trois principes clés sont ainsi mis en œuvre à l'horizon 2013 : l'instauration d'un ratio minimum de liquidités pour les grandes banques internationales, la création de « coussins de sécurité » supplémentaires pour les banques aux activités les plus risquées, et la redéfinition des fonds propres. Au sein de l'Union européenne, les accords sont transcrits dans la directive CRD IV de juillet 2011.

Le continent européen se prête aussi au jeu d'un meilleur encadrement de l'activité bancaire. Désormais, la rémunération variable des traders, en fonction de leurs bons chiffres, ne peut plus dépasser 100 % de leur rémunération fixe. Le rapport Liikanen de 2012, commandé par la Commission européenne, invite en outre à mener des réformes structurelles du secteur bancaire européen afin de séparer les activités risquées des activités de dépôt. Il s'agit d'éviter que l'argent du contribuable soit engagé pour sauver les activités bancaires risquées. En France, l'idée de cette séparation est appliquée par une loi de janvier 2013, relative à la séparation des activités du secteur bancaire.

Dans l'optique de renouveau de la confiance dans les institutions, cette loi de janvier 2013 renforce les pouvoirs de l'Autorité de contrôle prudentiel et de résolution et met en place un Conseil de stabilité financière, afin d'imposer des exigences contraignantes à l'activité des banques. À sa suite, la directive européenne *Market in Financial Instruments Directive* (MiFID) d'avril 2014 a accru les règles en matière de transparence des marchés et de concurrence entre les plateformes boursières, et la directive Abus de marchés de 2002 a été révisée afin de sanctionner plus durement les opérations de délit d'initié. Le nouvel angle de la régulation des marchés financiers est donc celui de la protection des investisseurs et du renforcement des moyens de sanction à l'égard des banques.

En France, ces nouveaux régulateurs de la vie économique et sociale prennent la forme d'autorités administratives indépendantes (AAI), des institutions chargées d'agir au nom de l'État afin d'assurer la régulation d'un secteur donné, sans pour autant être soumises à l'autorité hiérarchique d'un ministre. Cette indépendance se veut le gage d'une certaine liberté d'action, en rupture avec l'image d'un gouvernement tout-puissant. Créées par une loi de janvier 1978, les AAI répondent ainsi au besoin de davantage d'impartialité dans la vie publique, mais aussi à la mobilisation de professionnels dans certains secteurs techniques.

Dotées de pouvoirs propres, ces autorités peuvent émettre des avis ou des recommandations, voire détenir des pouvoirs de réglementation avec une portée limitée. Ainsi, l'Autorité des marchés financiers (AMF) peut infliger des amendes importantes en cas de non-respect des règles de son secteur, par exemple en cas de violation des règles

boursières. À l'identique, le Conseil supérieur de l'audiovisuel (CSA) peut interdire la fusion de deux chaînes de télévision ou suspendre l'autorisation d'émission d'une émission de radio ou de télévision pour non-respect des règles élémentaires du journalisme. La multiplication de ces AAI témoigne de la démarche des pouvoirs publics à s'engager vers plus de transparence, bien que ces institutions demeurent encore très technocratiques.

Réguler les banques et la dette

La problématique de la dette a pâti de la crise économique et financière de 2008-2010. Les pays les plus précaires structurellement parlant ont ainsi eu de nombreuses difficultés à remonter la pente. Depuis l'arrivée du gouvernement Syriza au pouvoir, en Grèce, en janvier 2015, la question des réformes imposées en échange des plans de sauvetage a ainsi été remise sur le tapis. Au moment de son élection, le mouvement d'Alexis Tsipras, devenu Premier ministre, a en effet mis en avant l'hostilité du peuple grec au programme de réformes imposé par les bailleurs internationaux, et le référendum national de juillet 2015 a confirmé cette colère populaire à l'égard des institutions étrangères. La question de la souveraineté nationale a ainsi percuté de plein fouet le pouvoir détenu par les créanciers du pays.

Le fait que le gouvernement grec ait finalement accepté un plan de sauvetage sujet à des obligations de réforme quasi identiques a fait couler beaucoup d'encre. L'hypothèse d'un effacement de la dette grecque a, un temps, été envisagée, avant d'être repoussée par l'Allemagne. En 1996, l'initiative pays pauvres très endettés (PPTE) avait pourtant fait de même en supprimant la dette d'une trentaine de pays pauvres, essentiellement en Afrique, afin d'encourager la reprise de leur croissance économique. Vingt ans après, dans une synthèse inquiétante, le Trésor français note que de nombreux pays sont retombés dans l'écueil de l'endettement massif, soumis au cycle infernal du prix des matières premières.

L'effacement de la dette est un principe ancien, d'ailleurs inscrit dans les écrits bibliques, qui a donné lieu à de nombreuses pratiques au cours des deux siècles passés : Mexique et Cuba, à la fin du XIX^{e} siècle,

Union soviétique en 1918, au lendemain de la Première Guerre mondiale, République fédérale d'Allemagne en 1953, en pleine guerre froide, ou encore Égypte en 1991, au moment de la première guerre du Golfe. Plus récemment encore, en 2008, l'Islande a refusé de régler une partie de sa dette à des créanciers étrangers à la suite d'une forte mobilisation populaire. L'hypothèse d'un nouvel effacement de la dette publique n'est donc pas absurde : « *Concrètement*, écrit le professeur Bruno Colmant, dans une tribune dans les *Échos* de septembre 2015, *si l'absence d'accès aux marchés financiers de certains pays du sud de l'Europe se confirme, il faudra alors se préparer à un effacement des dettes. Ce ne sera pas un défaut généralisé de la dette européenne, mais des dissolutions et des compensations nationales de dettes. Il s'agira de défauts "internes", comme la Russie l'a effectué en 1998, sous forme d'un probablement ré-échelonnement (c'est-à-dire d'une prolongation forcée des maturités) des dettes publiques avec un allongement simultané des engagements vis-à-vis des assurés et des pensionnés (les capitaux se transformant en rente, etc.).*

« *Ce scénario d'effacement des dettes n'est plus de la science-fiction car de nombreux indices sont décelables. Parmi ces derniers, les dettes publiques ont re-migré vers leur pays d'origine (la dette publique portugaise a été rachetée par des banques portugaises, etc.). Les transferts financiers du nord vers le sud ont été parcimonieux, tandis que l'idée d'eurobonds a été écartée. Cela rejoint la logique allemande, qui veut que les dettes d'un pays soient strictement financées par l'épargne domestique.* »

En 2014, Yanis Varoufakis le tumultueux et éphémère ministre des Finances grec du gouvernement Tsipras, va alors proposer de mettre en place une monnaie complémentaire, le *FT Coin* (*Future Tax Coin*), destinée à éteindre des dettes fiscales de son pays. Il imagine ainsi créer une économie à deux monnaies (euro et FT Coin), capable de capter l'épargne nationale et de lui donner un avantage fiscal. Bien que fortement centralisé, le nouveau système est très tôt apparenté à une crypto-monnaie et plusieurs articles de l'époque font état d'une prochaine introduction du bitcoin comme monnaie officielle dans la péninsule hellénique. Un fantasme toutefois bien vite oublié.

Le retour aux monnaies locales

Ce retour à l'épargne domestique, à la monnaie nationale est aussi la matrice de naissance des monnaies locales. Depuis plusieurs années, en effet, des deux côtés de l'Atlantique, des monnaies locales font leur apparition, en complément de la monnaie nationale. En France, depuis janvier 2013, le Pays basque est ainsi le lieu d'échange de l'*eusko*, utilisé par plus d'un demi-millier de commerçants locaux pour soutenir le commerce de proximité et les circuits courts, à la fois bons pour l'environnement et pour l'emploi local. Dès 2010, la commune de Villeneuve-sur-Lot avait fait sienne cette idée de monnaie locale, avec l'Abeille, suivie de Roanne avec la Commune, de l'Ardèche avec la Luciole ou encore de Toulouse avec le Sol-Violette. « *L'intérêt d'une monnaie locale est de renforcer le commerce de proximité, menacé par les grandes surfaces et le développement du e-commerce sur Internet*[17] », explique ainsi Dante Edme-Sanjuro, co-président de Euskal Moneta.

L'utilisation de l'eusko est tolérée par le Code monétaire et financier français, à condition qu'il ne circule qu'entre les membres de l'association Euskal Moneta, à l'origine de cette monnaie locale. Comme l'adhésion à l'association est à la fois libre et gratuite, la monnaie locale ne connaît pas d'entrave juridique à son développement. Toutefois, cet encadrement permet au législateur de s'assurer un certain contrôle sur le développement futur de cette monnaie, en le circonscrivant à un espace local, et ainsi de préserver l'euro, comme monnaie unique de l'espace européen.

À son lancement, un peu moins de 350 000 euskos ont été mis en circulation et cette initiative a suscité la création d'une mission interministérielle d'étude des monnaies locales complémentaires par le gouvernement de Jean-Marc Ayrault. Ces systèmes d'échange locaux sont en effet un outil pratique de l'encouragement à l'économie circulaire prônée par l'actuel pouvoir en place. La politique d'accompagnement de l'économie locale, le « Made in France » vanté par les anciens ministres Yves Jégo et Arnaud Montebourg, a en effet tout à gagner du développement de ces monnaies locales.

En octobre 2015, à l'identique de l'initiative basque, Strasbourg a lancé le *stück*, une monnaie locale visant à alerter sur les

conséquences de la consommation au niveau de l'économie locale. Environ 100 000 stücks ont été mis sur le marché par le Crédit municipal et l'association Nouvelle économie fraternelle, pour une valeur globale de près de 100 000 euros. Une centaine de commerces pratiquent aujourd'hui son utilisation limitée aux membres de l'association Le Stück. Contrairement à l'eusko, l'inscription est payante (entre 5 et 20 euros pour les consommateurs, entre 20 et 200 euros pour les professionnels), ce qui limite donc l'usage populaire du nouveau dispositif.

En Bretagne, une demi-dizaine de monnaies locales circulent aujourd'hui : le *heol*, le *buzuk*, le *galleco* ou encore la *bigaille*. Elles servent de monnaie de paiement pour les clients, de monnaie d'achat auprès des producteurs locaux, mais aussi de monnaie de salaire auprès des employés. La prochaine étape de transformation de ces monnaies locales est leur numérisation et le bitcoin entre, ici, en phase avec cette thématique, fort de ses quelques années d'existence et de son expérience pratique. Les fondateurs brestois de l'heol envisagent ainsi de mettre en œuvre un paiement numérique basé sur leur devise bretonne, au risque de perdre le contact physique avec la monnaie mais avec l'ambition de renforcer le réseau des utilisateurs.

Soyons toutefois réalistes et très directs, les monnaies complémentaires sont aujourd'hui encadrées de façon à n'avoir aucun avenir. Elles sont retenues au sol par deux contraintes majeures : d'une part, leur obligation d'être circonscrites à un territoire limité géographiquement, et de ce fait de ne participer qu'à l'activité d'un seul territoire ; d'autre part, leur centralisation naturelle et donc l'adoption d'un modèle déjà rejeté par les populations. Ces monnaies locales sont vouées à disparaître avec la fin des transactions liées car, contrairement aux crypto-monnaies, il n'est pas possible de les thésauriser.

La monnaie est-elle encore un bon indicateur de la richesse ?

La richesse d'une nation a longtemps été mesurée à hauteur de sa capacité à faire croître ses réserves d'argent et de ressources, d'où

l'usage du produit intérieur brut pour comparer les nations à l'aune d'un indicateur commun. Dans les années 1960 et 1970, les économistes commencèrent cependant à introduire la notion de bien-être dans leurs travaux, mesurant les retombées sociales de certaines politiques publiques. La richesse ne se mesure dès lors plus au seul stock de valeurs accumulées, mais aussi au regard des conditions de vie de la population ou des inégalités. Au début des années 1980, dans un essai intitulé *Pauvreté et famines* (1981), l'économiste indien Amartya Sen fait ainsi connaître ces théories du grand public.

En 1990, à l'invitation de l'économiste pakistanais Mahbub ul Haq et d'Amartya Sen, des économistes du monde entier s'associent pour rédiger un *Rapport sur le développement humain*, sous l'égide de l'Organisation des Nations unies. Présenté à l'Assemblée générale des Nations unies et depuis conduit annuellement dans plus de 140 pays, le rapport s'interroge en permanence sur la pertinence de la monnaie comme marqueur de la richesse nationale et de la richesse individuelle des habitants de notre planète : « *Les revenus ont d'abord été développés comme un moyen de mesurer le bien-être et la protection sociale par Pigou, qui a décrit l'économie du bien-être comme une part mesurable du bien-être humain – la part qui peut être mise en relation avec "la barre mesurable de la monnaie"* (measuring rod of money). [...] *En cherchant à mesurer le prix du panier de consommation d'un ménage pauvre, il apparaît que les achats non alimentaires sont les moins importants. Ce problème est fréquemment souligné par la multiplication de l'argent nécessaire à l'achat de la nourriture dans le panier de consommation, selon un coefficient connu sous le nom de coefficient d'Engel, le ratio des dépenses en nourriture sur le total des dépenses*[18]. »

La monnaie ne mesure donc pas complètement la richesse de l'individu, dont les schémas de consommation sont aussi guidés par sa place dans l'économie et dans la société. En 1990, Amartya Sen a donc développé un nouvel indicateur de croissance des pays, l'indice de développement humain (IDH), basé sur le PIB par habitant, c'est-à-dire la répartition de la richesse nationale entre les habitants, l'espérance de vie à la naissance et le niveau d'éducation. Ce nouvel outil statistique a révolutionné l'approche de l'économie de la richesse. À sa suite et avec son concours, en 2009, les économistes Joseph Stiglitz et Jean-Paul

Fitoussi ont publié un nouveau rapport consacré, cette fois, à la mesure des performances économiques et du progrès social, invitant à mesurer la richesse à l'aune d'autres éléments[19].

La France s'est aussi penchée sur cette question des indicateurs de richesse, constatant que le rapport Sen-Stiglitz-Fitoussi de 2009 n'avait pas suffisamment défini de nouveaux indicateurs pour mesurer la croissance. En 2014, le gouvernement socialiste a donc chargé France Stratégie, un organe de réflexion placé auprès du Premier ministre, et le Conseil économique, social et environnemental (CESE), de rédiger un rapport sur « les nouveaux indicateurs de richesse ». Le 13 avril 2015, le Parlement a complété cette ambition à l'appui d'une loi, garantissant un suivi régulier de cette mission d'édiction de nouveaux indicateurs, avec la publication d'un rapport annuel sur les récentes découvertes.

Les dix nouveaux indicateurs proposés par France Stratégie et le CESE en 2015 sont le taux d'emploi, l'effort de recherche (public et privé), l'endettement, l'espérance de vie en bonne santé, la satisfaction dans la vie, les inégalités de revenus, la pauvreté en conditions de vie, les sorties précoces du système scolaire, l'empreinte carbone et l'artificialisation des sols. Certains de ces éléments sont ainsi purement subjectifs et prêtent à débat au sein de la communauté scientifique. La monnaie, en tant que mesure de l'accumulation des richesses, n'apparaît donc plus comme un indicateur fixe de la richesse des individus – les conditions et le temps de travail, l'accès aux services publics et aux loisirs paraissent des indicateurs plus fins de l'économie du bien-être.

Numériser la monnaie, est-ce pourtant une solution ? Au lendemain de la crise économique et financière, l'idée d'une monnaie numérique non régulée peut interroger le grand public. Alors que les banques sont soumises à davantage de contrôle, que les institutions de surveillance et de supervision se multiplient, comment imaginer le fonctionnement d'une monnaie décentralisée, sans contrôle des banques centrales ? Pour Michael Parsons, l'un des cadres de KPMG Moscou, le bitcoin n'échappe pas complètement à la régulation et a donc les moyens techniques de s'imposer comme une monnaie internationale : « *Le bitcoin est régulé par ses pairs et par les mathématiques*, explique-t-il. *C'est un système de transferts de valeurs, dans lequel la valeur est donnée par les utilisateurs*[20]. »

Le bitcoin a-t-il une valeur juridique ?

La révolution bitcoin, dans le sillage des expériences passées de la *b-money* (1999) ou du BitGold (2005), a résolu la problématique de la traçabilité des paiements. En août 2013, le Sénat américain a décidé l'ouverture d'une commission sur les monnaies virtuelles, afin d'accompagner les autorités fédérales dans la reconnaissance juridique de cette crypto-monnaie. L'hostilité des banques centrales, dont nous avons déjà longuement parlé, n'a pas été extérieure au débat : dans une lettre du 12 novembre 2013, la Réserve fédérale américaine (FED) a ainsi estimé ne pas être la mieux placée pour superviser ou réguler « *ce type d'innovation* », déniant la qualification légale de monnaie au bitcoin. Cependant, le même courrier a reconnu que « *toutes les monnaies virtuelles n'étaient pas illégales* ».

Lors de son audition devant la commission sénatoriale, le 18 novembre 2013, le représentant du ministère de la Justice a même souligné que le bitcoin pouvait avoir « *une valeur juridique d'échange* ». En mars 2014, à l'issue de ces travaux, le ministère de la Justice de l'État de New York a annoncé vouloir étudier la régulation du bitcoin, afin d'en faciliter l'utilisation. En France, le Sénat s'est penché sur la question en janvier 2014, à l'occasion d'une audition relative aux enjeux liés au développement des monnaies virtuelles, considérant notamment les travaux menés par la Banque centrale européenne, à travers son étude de 2012 relative aux monnaies virtuelles et à leur définition.

En vertu de la Constitution d'octobre 1958 et de ses vingt-quatre révisions, « la monnaie de la France est l'euro », ce qui prive officiellement le bitcoin de toute valeur juridique, au moins sur le plan constitutionnel. Toutefois, deux directives européennes ont posé les bases d'une reconnaissance légale des moyens de paiement électroniques, sans toutefois s'intéresser vraiment aux « monnaies électroniques » : une première directive de 2000 a posé la définition juridique de monnaie électronique, tandis qu'une seconde directive de 2009 a élargi cette définition à « *toute valeur monétaire* [...] *stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement* [...] *et qui est acceptée par une personne physique ou morale autre que l'émetteur de la monnaie*

électronique[21]. »

Le bitcoin pose donc un double problème : d'abord, il n'y a pas d'émetteur à proprement parler, ensuite la remise initiale de bitcoins ne correspond pas à un versement de fonds. De fait, pour la Banque de France, le bitcoin n'est pas un moyen de paiement couvert par la directive SEPA (Espace unique de paiement en euros) de novembre 2007 et, en conséquence, elle n'a pas à en réguler l'émission. Cependant, la conversion ou le change de monnaies virtuelles en devises ayant un cours légal entre dans le champ de la réglementation bancaire opérée par la banque centrale française.

Hubert de Vauplane, associé au cabinet américain Kramer Levin, spécialisé dans les nouveaux développements de la finance, a cherché assez tôt à décrire ce que pouvait être ce nouvel objet non identifié. Dans un de ses articles, il résume assez bien l'incapacité des juristes à définir juridiquement la blockchain : « *Les monnaies virtuelles ne sont pas une monnaie légale. C'est la question la plus facile. Pour être définie comme telle, une monnaie doit avoir un cours légal, être définie comme la monnaie d'un territoire par un État dans son ordre juridique, ce qui suppose qu'elle soit "émise" par une entité* [...] *et enfin être libératoire, c'est-à-dire permettre aux personnes résidentes sur un territoire donné d'éteindre leur dette (suite par exemple à l'achat d'un bien ou d'un service) par remise de cette monnaie, sans que le créancier ne puisse contester cet échange et sa valeur.*

« *Les monnaies virtuelles ne sont pas une monnaie électronique. Là encore, la réponse est assez simple. Une monnaie électronique suppose, tout au moins en droit européen, une créance de son détenteur contre l'émetteur qui peut à tout moment demander à ce dernier de lui « rembourser » cette valeur contre une somme d'agent dans une devise ayant cours légal.* [...]

« *Les monnaies virtuelles ne sont pas des instruments financiers en ce qu'elles ne répondent à aucune des énumérations proposées par la directive Marchés d'Instruments Financiers définissant les instruments financiers.*

« *Les monnaies virtuelles ne sont pas un service de paiement, mais l'échange de devises contre une monnaie virtuelle peut être qualifié de service de paiement*[22] ».

Comme il l'écrit avec beaucoup de justesse, les monnaies « décentralisées » ne sont ni des monnaies légales, ni même des monnaies électroniques, ni des instruments financiers, ou un service de paiement. Elles sont toutes ces choses à la fois, sans être définie par chacune séparément. Le bitcoin est défini juridiquement par ce qu'il n'est pas.

Un statut juridique à venir

L'ambition d'un statut juridique du bitcoin est aussi d'imposer cette nouvelle devise internationale et de générer une recette fructueuse pour les États, dans un contexte de crise budgétaire. Entre 2 et 3 milliards de dollars circulent aujourd'hui dans le monde entier sous forme de bitcoins. Avec une prévision d'environ 21 millions de bitcoins en circulation en 2033 et à un cours maximum de 1 000 dollars, observé au cours des dernières années, le marché mondial du bitcoin a donc de beaux jours devant lui.

Pour imposer le bitcoin, les administrations publiques peuvent taxer la plus-value générée par sa conversion en euro ou en devises étrangères. Lorsque le bitcoin est converti en devises étrangères puis rapatrié en France, il est alors soumis à l'impôt sur le revenu et une fraude à la déclaration peut entraîner une amende de 40 % des sommes transférées. De quoi dissuader d'éventuels fraudeurs ! En Allemagne, depuis août 2013, l'administration fiscale considère le bitcoin comme une « monnaie privée », avec une taxation des profits à hauteur de 25 % et une exonération totale au bout d'un an de détention des actifs monétaires. Un régime beaucoup plus attrayant.

La production de bitcoins peut, parallèlement, engendrer des frais pour l'internaute, notamment à travers les dispositifs de minage, des puissances de calcul permettant d'effectuer des transactions numériques soumises à de très fortes charges d'électricité. Pour justifier de ces dépenses aux services des impôts et les déduire de sa retenue fiscale, l'imposé doit disposer d'une trace écrite de sa perte de recettes, mais le système bitcoin n'offre aujourd'hui ni facture, ni ticket de caisse. L'imposition, nouvelle frontière du bitcoin ? Ce sera, en tout cas, une relation motrice dans les transformations à venir de la monnaie virtuelle.

La monnaie, une révolution permanente

Les interactions entre la monnaie et la politique sont, c'est l'essence de cette partie de nos travaux, une sorte d'aller-retour incessant, les deux affluents nourrissant un seul et même fleuve. Faire évoluer notre monnaie, c'est donc poser les ferments d'une révolution politique. Mettre fin à la pensée unique sur la monnaie moderne et donner ses lettres de cachet à la monnaie numérique, aux systèmes décentralisés et transparents, c'est se donner un nouvel objectif de société à atteindre. L'économiste français François Morin met en évidence cette promiscuité avec cette formule forte : « *La monnaie est un commun* ». Cette proximité de la réflexion sur la monnaie et de celle sur notre système politique est à la fois un gage d'espérance pour l'avenir et un point de blocage des discussions publiques sur le bitcoin et la blockchain.

Au début de l'année 2014, j'ai ainsi eu la chance d'aborder ces questions avec le sénateur de l'Oise, Philippe Marini, président de la commission des Finances. Nous échangeons longuement sur le sujet, y compris sur la question du bitcoin et du protocole blockchain. Il y consacrera, quelques mois plus tard, un temps précieux à la rédaction d'un rapport sur le sujet, qui sert, aujourd'hui encore, de référence. La situation m'est alors apparue cocasse : nous étions, lui et moi, en plein éloge d'une technologie issue d'une communauté de hackers, à peine sortie de la pénombre du Net, plaidant pour une organisation décentralisée et transparente, dans ce temple de la République, sous le regard des portraits d'illustres hommes d'État, garants de l'autorité d'un État jacobin et régulateur. Quelle ironie ! Le ton changea pourtant brusquement au détour d'une simple phrase.

Évoquant les perspectives de développement de la blockchain, je me laissais aller à présager que le bitcoin sera peut-être, demain, une monnaie complémentaire à l'euro. Mon interlocuteur se braque, agrippe fermement les poignées de siège, se redresse froidement et me fait signe de la main qu'une barrière invisible vient d'être franchie. « *La monnaie de la République est une monnaie unique et s'appelle l'euro* », me précise-t-il laconiquement. Si la classe politique est prête à charmer la technologie blockchain, la promesse d'émancipation de la monnaie est plus dure à accorder. Le sujet est pourtant au cœur des débats

politiques.

Au fond, il existe trois types de monnaie : la monnaie privée, la monnaie d'État et la monnaie décentralisée, pensée comme un bien commun. La blockchain accompagne le développement de cette dernière forme de monnaie, une « monnaie libre » selon la formule de Pierre Noizat, instrument monétaire du futur et outil de reconquête de nos libertés. Une affirmation encourageante mais qui nécessite de comprendre le fonctionnement concret de la blockchain et d'en étudier les usages. C'est l'objet de ces prochains chapitres. Alors embarquez rapidement.

Tout ce que vous avez toujours voulu savoir sur le fonctionnement d'une blockchain… sans jamais oser le demander

« *Nous avons proposé un système de transactions électroniques ne reposant pas sur la confiance* »

Satoshi Nakamoto, « Bitcoin : système de monnaie électronique en pair-à-pair », 2008

La blockchain, comment ça marche ?

Afin d'expliquer le plus simplement possible le fonctionnement de la blockchain, nous allons présenter les grandes règles sous-tendant le fonctionnement du bitcoin, sa première mise en pratique. Pour distinguer la blockchain mobilisée dans le fonctionnement du bitcoin des autres blockchains, nous parlerons de la blockchain Bitcoin, différenciant ainsi une des multiples formes d'utilisation de cette technologie des nombreuses autres aujourd'hui à l'œuvre. Ce chapitre sera donc l'occasion de faire une brève présentation de ces blockchains alternatives. Ce sera aussi le moment de plonger dans les coulisses de cette technologie parfois mystérieuse, pour mieux en comprendre le fonctionnement et les évolutions.

Sur le plan technique, la blockchain fonctionne comme un vaste registre public, intégrant l'ensemble des transactions validées dans une liste sans fin. Ce registre fait donc figure d'historique de toutes les transactions menées par tous les utilisateurs depuis le début de la constitution du réseau. Depuis le 3 janvier 2009 et l'émission des 50

premiers bitcoins de l'histoire, ce répertoire immense de l'ensemble des échanges de la monnaie numérique fait office de mémoire universelle. Comme le fonctionnement du système est basé sur la confiance, chaque utilisateur dispose d'une copie de la blockchain afin, ainsi que le mathématicien Ricardo Pérez Marco l'explique, de pouvoir « *remonter l'histoire de toutes les transactions passées et de déterminer, en conséquence, si une transaction est valide ou non* ».

Transférer une valeur d'un utilisateur à un autre

Dans le cas du bitcoin, son fonctionnement peut s'expliquer, de manière résumée, selon le texte fondateur : « *Un système de monnaie électronique entièrement en pair-à-pair permettrait d'effectuer des paiements en ligne directement d'un pair à l'autre sans passer par une institution financière. Les signatures numériques offrent une telle solution, mais perdent de leur intérêt dès lors qu'un tiers de confiance est requis pour empêcher le double paiement. Nous proposons une solution au problème de la double dépense en utilisant un réseau pair-à-pair. Le réseau horodate les transactions à l'aide d'une fonction de hachage qui les traduit en une chaîne d'empreinte continue de preuves de travail, formant un enregistrement qui ne peut être modifié sans ré-effectuer la preuve de travail.*

« *La plus longue chaîne d'empreintes sert non seulement de preuve du déroulement des événements constatés, mais également de preuve qu'elle provient du plus grand regroupement de puissance de calcul. Aussi longtemps que la majorité de la puissance de calcul (CPU) est contrôlée par des nœuds qui ne coopèrent pas pour attaquer le réseau, ils généreront la plus longue chaîne et retiendront les attaquants. Le réseau en lui-même ne requiert qu'une structure réduite. Les messages sont diffusés au mieux, et les nœuds peuvent quitter ou rejoindre le réseau à leur gré, en acceptant à leur retour la chaîne de preuve de travail la plus longue comme preuve de ce qui s'est déroulé pendant leur absence*[23].

Fonction de hachage, chaîne d'empreinte continue, preuve de travail ? Si vous n'êtes pas initié aux mécanismes de la cryptographie, cela peut

vous paraître un peu compliqué. Ne vous inquiétez pas, ce chapitre vise précisément à vous donner les outils nécessaires à la compréhension technique du fonctionnement de la blockchain.

Reprenons, en conséquence, le fonctionnement d'un échange de valeur sur la blockchain. Avançons, ensemble, pas à pas, afin de bien comprendre chacune des étapes. Alice dispose d'un certain nombre d'unités de compte sur le réseau bitcoin et souhaite en transférer une partie à Bob, dans le cadre d'un échange. Pour fonctionner, la blockchain a besoin d'une capacité énorme de calcul et mobilise donc un réseau d'ordinateurs distribués. Comme nous l'avons vu dans le chapitre précédent, cette innovation technologique a été développée par des communautés de mathématiciens et d'informaticiens à la fin des années 1990 et au début des années 2000. L'échange entre Alice et Bob est ainsi porté par un nombre élevé de tiers, appelés les membres de la blockchain.

Sur son téléphone ou son ordinateur, Alice dispose d'un porte-monnaie virtuel, grâce auquel elle stocke ses économies en bitcoins, les fameuses unités de compte du réseau, et peut les échanger avec un autre utilisateur. L'accès à ce porte-monnaie est sécurisé par deux codes de sécurité : une clé publique et une clé privée. Ce couple de deux clés de sécurité fonctionne sur le modèle du couple adresse mail et mot de passe, que vous connaissez certainement. Vous avez besoin de ces deux informations pour accéder au porte-monnaie virtuel et à l'ensemble de ses fonctionnalités. Une des deux informations est publique, c'est la clé publique (adresse mail), l'autre est privée et connue du seul utilisateur, c'est la clé privée (mot de passe).

Lorsqu'Alice utilise les deux clés de sécurité dans le réseau, elle peut transférer un certain nombre de crédits à Bob. Le réseau repose en effet sur un logiciel de transaction entre ses utilisateurs, inscrivant chaque opération de transfert dans un registre commun à l'ensemble de la blockchain. L'information du transfert du porte-monnaie d'Alice à celui de Bob est envoyée vers un nœud de réseau, une sorte de carrefour informatique entre les ordinateurs individuels. À cette étape, les ordinateurs connectés au réseau, ceux d'Alice, de Bob et de l'ensemble des membres de la blockchain, vérifient si la transaction est valide. Cela suppose, d'abord, de vérifier qu'Alice dispose bien des crédits qu'elle entend transférer à Bob.

À chaque nœud de réseau, les transactions sont réunies par groupe au sein d'un bloc de transactions (*block*). Les membres de la blockchain en charge de la vérification de l'opération de transfert décident de manière consensuelle de la validité ou de l'invalidité de la transaction. Si l'opération est jugée valide, le bloc est donc créé, inscrit dans le registre commun, et ajouté à une longue série de blocs, continuellement agrandie depuis la création de la blockchain. Cette chaîne de blocs donne son nom à la blockchain. Dans la chaîne, chaque bloc contient la signature, c'est-à-dire la « marque » numérique, du bloc précédent, ce qui lie les blocs les uns aux autres sous la forme d'une chaîne continue.

Comment fonctionne le processus de consensus décentralisé ?

L'opération de validation des opérations de transaction est appelée processus de consensus décentralisé. Elle impose, en effet, le consensus des membres de la blockchain, puisque le réseau ne dispose pas d'autorité centrale dotée du « dernier mot ». Elle repose aussi sur la disposition du registre commun des transactions par l'ensemble des membres de la blockchain, afin de s'assurer que personne ne puisse modifier individuellement la chaîne sans devoir falsifier l'ensemble des registres enregistrés dans les ordinateurs individuels des membres du réseau. Plusieurs outils cryptographiques concourent à ce processus de consensus décentralisé.

L'outil de base de la cryptographie informatique est la méthode de cryptographie asymétrique, basée sur un chiffrage à deux clés. Admettons qu'Alice souhaite envoyer un message privé à Bob et ne désire pas que, intercepté, ce message soit déchiffrable. Ces conditions supposent qu'Alice et Bob disposent, seuls, d'une clé de codage et de décodage du message. Alice génère donc une paire de clés : une clé publique (C Pu) et une clé privée (C Pr). Ces deux clés ne peuvent fonctionner qu'en couple : vous ne pouvez pas vous connecte à l'adresse mail d'un de vos amis avec votre mot de passe.

Dans son message, Alice utilise donc sa clé publique pour crypter son message. Grâce à sa clé C Pu, son message « Bonjour Bob » devient « eGSxerS23 ». Si le message est intercepté, il sera tout simplement

incompréhensible. Lorsque Bob reçoit le message, il utilise sa clé C Pr, couplée à la clé C Pu d'Alice, pour décrypter le message et « eGSxerS23 » redevient « Bonjour Bob ». Cette technologie de la cryptographie asymétrique est la base de nombreuses applications de sécurité informatique.

Alice peut vouloir signer ses messages. Pour cela, l'informatique mobilise un autre outil cryptographique, la fonction de hachage. Il s'agit d'un procédé à sens unique, permettant d'obtenir à partir d'une valeur d'entrée, une valeur de sortie, parfois appelée « empreinte », rédigée de manière aléatoire. Le changement d'une seule lettre d'une valeur d'entrée à l'autre peut donc donner une valeur de sortie totalement différente. Ainsi, la fonction de hachage de la phrase « Blockchain est une révolution » donne « h(Blockchain est une révolution)=E7oiu2J9N43JCxR », alors que la fonction de hachage de « Blockchain est une revolution », avec le simple retrait de l'accent aigu, donne « h(Blockchain est une revolution)=vvl7Jn43xvi4RF ».

La fonction de hachage est un outil pratique pour vérifier l'intégrité d'un document, en d'autres termes sa signature. Si Alice envoie à Bob le fichier haché, Bob peut comparer les deux documents grâce à la fonction de hachage et vérifier que le bon message est bien arrivé. L'algorithme de hachage le plus communément utilisé, appelé SHA, permet de stocker des informations sensibles, comme les mots de passe. Grâce à SHA, les empreintes des mots de passe sont conservées sur un serveur privé, si bien que le déblocage de l'accès à votre compte se fait en comparant le mot de passe entré manuellement et l'empreinte stockée sur le serveur. Le hackage du serveur devient ainsi inutile, car il ne conserve pas les mots de passe mais seulement leur empreinte. La fonction de hachage est une fonction intéressante en sécurité, car elle est extrêmement difficile à inverser. La lecture de l'empreinte rend quasi impossible la détection du message d'origine à qui ne détient pas la clé de hachage.

La signature d'un document utilise à la fois la cryptographie asymétrique et les fonctions de hachage. Imaginons maintenant qu'Alice souhaite envoyer un document (D), signé de sa main, à Bob. Elle doit d'abord générer l'empreinte du document au moyen d'une fonction de hachage (E(D)). Elle crypte ensuite cette empreinte avec sa clé publique C Pu (E(D)). Elle peut ensuite envoyer son message. Pour

vérifier la validité du document reçu, Bob déchiffre d'abord la signature avec sa clé privée (C Pr [C Pu (E(D))]), ce qui lui permet de confirmer que le message a bien été envoyé par Alice, en la comparant à l'empreinte du document. Si ces deux empreintes sont identiques, la signature est valide et le document reçu est bien celui qu'Alice avait envoyé dans son message. Sur la blockchain, toutes les transactions sont signées afin de prouver qu'elles ont bien été émises par les propriétaires des portefeuilles, ce qui mobilise la cryptographie asymétrique et les fonctions de hachage.

La vérification des opérations de transaction par les membres de la blockchain mobilise, enfin, un troisième et dernier outil, la preuve de travail (*proof of work*). Il s'agit d'une énigme mathématique complexe à résoudre, dont la vérification est, elle, relativement simple. Prenons l'exemple d'un sudoku de plusieurs milliers de lignes et de colonnes : il s'agit d'un jeu complexe et très long à résoudre mais, une fois complété, sa vérification peut être effectuée assez rapidement. La preuve de travail fonctionne sur le même modèle. Elle paraît s'apparenter à l'énigme *captcha*, cette vérification qui vous est souvent demandée en fin de questionnaire (afin de vérifier que vous n'êtes pas un programme informatique). Alors que le captcha fonctionne sur la base d'un « test de Turing », vérifiant votre humanité, la preuve de travail vérifie à l'inverse que son interlocuteur est bien un ordinateur, capable de résoudre une énigme mathématique infiniment complexe. En d'autres mots, le captcha est un anti-test de Turing.

Les ordinateurs des membres de la blockchain sont amenés à résoudre une énigme mathématique comme celle-ci :

- Si l'on crée un document dans lequel on ajoute l'empreinte du bloc précédent, l'empreinte du bloc en cours et une valeur libre,
- Pour quelle valeur libre obtient-on une empreinte du document qui contient des 00000 au début (par exemple « 000000000ffxjU67Tfr45Nj3G1 ») ?

Il n'y a, nous l'avons dit plus haut, aucune relation entre la valeur d'entrée du hachage et l'empreinte : l'ordinateur doit tenter des milliards de combinaisons pour obtenir la réponse à la question.

En une dizaine de minutes, les ordinateurs de la blockchain ont donc essayé des centaines de milliards de combinaisons et l'un d'eux est parvenu à une solution. Les ordinateurs sont appelés des « mineurs »

et le procédé de calcul, une « opération de minage ». La réponse obtenue est automatiquement transmise à l'ensemble des ordinateurs connectés. La vérification de la solution est très rapide et, si elle est validée, un nouveau bloc est créé et arrimé à la blockchain. L'opération de validation est en effet beaucoup moins coûteuse en termes de puissance de calcul que l'opération de vérification : il est ainsi plus facile de valider que 53 fois 113 font bien 5 989, plutôt que de chercher à retrouver les différents facteurs générant 5 989.

Statistiquement, seul un ordinateur peut réellement faire ce calcul dans le temps qui est imparti. Ainsi pour pouvoir insérer un nouveau bloc dans la chaîne, il faut avoir, dans l'ordre, vérifié que les transactions étaient valides, résolu une énigme mathématique complexe du niveau d'un ordinateur, et obtenu le droit, par un consensus des autres participants, d'insérer ce nouveau bloc dans la chaîne de blocs, en le liant aux anciens blocs par les signatures précédentes. À ce moment précis, cette nouvelle chaîne de blocs constitue le nouvel état du registre automatiquement enregistré sur tous les ordinateurs du réseau.

La viabilité de ce procédé ne repose heureusement pas sur l'éthique de ces « mineurs », car certains agents sont supposés corruptibles. Des mineurs malveillants peuvent, en effet, valider des transactions fictives ou illégales et ainsi corrompre l'ensemble de la blockchain, mais la contrainte de la preuve de calcul les en empêche la plupart du temps. En effet, il faudrait une ressource numérique supérieure à la puissance totale du réseau pour créer une sous-chaîne de blocs qui serait valide pendant un certain temps.

L'émergence de la monnaie numérique n'a pas été seulement une rupture culturelle et politique, elle a aussi consisté en un défi mathématique et technique. Le mathématicien français Jean-Paul Delahaye est un grand vulgarisateur des sciences dures. Je suis un grand lecteur de ses livres et j'étais très heureux de le voir s'intéresser à la blockchain et de pouvoir en parler avec lui. Il insiste sur l'interaction très forte entre enjeux cryptographiques de la monnaie numérique et résolution des équations mathématiques, comme l'algorithme « ECDSA » qui sert de signature numérique à clé publique dans le système bitcoin.

Les preuves de la blockchain

Le processus de création d'un nouveau bloc de la blockchain peut s'effectuer avec deux preuves : la preuve de travail ou la preuve d'enjeu. Comme nous l'avons vu, la preuve de travail est une fonction cryptographique consistant à faire résoudre par un ordinateur une énigme compliquée mais facilement vérifiable. La transaction numérique est ensuite complétée grâce à la réponse à cette énigme mathématique. Cette étape permet de s'assurer que le mineur est bien un ordinateur, et pas un utilisateur malveillant, en raison de la rapidité nécessaire à la résolution des calculs. Pour prendre une image, ce mécanisme ressemble à la pose de scellés cryptographique sur le grand livre des transactions.

Par ailleurs, la preuve d'enjeu (*proof of stake*) est une fonction de consensus très différente, elle va donner un poids différent au vote de consensus en fonction de la détention des unités de la blockchain. Plus un utilisateur dispose d'unités de compte de la blockchain, plus sa participation à la validation d'une transaction est importante. Utilisée pour la première fois par la blockchain Peercoin, créée en 2012, cette deuxième preuve de création d'un bloc est sujette à de nombreuses critiques. Alors que plusieurs analystes dénoncent l'empreinte carbone de la preuve de travail, c'est-à-dire son impact négatif sur l'environnement lié à la puissance informatique nécessaire à la réalisation de cette opération de calcul, la preuve d'enjeu est un outil de vérification beaucoup plus écologique. Elle reste néanmoins un véritable enjeu de sécurité pour la blockchain et donc pour la stabilité de celle-ci, basée sur la confiance des utilisateurs.

En fait, ces fonctions de consensus basées sur les preuves de travail ou d'enjeu répondent à la problématique des généraux byzantins. Dans cette parabole, plusieurs généraux byzantins font le siège d'une ville et doivent attaquer conjointement pour espérer vaincre leur ennemi commun. Un général qui attaquerait seul serait voué à une mort certaine. Cependant, certains d'entre eux sont des traîtres et risquent de compromettre l'attaque conjointe. Si les généraux échangent entre eux, les traîtres pourraient falsifier les messages et faire échouer la stratégie de groupe. La blockchain permet de résoudre cette équation issue de la théorie des jeux. Les preuves d'enjeu et de travail

permettent de s'assurer que tous les généraux se sont accordés sur un moment précis d'attaque avant de lancer leur initiative. Après mise en place de la première blockchain, Satoshi Nakamoto a compris que ce problème d'informatique et de théorie des jeux était résolu. Il a repris cette illustration en recréant une nouvelle parabole avec l'image de hackers attaquant « par déni de service » (*Distributed denial of service*, DDoS) un routeur wifi. Geek un jour, geek toujours.

La preuve d'enjeu constitue, selon Pierre Noizat de Paymium, un mécanisme de consensus intéressant mais pas assez fort pour pouvoir offrir une pérennité assez longue. Pour certains analystes dont il fait partie, seul le consensus obtenu par la preuve de travail permet de créer une chaîne aux maillons suffisamment forts, parce que les reconstituer demande une puissance informatique démesurée par rapport au problème à résoudre.

Une blockchain distribuée entre les « mineurs »

Le registre des transactions de la blockchain, outil authentique, inaltérable et transparent, est un outil distribué, enregistré sous forme de dizaines de milliers de copies dans les ordinateurs autonomes des membres de la blockchain. Cette répartition égale de la mémoire de la blockchain n'empêche pourtant pas une certaine compétition entre les mineurs. Sur le fondement de la règle « *the winner takes all* » (le gagnant emporte tout), seul le premier membre de la blockchain à accomplir l'opération mathématique de preuve de travail empoche une récompense. Dans le cas de bitcoin, ce membre est récompensé par quelques nouveaux bitcoins générés pour chaque bloc supplémentaire intégré à la blockchain.

Le « mineur » est donc un acteur à part entière de la vérification des transactions et de la création monétaire sur la blockchain. Il fait ainsi figure de chercheur d'or, filtrant l'eau de sa rivière avec son matériel d'orpaillage ou piochant au fond d'une mine pour chercher une pépite. Toutefois, au lieu d'un tamis ou d'une pioche, ce mineur du XXI^{e} siècle est doté d'un ordinateur, puissance de travail appliquée à la résolution d'énigmes mathématiques. Plus la communauté blockchain grandit,

plus la puissance informatique mise à disposition des opérations de preuve de travail grandit, plus la durée pour résoudre les énigmes mathématiques et de créer des bitcoins diminue.

La blockchain repose ainsi essentiellement sur l'activité de minage. Toutes les dix minutes environ, une activité de minage est achevée et un nouveau bloc de transactions validées est ajouté à la blockchain. Cela veut dire que, toutes les dix minutes, une somme d'énigmes mathématiques est résolue et de nouveaux bitcoins sont créés au sein du réseau, en récompense de l'activité de minage. Cette temporalité de l'activité est fortement régulée et, lorsque le réseau résout une équation en moins de dix minutes grâce à une puissance informatique augmentée par l'extension de la blockchain, le système bitcoin accroît la difficulté de l'opération de minage. Ainsi, tous les quinze jours, le protocole de la blockchain définit un nouveau niveau de difficulté de la preuve de travail, augmentant le nombre de zéros à trouver dans la résolution de l'énigme mathématique. Pour stimuler l'intérêt à la réalisation des opérations de travail, le salaire d'un mineur évolue dans le temps, afin de demeurer incitatif sur le long terme.

L'émission globale de bitcoins sur la blockchain Bitcoin est aujourd'hui limitée à 21 millions de bitcoins et, selon une règle intangible, tous les 210 000 blocs créés, la quantité d'argent contenue dans chaque bloc est divisée par deux (*bitcoin halving*). Comme le temps de minage est encadré et fixé à dix minutes par bloc, l'émission de 210 000 nouveaux blocs équivaut systématiquement à quatre années de fonctionnement du réseau. La création de 210 000 blocs correspond à près de quatre ans de minage. Les quatre premières années, la prime de minage était ainsi de 50 bitcoins, puis de 25 bitcoins, de 12,5 bitcoins depuis juillet 2016 et, aux alentours du 4 juillet 2020, de 6,25 bitcoins.

Dans un billet publié par *CNRS Le Journal*, en mai 2016, le chercheur Ricardo Pérez Marco conclut sur l'infaillibilité de ce système de validation des transactions numériques : « *Cette robustesse du protocole s'incarne dans la blockchain, un fichier qui rassemble donc l'ensemble des blocs validés. Celle-ci est incorruptible car, pour la falsifier, il faudrait déployer la totalité de la puissance de calcul qui a été utilisée pour valider chacun de ses blocs. Une tâche virtuellement impossible au vu de la puissance actuelle du réseau Bitcoin, qui dépasse aujourd'hui les 15 millions de PetaFLOPS ; sachant que*

l'ordinateur actuel le plus puissant tourne à quelques dizaines de PetaFLOPS. »

Dans la mine, dans la mine !

L'écosystème de la blockchain publique bitcoin repose finalement sur deux piliers : une machinerie cryptographique et une économie créatrice de valeurs. En Chine, à Dalian, Changcheng, dans une partie reculée et rurale du pays, six mines de bitcoins, installées dans un hangar souterrain, tournent ainsi à plein régime, avec une génération moyenne de 4 050 bitcoins par mois sous forme de prime de minage, soit près de 1,5 million d'euros au cours de la seule année 2014. Plus de 3 000 mineurs informatiques travaillent quotidiennement à résoudre des algorithmes numériques, avec un coût électrique très élevé pour l'entreprise, environ 80 000 dollars de factures par mois.

À cause de défaillances techniques, de la vétusté des matériels ou du faible rendement comparé au coût électrique, 900 mineurs sont déjà sur le carreau. Signe d'une nouvelle ère, ces immenses hangars consommateurs d'énergie s'approvisionnent à base d'énergies renouvelables (solaire, éolien ou encore hydraulique). La région voisine du Tibet est en effet propice au déploiement de ces énergies vertes, souvent disponibles pour un coût moindre et un rendement conséquemment plus élevé pour les mineurs.

L'entrepreneur chinois Eric Mu décrit ainsi la mine de HaoBTC, en de nombreux points similaire : « *Deux bâtiments ont maintenant été construits pour abriter les mineurs et deux autres sont actuellement en cours. La ferme exploite plus de 10 000 unités de "Antminer S3", qui, aux côtés des énormes ventilateurs, génèrent un bruit qui est plus qu'un peu ennuyeux. Pas ce que j'appellerais un bruit assourdissant, mais vous devez parler très fort quand vous vous adressez à quelqu'un, même à proximité de vous – c'est un environnement idéal pour vous apprendre à être économe en mots ! En ce qui concerne la température, c'est souvent autour de 30 °C, mais le vent souffle beaucoup, ce qui aide à supporter la chaleur*[24]. »

En moyenne, en 2016, chaque bloc de la blockchain récompense le mineur de 25 bitcoins, soit 11 200 dollars par bloc. Très tôt dans

l'histoire de la blockchain Bitcoin les mineurs se sont regroupés dans des groupes (des pools) qui leur permettent de partager les gains et donc de lisser leurs revenus en apportant leur puissance informatique à ces groupes qui s'organisent librement.

Alors que le marché du minage est aujourd'hui tenu par quatre pools chinois à plus de 70 % (AntPool, BTCCPool, BwPool, F2Pool), de nombreux observateurs craignaient que la division par deux de la prime de minage intervenue en juillet 2016 n'accroisse cette marche vers un oligopole asiatique de l'activité de minage. L'analyse de l'évolution du cours du bitcoin au regard du *bitcoin halving* de juillet 2016 reste néanmoins très complexe, compte tenu des effets du référendum britannique sur la sortie de l'Union européenne (fin juin 2016) sur le cours de la monnaie numérique. Bref, si le bitcoin ressemble beaucoup à un métal précieux, comme l'argent ou l'or, la volatilité de son cours repose aussi sur une équation complexe.

La blockchain est-elle publique ?

Lorsque Wei Dai et Satoshi Nakamoto ont théorisé la crypto-monnaie dans les années 1990 puis dans les années 2000, ils se sont tournés vers un accès public de la base de données des transactions de cette monnaie numérique afin d'en assurer un contrôle optimal par le grand public. Tout utilisateur doté du logiciel adéquat peut donc prendre connaissance de l'historique des transactions, mais aussi contribuer en mettant la puissance de calcul de sa machine au service des opérations de minage des transactions en bitcoin.

La technologie blockchain du bitcoin est une blockchain dite publique, dans la mesure où tout un chacun peut consulter les données mobilisées dans l'utilisation du réseau. L'évolution de l'activité de minage vers un oligopole aux mains de quelques entreprises chinoises tend néanmoins à nuancer cette affirmation. Parallèlement, dans une certaine configuration moins portée par l'esprit d'ouverture, la blockchain peut être dite privée. Le nombre de mineurs y est alors limité et la validation des blocs est une activité plus régulée, soumise à quelques acteurs omnipotents.

L'émergence de cette blockchain privée ne signe pas la fin de la

blockchain publique, mais elle répond à des besoins en termes de rapidité du processus de validation des transactions et de coûts des infrastructures. Elle tend aussi à pousser le bitcoin à progressivement dériver vers la possibilité de devenir une monnaie privée aux mains d'une banque centrale privée. Comme l'esprit de naissance du bitcoin s'inscrit dans une révolution libertaire et démocratique, il apparaît toutefois plus probable que cette privatisation de la blockchain accompagne l'émergence de nouvelles crypto-monnaies privées, concurrentes du bitcoin, disposant des mêmes atouts mais peut-être d'une plus grande tolérance des milieux bancaires, si cette nouvelle configuration leur permet un contrôle plus efficient.

Est-ce que cette privatisation est pour autant l'avenir de la blockchain ? Le choix du Minitel (créé en 1980) de s'orienter vers un accès privé, alors qu'Internet (existant dès 1983, sous la forme d'Arpanet) avait choisi un accès public, montre bien que la question n'est pas si simple et que le choix de la privatisation n'est pas forcément l'assurance d'un succès. La crise démocratique vécue par nos sociétés nourrit en effet un besoin fort de transparence et les récentes crises de la surveillance (WikiLeaks, affaire Snowden) ont accru le désir des populations de pouvoir exercer un contrôle direct sur nos sociétés, sur le modèle du « citoyen-contrôleur » imaginé par le philosophe français Alain, dans les années 1920.

Le groupe français Orange semble pourtant croire à cette blockchain privée. En septembre 2015, il a ainsi annoncé sa participation au financement de Chain, une blockchain privée destinée à tout type de transactions (titres financiers, cartes cadeaux, points de fidélité, crédit mobile). Aux côtés d'un consortium d'autres grands investisseurs internationaux, parmi lesquels Capital One ou encore Citi, Orange participe à une dotation de 30 millions de dollars pour développer cette plateforme sécurisée de transferts et appuyer sa stratégie d'accompagnement du développement numérique et technologique du continent africain. « *Devenir un partenaire clé et un investisseur de Chain*, explique Pierre Louette, le directeur général adjoint d'Orange, *nous permettra d'apprendre plus vite et de lancer des essais autour de cette technologie*[25]. »

Alors que des banques comme JP Morgan ou UBS travaillent déjà à l'établissement de ces blockchains privées, avec des systèmes

centralisés dans la validation et la vérification des transactions, une troisième alternative de blockchain fait aussi aujourd'hui son apparition : la blockchain consortium aussi appelée blockchain sous contrôle. Cette ultime configuration allie l'ambition de démocratie et de transparence de la blockchain publique et les acquis de rapidité et d'efficacité de la blockchain privée. Le processus de validation des transactions est, en effet, confié à un consortium d'une quinzaine ou d'une vingtaine de mines détenues par des institutions majeures du réseau blockchain. Le droit de lecture de la blockchain y est, au choix, public ou réservé à certains participants.

Les contrats intelligents, une exécution sans condition

Les transactions numériques sont donc validées lorsque les protocoles informatiques vérifient et exécutent une négociation selon des critères prédéfinis, comme l'identité des deux contractants ou la balance de leur compte numérique. Ces critères sont inscrits dans des contrats intelligents (*smart contracts*), une sorte de registre informatique des opérations de vérification et exécution d'une transaction, rédigé sous la forme de protocoles cryptographiques et de mécanismes de sécurité numérique. Décrite en 1994 par Nick Szabo, la notion de « contrat intelligent » a évolué avec l'émergence de la crypto-monnaie bitcoin à la fin des années 2000. « *Un contrat intelligent*, écrit-il, *est un protocole de transaction informatisé qui exécute les termes d'un contrat. Les objectifs généraux sont la satisfaction des conditions contractuelles mutuelles (telles que le paiement des termes, les privilèges, la confidentialité et même l'exécution forcée), la minimisation des exceptions à la fois malicieuses et accidentelles, et la minimisation des besoins d'intervention d'un tiers médiateur. Les buts économiques afférents incluent une diminution des pertes liées à la fraude, les coûts d'application arbitraire ou forcée et les autres coûts de transaction*[26]. »

Les contrats intelligents sont répliqués à travers toute la blockchain Bitcoin et tous les ordinateurs connectés au réseau, ce qui les rend visibles à tous, à tout moment. Cette transparence absolue n'assure pas, pour autant, leur infaillibilité, à l'image de l'attaque pirate menée à

l'encontre du réseau The Decentralized Autonomous Organization (DAO) de la blockchain Ethereum, en juin 2016, pour un coût final de 50 millions de dollars, sur laquelle nous reviendrons plus loin. Depuis 2002, ces contrats intelligents sont rédigés grâce à *Sheme*, un langage programmatique développé par Guy L. Steel et Gerald Jay Sussman, dans les années 1970, disponible depuis 2013 dans une version R7RS.

Les contrats intelligents apportent aussi une garantie d'exécution des termes stipulés, quelle que soit la situation. Dans l'exemple développé par Nick Szabo, au début des années 1990, le contrat intelligent vise ainsi à redonner automatiquement le contrôle d'une voiture à son bailleur au cas où le locataire ne règlerait pas son paiement à temps. À Londres, en 2015, un hackathon a ainsi permis d'appliquer les règles du *smart contract* aux assurances pour retard de vols civils – avant cette initiative, plus de 60 % des passagers assurés ne revendiquaient pas leur argent, au bénéfice de leur assurance, ce que l'applicabilité automatique du contrat intelligent cherche à résoudre. Pour autant, ces contrats n'ont pas véritablement de valeur juridique.

Pour Primavera De Filippi, chercheuse au Centre d'études et de recherches de sciences administratives et politiques (CERSA) du Centre national de la recherche scientifique (CNRS) : « *Un* smart contract *est un logiciel. Au vu de leur appellation, on a tendance à les assimiler à des contrats, mais ils n'ont pas en eux-mêmes d'autorité juridique. Lorsqu'un contrat juridique existe, le* smart contract *n'est qu'une application technique de ce contrat*[27]. »

Le contrat intelligent, quelle base légale ?

La question de la valeur juridique du contrat intelligent est pourtant un thème en pleine transformation, au fur et à mesure de la reconnaissance progressive de la blockchain Bitcoin. Un contrat se définit aujourd'hui par des conditions de fond (contrat écrit, avec des clauses obligatoires) et de forme (conclu devant une autorité légale, la plupart du temps un notaire). Ce document doit être clair et compréhensible, être accepté par les deux parties en toute connaissance de cause et de ses conséquences juridiques, et peut être conclu de manière électronique, ainsi que la loi française l'a reconnu

depuis plusieurs années maintenant.

L'encadrement de ces contrats électroniques répond, cependant, à un formalisme tout particulier, avec l'exigence de trois conditions : intelligibilité du contrat, c'est-à-dire que le logiciel d'écriture du contrat ne doit pas être obsolète ou disparu du marché afin qu'un support de lecture existe encore ; intégrité du contrat, c'est-à-dire qu'il ne peut pas être altéré par une des deux parties ou par un tiers ; et imputabilité du contrat, c'est-à-dire identification fiable et certifiée de l'auteur de l'acte. La blockchain Bitcoin peut répondre aux conditions d'intelligibilité et d'intégrité du contrat grâce aux mécanismes du contrat intelligent.

L'imputabilité du contrat est plus délicate, car elle suppose la création d'un cadre juridique à la signature électronique d'un contrat intelligent. En droit, la signature électronique est reconnue comme valable dès lors qu'elle remplit quatre conditions : elle doit être exclusivement liée au signataire, doit permettre de l'identifier, doit avoir été créée par des moyens que le signataire garde sous son contrôle exclusif, et il doit exister un lien évident entre la signature et l'acte auquel elle s'attache. La blockchain Bitcoin ne permet pas, aujourd'hui, de vérifier la fiabilité d'une signature électronique à l'aide d'un certificat délivré par un prestataire qualifié et agréé, ce qui ne lui fournit pas de base juridique et nuit donc à la qualification juridique des contrats intelligents.

En avril 2016, la Cour de cassation a néanmoins révolutionné le droit des signatures électroniques en constatant que le juge avait suffisamment vérifié les conditions intrinsèques de fiabilité d'une signature pour que celle-ci ait une valeur légale, alors même que le site de contractualisation en ligne n'avait pas eu recours à l'utilisation d'un certificat électronique qualifié ainsi que l'y obligeait la jurisprudence passée. Dans un article consacré à ces nouvelles problématiques, Jérôme Giusti, avocat et fondateur du cabinet 11.100.34, voit dans cette décision juridique l'occasion de faire évoluer le droit français dans ce domaine : « *J'appelle de mes vœux une réforme de notre droit de la preuve littérale des contrats vers moins de formalisme pour reconnaître que des dispositifs comme la blockchain suffisent, par les garanties intrinsèques qu'elle offre, à faire signature. D'ailleurs, subrepticement et à demi-mot, le gouvernement semble avoir commencé à faire référence à la blockchain, dans une récente ordonnance relative aux bons de caisse, en date du 28 avril 2016. Ces derniers peuvent être inscrits*

dans un registre tenu par l'émetteur mais "l'émission et la cession de minibons peuvent également être inscrites dans un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations dans des conditions, notamment de sécurité, définies par décret en Conseil d'État[28]". »

La blockchain Ethereum, une blockchain et des contrats

En décembre 2013, le programmateur russo-canadien Vitalik Buterin a posé, nous en avons parlé dans notre brève histoire de la blockchain, les premières bases d'Ethereum, une nouvelle blockchain permettant la création de contrats intelligents par les utilisateurs. Les contrats intelligents, rédigés en langage programmatique « Turing-complet », y sont consultables publiquement sur la blockchain. Cette catégorie de langage de programmation se définit par une série d'instructions plus ou moins modulables, capable de reformuler n'importe quel autre programme informatique, quel que soit son langage d'écriture. En adoptant un langage programmatique de ce type, la blockchain Ethereum entend donc être capable d'exécuter n'importe quel programme pour concurrencer la blockchain Bitcoin : l'alliance du Turing-complet, du système IFPS et de la blockchain a ainsi posé les bases d'un ordinateur universel. Ce nouvel ordinateur vit dans la communauté des ordinateurs des participants. Il devient très difficile à pirater, tant ses opérations sont difficiles à falsifier.

Au lancement de la blockchain Ethereum, 31 591 bitcoins (18 millions de dollars) ont été réunis en échange d'une nouvelle monnaie numérique, l'*ether*. En juillet 2015, la blockchain Ethereum a finalement été lancée avant d'être déclinée, en mars 2016, sous une nouvelle version du logiciel, Homestead. La première version de la blockchain Ethereum, intitulée Frontier, permettait ainsi d'échanger et de miner des ethers, mais aussi d'envoyer et d'exécuter des contrats intelligents.

La deuxième version, Homestead, est une phase de consolidation de la blockchain Ethereum, plus stable et plus sécurisée, afin de s'engager progressivement vers une ouverture au grand public de ce réseau. Deux autres versions du logiciel devraient être prochainement lancées,

sans qu'aucune date n'ait été encore communiquée : Metropolis, lancement grand public avec un navigateur spécial et une série d'applications liées, et Serenity, avec un passage d'un mode de fonctionnement par minage à un mode de fonctionnement par investissement. Dans cette ultime phase de développement de la blockchain Ethereum, les utilisateurs du réseau seront rémunérés proportionnellement à leur investissement initial.

Le système de minage de la blockchain Ethereum répond, aujourd'hui, à des caractéristiques classiques : 72 millions d'ethers créés au lancement de la blockchain, création par minage depuis 2015, au rythme de 5 ethers par bloc miné, en moyenne toutes les cinq secondes, soit près de 10 millions d'ethers par an. L'exécution des contrats intelligents inscrits dans la blockchain Ethereum nécessite cependant un coût de vérification payé aux mineurs sous la forme de frais de traitement, mesurés en ethers et définis selon les fluctuations du marché, environ 0,00047 ether par contrat intelligent, en juin 2016.

Dans le détail, l'exécution d'un contrat intelligent requiert du « gaz », une mesure infinitésimale de l'ether (1 gaz = 0,0000000225 ether) et une transaction basique, c'est-à-dire un virement entre deux utilisateurs de la blockchain Ethereum, demande 21 000 gaz, soit les 0,00047 ether requis par contrat intelligent. Le prix en gaz de l'exécution d'un contrat intelligent dépend de la complexité de l'opération à exécuter et le prix du gaz s'ajuste, lui-même, par rapport au cours de l'ether pour éviter une escalade des prix des contrats intelligents, en fonction de l'appréciation de l'ether. L'utilisateur peut choisir de payer moins de gaz que le coût moyen, au risque de subir un temps d'exécution plus long que la moyenne, puisque les transactions les plus rémunératrices sont exécutées en priorité par les mineurs.

DAO, une organisation sans humain

En décembre 2015, Stephen Tual, Simon et Christoph Jentzsch présentent Slock.it devant un parterre parisien, une infrastructure de la future économie de partage hébergée par la blockchain Ethereum. Cette interface permet en effet de louer, vendre ou partager des objets physiques à travers des contrats intelligents signés sur la blockchain. Le

mot d'ordre est simple : allier échanges du quotidien (vélo, imprimante, machine à laver) et révolution numérique (immuabilité, sécurité, fiabilité). Lors de leur présentation au public de leur plateforme, les trois programmateurs prennent ainsi l'exemple d'un appartement, dont la serrure de la porte d'entrée serait connectée à la blockchain Ethereum et se verrouillerait automatiquement à l'issue du contrat intelligent.

Les objets du quotidien sont alors connectés à la blockchain par des systèmes de transfert d'informations déjà existants, comme Bluetooth, Wi-Fi ou encore ZigBee et Z-Wave. L'utilisateur les inscrit sur la blockchain à travers un site intermédiaire, Ethereum Computer, appelé à prochainement changer de nom, qui lui attribue un numéro d'identifiant unique ensuite utilisable dans la rédaction du contrat intelligent. Sur la partie technique, Slock.it s'est très tôt associé avec de grands groupes industriels, comme Samsung, SafeShare ou encore RWE, afin de développer les solutions pratiques sous-tendues par l'usage des contrats intelligents.

Pour financer les activités de Slock.it et superviser la gestion des contrats intelligents, une société entièrement dématérialisée a été mise en place, The Decentralized Autonomous Organization (DAO). Cette organisation décentralisée n'a pas de bureaux, pas de conseil d'administration, pas de directeur, pas même de structure juridique. Elle repose simplement sur un code organisé sous forme de contrats intelligents, qui régissent son organisation et son fonctionnement. Certains contrats permettent de lever de l'argent, d'autres de choisir des projets d'investissements, d'autres encore d'investir ou de transférer des ethers vers ces projets en question. Une sorte de capital risqueur d'un nouveau genre.

Lancée en juin 2016, elle a formé un capital de 150 millions de dollars grâce aux investissements levés et s'est co-construite grâce à la participation de 4 000 membres de sa communauté, ce « conseil d'administration doté d'un pouvoir de décision et d'un pouvoir financier » supervise l'allocation des fonds enregistrés sur la blockchain Ethereum entre les différents partenaires recrutés. Le contrôle des utilisateurs sur le pilotage de The DAO est proportionnel à leur investissement de départ dans la société. Leurs parts dans la société sont mesurées en jetons (*tokens*). Sur le modèle de l'actionnariat, la DAO peut ainsi se rémunérer sur les activités de contrat intelligent, en

prélevant une commission, et transmettre un pourcentage de ce bénéfice à ses membres.

Les limites de la DAO

The DAO n'est, en fait, qu'une forme de DAO. Une DAO est une organisation autonome et décentralisée. C'est une organisation qui va allouer des monnaies numériques ou des jetons numériques dans le cadre des contrats intelligents. Chaque blockchain peut générer ainsi des DAO propres, mais leur fonctionnement est aujourd'hui quelque peu chaotique. Beaucoup de ces structures, nées en 2016, manquent de cohésion sociale, ce qui est pourtant vital au bon fonctionnement d'une structure de prise de décision dans le cadre d'échanges, de débats et finalement de votes.

Prenons pour exemple un projet communautaire qui vise à transformer un espace public, comme un parc. La première étape consiste à lever des fonds avec un procédé basé sur une crypto-monnaie. Les fonds sont apportés à une entité qui attend de recevoir à l'adresse d'un porte-monnaie numérique le total des souscriptions au projet en crypto-monnaie, par exemple. Si elle atteint le seuil du montant nécessaire au projet, elle peut démarrer son activité, sinon elle renvoie automatiquement les participations à chacun des donateurs. Une fois les fonds reçus, elle peut continuer d'appliquer d'autres contrats décentralisés. Elle peut embaucher des contributeurs qui vont mener des tâches précises rémunérées par les fonds recueillis. Les collaborateurs au projet recevront un salaire, non pas d'une personne morale, mais d'une organisation décentralisée et transparente dont les règles sont inscrites dans son code qui est partagé et ouvert. La participation à la souscription donne des droits aussi à la gouvernance du tout, des projets concrets peuvent être votés et donc décidés par les souscripteurs.

L'entreprise est devenue un simple programme dans la blockchain. Il organise la gouvernance entre actionnaires et salariés, clients et fournisseurs, selon des règles définies et votées par les parties prenantes. En outre, le manque d'encadrement juridique du régime des DAO empêche toute récupération des fonds alloués en cas de

mauvaise exécution du service commandé dans le cadre d'un contrat intelligent. Pour Andrew Hinkes, avocat au sein du cabinet Berger Singerman LLP, le droit doit évoluer pour pouvoir prendre en compte ces nouvelles formes d'intervention dans le champ économique et financier : « *L'idée et la structure de The DAO présentent des ambitions légales extrêmement significatives. En particulier, les cours de justice seront forcées de réfléchir aux implications de la création d'une toile de contrats imitant le fonctionnement d'une entité, plutôt que le cas classique d'une entité reconnue juridiquement*. [...] *Les DAO ne sont aujourd'hui pas reconnues comme des acteurs de droit aux États-Unis*.

« *Cela crée un doute sur les actions légales portées par une DAO et les droits légaux d'une DAO. Il n'est pas clair si les actions d'une DAO seront attribuées à ses créateurs, à ceux qui entretiennent la DAO, à ceux qui proposent des projets, ou à ceux qui ont des intérêts dans la DAO. Bien que cela soit pratique de désigner un représentant humain, les détenteurs de jetons d'une DAO pourraient choisir de ne pas révéler l'identité d'un acteur de premier plan*[29]. »

Aujourd'hui, The DAO bénéficie de l'aura des membres de son conseil de surveillance (*curators*), Vitalik Buterin et une partie des membres fondateurs de la Fondation Ethereum, mais demain la confiance fondée sur la viabilité de cette société pourrait être remise en cause en leur absence. Dans le cas d'un changement de ce conseil, si les actionnaires majoritaires en termes de jetons possédés refusaient la nouvelle configuration de l'organisation de surveillance, The DAO serait alors scindée en deux DAO distinctes : The DAO originelle et TheNewDAO, détenant 49 % des parts de The DAO, une nouvelle société totalement indépendante.

DAOLink, sortir de l'impasse judiciaire

Pour pallier le vide juridique entourant les DAO, DAOLink propose une solution physique : le recours à une société enregistrée en Suisse, chargée d'établir un contrat physique à partir du contrat intelligent. Le contrat intelligent est d'abord rédigé sur Rootstock, sur la blockchain Ethereum, entre les deux cocontractants puis un contrat physique est signé avec la société suisse, en miroir du contrat intelligent. La société

DAOLink est donc la représentante de The DAO dans ses relations avec le cocontractant et devra s'acquitter de l'ensemble des obligations juridiques et fiscales du pays helvétique.

Pour les sociétés engagées dans des contrats intelligents, ce doublement de leur contrat avec une société physique, DAOLink, est une garantie d'application du droit, mais le problème est simplement relégué à un étage supérieur. En effet, comme la DAO ne dispose pas de statut juridique en soi, son contrat avec DAOLink n'est pas mobilisable dans un procès juridique. Par exemple, si la DAO ne verse pas les fonds de paiement d'une prestation, comment DAOLink peut-elle s'en défendre sur le plan juridique alors qu'elle est, officiellement, le cocontractant du contrat avec le prestataire ?

En juillet 2016, le hackage de The DAO à hauteur de l'équivalent de 50 millions de dollars a ainsi conduit à faire péricliter la plateforme en mettant en évidence d'importantes failles de sécurité. Dans le courant de l'été, un contrat intelligent unique a été proposé aux membres de la plateforme, sous la forme d'un contrat de retrait de leurs jetons DAO en ethers. L'évolution du cours du jeton au-delà de 100 tokens par ether (après le 14 mai 2016) a compliqué la donne et les utilisateurs sont restés longtemps dans l'attente d'un remboursement complet de leur engagement au sein de cette société privée.

Blockchain : la technologie blockchain sans bitcoin

L'émergence de la blockchain Bitcoin repose ainsi sur l'accumulation de la puissance de tous les ordinateurs reliés au réseau, aux technologies de registres distribués (*distributed ledger technologies*, DLT). Ces registres de données sont répliqués au sein d'un nombre infini d'ordinateurs et un algorithme commun assure que les données sont identiques entre toutes les sources d'enregistrement au même moment. Les grandes banques et institutions financières y trouvent leur compte en utilisant finalement les sous-jacents technologiques plutôt que leur version première. Ainsi pour les institutions financières, les registres distribués sont un outil de passage du bitcoin à la blockchain et de la blockchain à une technologie plus générique, sans mêler leurs

activités à la sulfureuse crypto-monnaie. C'est un glissement sémantique intéressant, mais qui vide beaucoup du contenu d'origine

Pour les experts de la Banque centrale européenne, les registres distribués dessinent ainsi l'avenir des grandes institutions financières. Certains consultants abondent dans le sens de leurs clients comme l'équipe de Bain & Company qui, dans son analyse de la blockchain en juillet 2016, expliquait : « *Le protocole originel sous-tendant les DLT trouve ses racines dans le monde anarchique des monnaies numériques, qui s'exprime et se développe à l'extérieur du système financier conventionnel. Le débat public sur les DLT a ainsi été concentré sur le potentiel révolutionnaire de cette technologie. Les DLT sont pertinents au-delà du bitcoin et son modèle de blockchain ouverte. D'autres types de DLT, comme les technologies restreintes et les smart contracts, sont plus adaptés aux besoins des institutions financières et pourraient contribuer au développement des procédures d'échange plus sûres, plus efficientes et plus efficaces*[30]. »

Le débat moderne sépare ainsi les registres distribués publics (*unrestricted DLT*) et les registres distribués privés (*restricted DLT*), en croisant le débat sur la sécurité des données et celui sur le secret de certaines données sensibles, comme les transactions financières et monétaires. Les registres distribués privés supposent de rendre publique l'identité des participants, au moins par « le corps de gouvernance du registre », pour pouvoir identifier des comportements douteux et sauvegarder la viabilité des données de la blockchain. Ce « corps de gouvernance » est placé entre les mains des utilisateurs ayant le plus long historique de transactions validées.

Comme on l'a vu plus haut, si l'on remplace les mineurs par des entreprises qui sont autorisées à miner, si l'on remplace la multitude des apports en puissance informatique, ces systèmes diminuent d'autant leur crédibilité en termes de sécurité et d'indépendance. Ça a le goût de la blockchain, la couleur de la blockchain mais ce n'est pas de la blockchain.

La cohabitation des blockchains

L'avenir est-il, alors, à la cohabitation de plusieurs formes de

blockchains ? C'est, en tout cas, la théorie de Luca Compari, actuel responsable de la blockchain chez IBM France : « "*La blockchain publique est idéale pour les marchés CtoC* [consommateur à consommateur] *et P2P* [pair-à-pair]*, tandis que les blockchains privées et les consortiums sont davantage adaptés au BtoB* [entreprise à entreprise]*. Pour le BtoC* [entreprise à consommateur]*, cela dépendra des contraintes du secteur". Résultat : des passerelles ou side chains vont être créées entre les différentes blockchains pour assurer leur interopérabilité*[31]. »

La chaîne latérale (*side chain*) est ainsi un outil de communication entre les différentes blockchains. L'idée est d'envoyer ses bitcoins d'une première blockchain B1 à une adresse d'immobilisation du réseau, puis d'adresser un message à une seconde blockchain B2 pour demander la création d'un nombre égal de jetons (tokens). Les bitcoins n'ont donc été ni créés, ni détruits, simplement déplacés d'une blockchain à l'autre. Cette opération de transfert des jetons peut être soumise à des frais, afin d'assurer la sécurisation du processus.

L'opération de communication entre les blockchains est donc devenue, en soi, une blockchain à part entière, ce qui en fait une structure entièrement décentralisée, sécurisée et visible de tous. À terme, rien n'empêche pourtant que la *sidechain* (chaîne collatérale) devienne une blockchain privée ou une blockchain consortium. Pour Adam Back et huit de ses collaborateurs, co-auteurs d'un papier « Permettre les innovations de la blockchain avec des chaînes latérales chevillées[32] » (2014), l'avenir de la sidechain est plutôt celui d'un système semi-décentralisé, miné par une centaine de compagnies, réunies en une confédération peu structurée (*loose confederation*).

La sidechain au service des contrats intelligents

En mars 2016, un groupe de programmateurs a eu l'idée d'appliquer le fonctionnement de la blockchain Ethereum, notamment en matière de contrats intelligents, à la blockchain Bitcoin, grâce à la technologie sidechain. Cette nouvelle interface, baptisée Rootstock, permettra ainsi d'appliquer des contrats intelligents sur la blockchain Bitcoin.

Aujourd'hui soumise à un rythme de 300 transactions par seconde, cette nouvelle sidechain ambitionne d'évoluer vers les 1 000 transactions par seconde à très court terme. Le minage sera néanmoins effectué conjointement à la seule blockchain Bitcoin dans le cadre d'une procédure de minage partagé (*merge mining*).

En tant que sidechain, Rootstock ne créera pas de nouvelle monnaie numérique, mais elle disposera d'un jeton propre (token), le RTC. Son système de rémunération du minage des transactions sera donc basé sur un ancrage dans deux monnaies (*two-way pegged*) : son jeton, le RTC, et le bitcoin. Les utilisateurs de cette nouvelle plateforme devront donc transférer des bitcoins vers Rootstock, selon le processus immobilisation/création détaillé plus haut. Les transferts entre les deux monnaies peuvent être répétés en sens inverse. Cependant, dans la mesure où la blockchain Bitcoin ne reconnaît pas les transactions inscrites sur d'autres blockchains, cette mobilité des capitaux nécessite quelques accommodements.

Rootstock recourt en effet au soutien d'une fédération d'entreprises bitcoin de premier ordre, chargées d'assurer la sécurité des transferts de fonds de la blockchain Bitcoin vers la sidechain Rootstock. Pour effectuer une transaction, le verrouillage et le déverrouillage nécessitent donc une opération multi-signatures gageant la viabilité du transfert monétaire. Cette mission d'assurance pourra générer des frais. Ce modèle limite donc considérablement l'aspect décentralisé de la blockchain, dans la mesure où le recours à un tiers est devenu une nécessité temporaire.

Être exhaustif sur le sujet est difficile tant de nouvelles initiatives se créent chaque jour et d'autres se défont aussi rapidement. Dans cette ébullition de projets, nous pouvons distinguer que les fondamentaux restent invariables. Il s'agit de bâtir sur le protocole blockchain, mariage de l'informatique fortement distribuée, la théorie des jeux et la cryptographie, pour produire de nouvelles applications capables de créer un consensus sur ce qui est vrai.

C'est une véritable mécanisation de la confiance que l'on vient d'inventer.

L'aventure ZCash, aux portes d'une nouvelle ère

Fin octobre 2016, la technologie blockchain a donné naissance à une nouvelle monnaie le *zcash* (ZEC), fondée sur davantage d'anonymat et de sécurité. Une constante dans l'univers des monnaies numériques. Dans ce nouveau système de crypto-monnaie, les gains de l'activité de minage sont répartis entre le mineur (10 ZEC/bloc) et les créateurs de la monnaie (2,5 ZEC/bloc). Le 28 octobre 2016, à son lancement, cette nouvelle devise numérique était surcotée à pas moins de 1 600 bitcoins, soit plus de 1 million de dollars par unité. À horizon de dix ans, le système ZCash était ainsi valorisé par près de 2 000 milliards de dollars, soit un tout petit moins que le PIB annuel de la France. Le cours s'est, depuis, rapidement stabilisé, avec une valeur unitaire autour de 10-12 bitcoins, soit 8 000 dollars.

En projet depuis deux ans, ZCash s'appuie sur le protocole ZKIP (en français, la preuve à divulgation nulle de connaissance), principe cryptographique permettant d'authentifier ou d'identifier sans fournir d'autre information que la réponse à la question posée. Il a été amélioré et rebaptisé pour l'occasion « Zk-Snark », pour accroître l'intraçabilité des échanges en ligne. La complexification à outrance des énigmes mathématiques utilisées dans les preuves d'enjeu et de travail permet en effet de sécuriser encore plus l'adresse d'envoi, de réception et même le montant de l'échange. Les opérations sont ainsi quasi indécodables. Vitalik Buterin, participant aussi dans ce nouveau projet, a récemment annoncé l'application de ce nouveau protocole Zk-Snark à la blockchain Ethereum d'ici 2018.

La sécurité de cette nouvelle crypto-monnaie, aux ambitions déclarées, sera la clé de son succès ou de son échec à venir. La clé publique de ce nouveau réseau a ainsi été éclatée en six « éclats » (*shards*) confiés aux six pères-fondateurs de cette nouvelle devise numérique : Zooko Wilcox (le fondateur), Andrew Miller, le chercheur Peter Van Valkenburgh, le développeur Peter Todd et deux autres personnes encore inconnues. Le protocole de sécurité est ainsi appelé « calcul à multi-parties prenantes » (*secure multi-party computation*, MPC), puisque tous les éclats sont nécessaires à une opération de piratage de la plateforme. Ces éclats, considérés comme des « déchets

toxiques » par Zooko Wilcox, ont fait l'objet d'un traitement particulier. À l'occasion d'une cérémonie quasi rituelle, chacun des six fondateurs a détruit son ordinateur avec une flamme au propane, afin de s'assurer que personne ne puisse jamais contourner la sécurité du réseau. Une mesure draconienne mais un gage de confiance sérieux à adresser aux futurs utilisateurs du zcash.

Mille et un usages de la blockchain

« Très loin d'un conte de fée libertarien ou d'une nouvelle de type "Sillicon Valley", Bitcoin offre une vue large des nouvelles méthodes de fonctionnement du système financier à l'ère d'Internet. C'est un catalyseur formidable de la construction d'un nouvel environnement à la fois bénéfique aux individus et aux entreprises. »

MARC ANDREESSEN, *The New York Times*, 21 janvier 2014[33]

À l'hiver 2014, assis autour d'une table recouverte d'une nappe de carreaux rouges et blancs du fameux restaurant « Le Roi du pot au feu », Thierry Petit, associé et dirigeant du site de vente privée ShowRoomPrivé depuis introduit en Bourse, me demande de lui expliquer à nouveau les usages possibles de la crypto-monnaie. Nous avons une longue discussion autour de notre plat hivernal préféré et, après quelques échanges sur l'impact qu'aura bientôt sur la société la blockchain, Thierry me dit « Essayons ! Acceptons les bitcoins sur l'un des plus grands sites de commerce électronique européens, lançons le projet cet été dès que nous aurons un peu de temps ». Après quelques jours et l'aide de l'équipe de Paymium, le site de e-commerce accepte les bitcoins. Le paiement dans un site de e-commerce par la monnaie décentralisée est un premier exemple mais mille nouveaux cas vont germer dans le monde.

Je vous ai parlé des origines culturelles et historiques, des mécanismes de fonctionnement et des théories les plus complexes, laissez-moi désormais vous présenter les usages pratiques de la technologie blockchain. En effet, je crois intimement que la blockchain peut aider à répondre aux défis des grandes transitions de notre siècle. Elles sont au nombre de cinq : transition démographique, transition écologique, transition numérique, transition monétaire et transition

démocratique. Ces sujets sont des problématiques centrales dans l'évolution de notre société, car ils vont bouleverser nos façons de penser et de vivre. Inutile donc de nous cacher le fait que nous devrons y faire face tôt ou tard.

Lorsque l'on s'intéresse aux différentes composantes du fonctionnement d'une société, cinq éléments reviennent en permanence dans l'agencement idéal d'une communauté travaillant en bonne intelligence. Ces cinq niveaux sont bien distincts mais permettent de comprendre la société comme un ensemble : l'identité, la propriété, le transfert ou l'échange, le contrat et le marché. Ils régissent ainsi la nature de l'individu et de ses possessions (identité/propriété), sa capacité à dialoguer avec d'autres individus (transfert et échange/contrat) et le processus global de création d'une société (marché).

Dans les premières années de la blockchain Bitcoin, l'implémentation informatique a surtout concerné la propriété et le transfert, parce que les nouvelles communautés numériques étaient portées par le désir d'échanger sans frontière, de partager sans s'imposer le respect de certaines règles contraignantes. Puis, avec le renforcement des technologies cryptographiques et l'émergence des contrats intelligents, l'identité et le marché ont changé de fonction et se sont retrouvés plongés au cœur des processus de transformation animés par la révolution technologique.

Figure 1 L'agencement idéal d'une communauté travaillant en bonne intelligence

Échange

Propriété

Identité

Ces transformations agissent, aujourd'hui, sur quatre principaux secteurs sociétaux ou, autrement dit, quatre grandes familles d'usage de la technologie blockchain : les crypto-monnaies, c'est-à-dire notre système monétaire, la finance au sens général du terme, les nouvelles gouvernances des organisations déjà existantes, notamment notre système politique, et l'émergence d'organisations décentralisées de gestion des communautés ou des nouvelles formes d'économie (économie collaborative, économie solidaire et sociale). C'est à travers ce prisme de sujets que nous traiterons des usages multiples de la technologie blockchain et ses perspectives de développement à venir.

Très tôt, les cypherpunks ont cherché à penser ces grands secteurs sociétaux dans une logique de protection de la vie privée. Une société de l'information fonctionnelle repose, en effet, sur un ensemble sur ces cinq couches : l'identité, la propriété, l'échange, le contrat et le marché. Ces cinq éléments appartiennent à une structure d'ensemble de communication, dans le fonctionnement de laquelle la cryptographie sert de protection des individus, par l'entremise d'outil comme l'anonymat ou la signature numérique.

Ce découpage de ma réflexion sur les usages de la blockchain est le produit de mon expérience personnelle de cette technologie. En 2014, j'ai travaillé avec les équipes en charge de la stratégie de BP2S (filiale

de BNP Paribas) à l'occasion d'un brainstorming sur les effets de la révolution blockchain sur le secteur de la titrisation. Deux ans plus tard, ils ont été les premiers à développer une application consacrée. À nouveau, en 2015, je me suis associé aux efforts de Benoît Bazzocchi, à l'époque en pleine création d'une plateforme de finance participative, SmartAngels, pour comprendre comment catalyser et orienter au mieux les nouvelles formes de financement numérique. Cette thématique est aujourd'hui au cœur des réflexions en matière d'évolution des finances publiques. La blockchain est donc un vecteur d'évolution de notre monnaie, mais plus généralement de notre système économique et financier.

Identité et propriété, quels piliers pour notre société ?

En philosophie, l'identité se définit comme ce qui demeure intact dans un corps en changement perpétuel. Elle caractérise aussi ce qui fait que plusieurs individus distincts témoignent d'un sentiment d'appartenance à une même chose. La société comme assemblée des hommes se construit donc sur la base d'une identité commune, une sorte de garde-fou culturel et comportemental, en dépit de nos millions d'années d'évolution. Pour des philosophes comme Thomas Hobbes ou Jean-Jacques Rousseau, les hommes ont conclu un pacte social, reconnaissant leurs intérêts communs et engageant une coopération en vue de l'établissement d'un monde meilleur.

Dans cet effort, les sociétés ont donc défini ce qui appartenait à chacun, la propriété privée, et ce qui appartenait à tous, la propriété publique ou commune. Autrement dit, elles ont créé et consacré la notion de propriété, c'est-à-dire le qualificatif d'appartenance d'un bien à une personne ou un groupe de personnes. En fait, la propriété a même précédé la naissance des communautés contemporaines : c'est le désir de prétendre à la propriété d'autrui qui nourrissait le vol et la violence. La souscription du contrat social a donc régulé les évolutions de la propriété selon des règles précises : échanges multiples, achats et ventes, legs et héritages, etc.

En 1840, dans *Qu'est-ce que la propriété ?*, le philosophe français

Pierre-Joseph Proudhon renverse cette vision des choses et accuse la propriété de privilégier les riches face aux pauvres : « *Si j'avais à répondre à la question suivante : Qu'est-ce que l'esclavage ? et que d'un seul mot je répondisse : c'est l'assassinat, ma pensée serait d'abord comprise. Je n'aurais pas besoin d'un long discours pour montrer que le pouvoir d'ôter à l'homme la pensée, la volonté, la personnalité, est un pouvoir de vie et de mort, et que faire un homme esclave, c'est l'assassinat. Pourquoi donc à cette autre demande : Qu'est-ce que la propriété ? ne puis-je répondre de même : c'est le vol, sans avoir la certitude de n'être pas entendu, bien que cette seconde proposition ne soit que la première transformée ?* »

Dans l'univers de la blockchain, ces deux fondements de la société humaine, l'identité et la propriété, sont pleinement remis en question. L'identité, d'abord, est plus que jamais nécessaire dans une société soumise à de profondes mutations technologiques et donc à des évolutions économiques et sociales : révolution des nouvelles technologies, émergence du Web 3.0, transformation de nos rapports et de nos comportements, etc. Que reste-t-il de notre société originelle et de notre contrat sociétal dans cette nouvelle configuration des rapports humains, économiques et sociaux ?

La propriété, ensuite, est remise en question à l'heure où les inégalités entre les plus riches et les plus pauvres n'ont jamais été aussi fortes. Le numérique a participé à accroître l'accessibilité de la connaissance et des brevets technologiques, interrogeant la pertinence du bien privé. Il a, en même temps, accéléré le partage des informations et nourrit une nouvelle forme de participation démocratique et politique. Ces inégalités ne sont-elles pas devenues intolérables ? Ne faut-il pas revenir sur la consécration de communs, propres au bien de l'humanité, insusceptibles d'être détenus par quelques-uns ?

Dès le XII^{e} siècle, nos ancêtres avaient compris la nécessité d'une gouvernance spéciale pour les biens essentiels à la vie (air, eau, terre). La gestion de l'agriculture et de l'alimentation des populations avait conduit à consacrer certains biens dans leur propriété collective. Le modèle d'appropriation à outrance des ressources naturelles connaît aujourd'hui ses limites et nous invite à redéfinir, ensemble, des biens communs, également distribués entre tous. Le numérique aide à cette révolution de l'esprit en facilitant les échanges entre les communautés

et en créant un espace virtuel, le Net, à la fois interface et plateforme de concentration des biens et des connaissances. L'économiste Michel Bauwens parle ainsi d'une « troisième voie » dans la gestion numérique des échanges.

Des échanges en quatre points

Remontons le temps un instant. Historiquement, le système d'échange entre les hommes peut être matérialisé comme une courbe tracée entre quatre points. Dans le cas d'un consommateur et d'un magasin, le consommateur donne d'abord un ordre de virement de la valeur du bien acheté à sa banque, laquelle transfère ensuite ce virement à la banque du magasin, laquelle prévient enfin le magasin de la réception du virement, ce qui conclut la transaction. L'information de l'échange monnayé est donc passée par quatre acteurs différents : l'acheteur, sa banque, la banque du magasin et le magasin. Dans le détail, ce système d'échange compte même un cinquième point, puisqu'une interface existe souvent entre le consommateur et sa banque, la plupart du temps sous la forme d'une carte de crédit.

La carte de crédit a, ainsi, fait son apparition il y a plus d'un siècle, en 1914, lorsque l'entreprise américaine Western Union, spécialisée dans le transfert d'argent, a abandonné ses prétentions dans le secteur du télégraphe et a recentré ses activités autour de la banque et de la finance. Un demi-siècle plus tard, la naissance des réseaux Interbank et Charge Master (1967), plus tard fusionnés au sein du géant MasterCard, et le développement du Groupe Carte Bleue (1971), alliance de six grandes banques françaises, a accéléré le déploiement de cette solution de retrait et de paiement. En 1974, un premier accord international est finalement signé.

Après la naissance de Visa, en 1977, et la mise en place du Groupe Cartes Bancaires en 1984, union des banques françaises liées à Visa ou MasterCard, la carte de crédit a enchaîné une série rapide de révolutions techniques : mise en place des cartes de crédit « prestige » dans la seconde moitié des années 1980, création d'une centrale des règlements interbancaires à gros montant en 1994, développement des lecteurs de puces dans les guichets automatiques bancaires en 1995,

expérimentation du porte-monnaie électronique en 1998, création d'une carte de paiement international à autorisation systématique la même année, et finalement lancement du paiement en ligne en 2000.

J'ai eu l'occasion, en 2016, d'assister à la grand-messe européenne des clients du système bancaire Visa. Cette expérience m'a laissé un sentiment diffus d'étonnement à l'égard de la politique menée par l'industrie financière dans ce secteur. La politique d'innovation y est claire : le système d'échange en quatre points y est un horizon indépassable. Les banques ont su s'imposer comme des acteurs incontournables des systèmes d'échange entre acheteur et vendeur et il n'est pas question que cette situation change à court terme.

L'émergence d'un nouveau système d'échanges en trois points a cependant forcé l'évolution de l'oligopole des banques sur nos pratiques bancaires. Vont-elles, pour autant, accepter de passer à un système à des millions de points ? C'est un réseau dans lequel les banques pourraient jouer un rôle tout à fait différent ! J'ai eu l'occasion de poser une question au CEO de Visa, et je l'ai naturellement interrogé sur la pertinence d'une « société sans cash ». Il m'a vite répondu du tac au tac que « le cash c'est pour les criminels ». Le tout numérique serait un outil de lutte contre le banditisme et la criminalité. La transformation monétaire serait alors le préalable d'une transformation de nos sociétés !

Les échanges en trois points

En 1998, deux start-up américaines, Confinity et X.com, fusionnent pour former l'entreprise PayPal, spécialisée dans le service de paiement en ligne. À l'époque, Confinity apporte une connaissance technique de l'ingénierie des paiements, avec une spécialisation en cryptographie, tandis que X.com, un des premiers-nés de l'entrepreneur américain à succès Elon Musk, propose des services de banque en ligne. L'alliance des deux compagnies met en place un système dans lequel un paiement bancaire peut être exécuté en ligne, sans communication des coordonnées bancaires.

Désormais, le paiement en ligne ne nécessite plus qu'une adresse électronique et un mot de passe. Le compte PayPal permet aussi

d'effectuer un transfert de fonds d'un compte bancaire à un autre, sans passer par l'intermédiaire de la banque, à condition que les deux acteurs du transfert disposent d'un compte sur le site. Cette interaction court-circuite les banques et permet d'éviter les frais bancaires de virement international. La globalisation des échanges et l'accélération des échanges en ligne ont assuré le succès de cette nouvelle application.

Dans ce nouveau système d'échanges à trois points, de l'acheteur à l'interface en ligne et de la même interface au vendeur, la réglementation des rapports entre les acteurs n'est plus la même. PayPal a en effet mis en place un système dans lequel les acheteurs bénéficient d'un traitement privilégié par rapport aux vendeurs. Lorsqu'un acheteur procède à l'acquisition d'un produit en ligne, il peut déposer une revendication à l'encontre du vendeur (à cause de la qualité du produit reçu, de son état ou encore du temps d'acquisition), gelant le paiement en ligne. PayPal est alors responsable de la procédure de règlement du litige et décide de l'état final du virement au regard des documents fournis par l'acheteur et le vendeur.

Pour les vendeurs, l'option de PayPal reste néanmoins une solution avantageuse, car elle permet d'économiser les frais imposés par les banques à l'installation d'une solution de paiement en ligne. PayPal ne requiert ainsi aucun contrat de vente à distance et se rémunère uniquement à travers une commission sur les transactions (entre 1,4 et 3,4 % selon le prix de la transaction, avec un prix fixe minium de 0,25 euro par transaction). Ce système de portefeuille centralisé souffre néanmoins de critiques sur sa faiblesse en termes de sécurité, d'abus de pouvoir et de protection de la vie privée.

La réglementation européenne encadre, depuis 2007, ce nouveau système d'échanges et de compte bancaire connecté à travers une directive originelle sur les services de paiement de novembre 2007 (DSP 1) et une directive renouvelée sur les services de paiement de novembre 2015 (DSP 2). Ce texte juridique garantit un accès équitable et ouvert aux marchés des paiements en ligne et renforce la protection des consommateurs, en particulier en cas de remboursement des prélèvements automatiques fraudés ou de frais liés à une perte ou un vol de carte de paiement. Il met notamment en œuvre un espace unique de paiement en euro, incluant une harmonisation des moyens de

paiement.

La nouvelle économie des transferts

Pour Nick Szabo, dans sa célèbre conférence sur l'histoire de la blockchain à Devcon One, qui se tenait à Londres en novembre 2015, la société s'est donc progressivement construite sur la base de cette notion de propriété et sur l'application du contrat. La régulation de l'échange entre deux parties a contribué à mieux comprendre et encadrer les différends relatifs à la propriété et à rémunérer chacun à hauteur de son influence sur son environnement direct. La dynamique du développement durable de nos sociétés a transformé nos modèles économiques en des comportements plus soucieux de la propriété publique : économie verte, économie de la fonctionnalité, économie de la performance environnementale, etc.

Ces nouvelles activités économiques visent à accroître le bien-être humain et l'équité sociale des hommes, voire la préservation de l'environnement, bref à considérer que la propriété n'est pas la seule mesure de la richesse humaine. Ce débat rejoint, ici, celui que nous avons ouvert plus haut sur la monnaie comme mesure de la croissance des pays. Ne faut-il pas prendre en compte de nouveaux indicateurs de richesse dans la mesure de la propriété humaine au XXI^{e} siècle ? Le capital d'un individu se mesure aussi à son éducation, à sa santé, à sa capacité à adopter des comportements respectueux de la nature.

Dans la nouvelle économie, la transparence des échanges est aussi devenue une règle de bonne conduite des rapports humains. La transparence est en effet consacrée comme un vecteur de sécurité économique et un outil de renforcement de l'état de droit et de la démocratie. Le citoyen moderne est ainsi, pour paraphraser Pierre Rosanvallon, « un électeur et un contrôleur », c'est-à-dire qu'il renonce à exercer un pouvoir politique au nom de son représentant public, mais qu'il exerce en même temps un contrôle sur l'action publique à travers son observation vigilante de la vie quotidienne.

Le manque de transparence est devenu intolérable dans les nouveaux systèmes économiques, parce que, dans une société du tout public, la sphère privée est devenue le marqueur du secret et des intentions

cachées : « *Tous les pays devraient être libres de fixer leurs propres taux d'imposition et de mettre en place leurs systèmes fiscaux*, écrit Grace Perez-Navarro, directrice adjointe du Centre de politique et d'administration fiscales de l'Organisation de coopération et de développement économiques (OCDE). *Ce qui n'est pas acceptable, c'est la concurrence fondée sur un secret excessif. Le secret bancaire lui-même n'est pas en question. Tous les pays l'appliquent sous une certaine forme, il répond à un objectif légitime dans le monde financier, notamment la protection de la vie privée et des droits individuels. Cependant, le respect de la confidentialité n'est pas un droit absolu et doit être compensé par le besoin légitime, pour les gouvernements, d'appliquer leur législation, y compris fiscale.*

« *L'OCDE estime que cet équilibre peut être atteint en assurant une certaine transparence pour l'échange effectif de renseignements. Cela implique l'interdiction de l'utilisation de comptes anonymes, désormais appliquée par tous les pays de l'OCDE, et l'amélioration de la qualité et de la disponibilité des informations concernant les propriétaires de sociétés fictives, de fondations ou autres entités non transparentes utilisées par les fraudeurs et autres auteurs d'abus fiscaux comme le blanchiment pour dissimuler leurs identités et leurs actifs aux autorités chargées d'appliquer la loi*[34]. »

La révolution bitcoin porteuse de multiples applications

La révolution des monnaies numériques, en particulier du bitcoin, est d'abord celle de la confiance. Les précédents chapitres sur la monnaie et le fonctionnement de la blockchain ont longuement insisté sur l'importance de cette croyance en la stabilité du système dans son maintien sur le long terme. La confiance a donc migré d'une confiance historique en les institutions, comme marqueurs de stabilité, à une confiance nouvelle en les individus, détenteurs d'un moindre pouvoir et donc moins poussés à en abuser. Après tout, Montesquieu n'a-t-il pas écrit dans *De l'esprit de lois* (1748) que « *tout homme qui a du pouvoir est porté à en abuser* » ?

En tant qu'outil décentralisé et transparent, la blockchain est

l'instrument technologique de cette nouvelle confiance. En 2015, un glissement s'est opéré entre la blockchain Bitcoin, historiquement conçue comme un instrument de fonctionnement et de régulation de la monnaie numérique, et les nouvelles blockchains, appliquées à de nombreux autres champs de la société. Nous avons, d'ailleurs, évoqué certaines d'entre elles, comme la blockchain Ethereum. Cette évolution est aussi un simple changement de terminologie. Une évolution de bitcoin à la blockchain qui accompagne en fait un mouvement de modernisation globale de nos sociétés, emportées par l'élan des nouvelles technologies, sans avoir à remettre en cause le rôle central et sacré de la monnaie.

L'émergence des contrats intelligents est ainsi le témoin de cette globalisation de la technologie blockchain. Il ne s'agit plus seulement de stocker des bases de données bancaires et financières mais d'appliquer les règles de la technologie blockchain à des domaines tels que la location de logements ou de véhicules. Dans une tribune-fleuve sur les récentes transformations de la blockchain, publiée à la fin du mois d'octobre 2015, *The Economist* est donc revenu sur les applications multiples de la blockchain : « *Les problèmes bancaires ne sont donc pas seuls* [à susciter des besoins de révolutions techniques]. *Toutes sortes d'entreprises publiques et privées souffrent aujourd'hui de bases de données trop difficiles à entretenir, souvent incompatibles entre elles, et très coûteuses en termes de gestion ou de coopération*. [...] *Et* [la blockchain] *vient répondre à cela, avec un langage programmatique qui permet à tous les utilisateurs d'écrire des contrats intelligents sophistiqués, et ainsi de créer des logiciels qui ordonnent automatiquement des virements lorsqu'un colis arrive ou qui partagent des certificats qui envoient automatiquement des dividendes à leurs possesseurs en cas de profits élevés*[35]. »

La blockchain au cœur du futur de la banque

Pour Blythe Masters, économiste et icône des marchés financiers modernes, ancienne cadre de JP Morgan, aujourd'hui à la tête de la start-up Digital Asset Holdings, la blockchain représente en effet l'horizon vers lequel les échanges bancaires et financiers évolueront

dans les années à venir. En avril 2016, à la conférence Money20/20 de Copenhague, elle est ainsi longuement revenue sur les évolutions technologiques à venir du secteur : « *Ma vision des choses est que nous verrons cette technologie* [blockchain] *se déployer sous des formes variées dans le secteur du commerce dans les deux années à venir. Cela ne signifie pas que cette technologie sera devenue la règle dans ce même temps, je pense d'ailleurs qu'il faudra cinq à dix ans pour qu'elle devienne suffisamment populaire !* »

Pour les banques, la blockchain est en effet l'assurance d'une plus grande transparence des transactions financières à l'heure des scandales de blanchiment et d'évasion fiscale, et d'une réduction des coûts de l'ordre de 5 à 10 %. La banque espagnole Santander, une des premières à introduire l'usage de la technologie blockchain dans ses paiements internationaux en juin 2016, estime ainsi que cette révolution technologique permettrait des économies de l'ordre de 15 à 20 milliards de dollars par an. Pour le journaliste des *Échos* Guillaume Meaujean, « *c'est toute la finance qui pourrait s'en trouver transformée – ubérisée, diraient certains*[36] ».

L'entreprise R3CEV LLC de David Rutter, créée en 2014, s'inscrit d'ailleurs dans cette perspective, en menant des recherches importantes dans le champ des usages financiers de la blockchain, pour près de 45 banques internationales (Barclays, JP Morgan, UBS, Société générale). En janvier 2016, de premiers essais ont lieu en partenariat avec la blockchain Ethereum et Microsoft, de nouveau répétés en mars 2016 avec le concours d'une quarantaine de banques internationales. Cet engouement n'est cependant pas sans limite, ainsi que Blythe Masters l'a maintes fois souligné : « *Trois facteurs sont souvent cités comme problématiques. Numéro un : il y a des incertitudes quant à la régulation. Numéro deux : la question de l'ambition de créer un effet de réseau, d'avoir de multiples parties s'accorder sur une infrastructure partagée. Et la dernière, numéro trois : la question de la création de standards communs, tels qu'il n'y a pas de risque pour un primo-pratiquant qu'une solution soit choisie sans publicité entraînant le réseau à devenir Betamax, alors que le reste du monde a engagé sa transition vers VHS*[37]. »

L'apparition de la « smart property »

Avec la multiplication des contrats émergents et la consolidation des bases de données de la blockchain, une nouvelle forme de propriété numérique s'est développée : la propriété intelligente (*smart property*). Elle désigne la propriété détenue à la fois sur des actifs matériels (location d'un appartement ou d'un véhicule) et sur des actifs immatériels (crypto-monnaie, brevets technologies). La *smart property* se caractérise aussi par un recours fréquent à la cryptographie et aux solutions de la tokenisation pour protéger les actifs de toute tentative de vol ou de corruption.

Pour Adam Rothsein, auteur freelance et journaliste spécialisé dans la blockchain, la *smart property* est une révolution culturelle tout autant que technique : « *Plutôt que d'enregistrer la propriété dans une unité de monnaie non physique et cryptographique utilisant des bases de données pair-à-pair, les bases de données de la* smart property *(la blockchain) suivent les contrats qui déterminent l'accès à des choses comme les voitures, l'immobilier ou les capitaux. Votre propriété sur une voiture n'est alors plus seulement une simple feuille rose, c'est aussi une entrée dans la blockchain, en d'autres monnaies, un crypto-coin*[38]. »

La *smart property* est ainsi aux biens ce que le bitcoin a été à la monnaie : une transformation conceptuelle, balayant du revers de la main le besoin d'une autorité centrale. En fait, cette évolution vers un système d'échange plus restreint, en tout cas à moins d'acteurs, recouvre la nouvelle capacité des individus à mieux se comprendre et s'appréhender, bref à saisir pleinement et rapidement l'identité de la personne avec laquelle ils échangent. Cela répond à l'émergence de nouvelles technologies d'identification depuis le début des années 2000 : reconnaissance numérique des empreintes digitales, de l'iris, du visage, etc.

La start-up Onename (née en 2014) surfe ainsi sur cette vague technologique, liant blockchain/tokenisation et procédures d'identification. Elle propose en effet de stocker sur la blockchain des caractéristiques d'identification de l'individu, de son identifiant à ses empreintes digitales ou son iris, afin de les lier irrémédiablement à d'autres comptes en ligne, comme Facebook ou Twitter. L'idée est ainsi

de consolider et de sécuriser l'identité blockchain des utilisateurs (*blockchain ID*). Cette transformation des usages techniques de la blockchain marque-t-elle la fin du règne de la blockchain anonyme ? La marche vers une popularisation de la blockchain signe-t-elle une nouvelle étape de son histoire ?

Onename prétend, cependant, préserver la sécurité de l'identité de ses utilisateurs en décentralisant ses données d'authentification sur les millions d'ordinateurs de ses utilisateurs, sur la base de la technologie blockchain. Le délai de validation de l'identité blockchain créée peut varier de douze heures à trois jours et réserve une nouvelle manne économique aux juteuses activités de minage des internautes. Jusqu'à présent hébergé sur la blockchain Namecoin, ce service monte, pas à pas, les marches de la notoriété et ambitionne aujourd'hui de migrer vers la blockchain Bitcoin. Autant dire que vous risquez d'en entendre parler prochainement !

Les « smart marketplaces », l'avenir de la blockchain

La décentralisation des bases de données ouvre la voie à la décentralisation des marchés : c'est l'ambition des marchés décentralisés (*smart marketplaces*). Aujourd'hui fortement développés dans le domaine de l'énergie, ces nouveaux marchés sont une réalité déjà concrète : les consommateurs énergétiques d'hier sont devenus des producteurs, dotés de panneaux solaires, de petites éoliennes ou de mini-centrales hydrauliques, et des vendeurs sur les marchés. Le développement des réseaux intelligents (*smart grids*) et la course à la modération des coûts carbone de l'énergie, c'est-à-dire liés à la pollution, encourage cette forme d'économie locale.

La technologie blockchain accompagne la création et le développement de ces nouveaux marchés, en assurant une communication rapide, efficace et sûre aux millions d'utilisateurs des réseaux énergétiques. Le numérique apparaît ainsi comme un accélérateur de notre ambition de mettre en œuvre un développement durable de nos sociétés et de retrouver des équilibres économiques et sociaux de proximité. Sur le plan culturel, c'est la naissance du

mouvement des « prosumers », citoyens producteurs des biens consommés, sous toutes les formes modernes de consommation.

La plupart des analystes prévoient qu'à cause de la réduction prédictible des crédits issus de la vente de ces excédents énergétiques, il y aura une augmentation du nombre d'installations de production et de vente locale d'énergie, au sein des communautés locales. La blockchain peut mettre en place un tel marché énergétique hautement décentralisé. C'est le cas de l'exemple de TransActive Grid, une start-up de Brooklyn, qui a mis en pratique un tel réseau énergétique fondé sur la blockchain. On peut citer aussi, Grid Singularity qui utilise un mécanisme « pay-as-you-go » dans les pays en développement.

Pour Goldman Sachs, ce marché décentralisé de l'énergie serait capable de dégager un profit de 2,5 à 6,9 milliards de dollars par an, grâce à la mobilisation de la technologie blockchain. Le déploiement des panneaux solaires et de l'énergie électrique d'origine photovoltaïque en serait considérablement accru, intégrant les démarches internationales de promotion des énergies vertes et d'une économie décarbonée. La blockchain est donc un atout incommensurable des politiques environnementales d'accompagnement du développement des énergies renouvelables dans leur substitution aux énergies fossiles (pétrole, gaz, charbon).

Plusieurs fois évoqué avec Julien Bayou, le jeune porte-parole d'Europe Écologie les Verts, la blockchain peut porter en son sein le pouvoir de résoudre l'équation du changement climatique par un meilleur partage des rapports entre consommation et production au niveau local. La technologie blockchain est, d'ores et déjà, au service de cette révolution des usages de l'énergie : TransActive Grid propose ainsi de supporter un marché régional de création et de vente d'énergie verte, Solcrypto s'inscrit sur le même segment mais se limite à la production électrique d'origine photovoltaïque, etc. Les avantages de la blockchain s'étendent ainsi du stockage des données de ressources énergétiques (ElectriCChain) à la mise en œuvre de l'Internet des objets (RWE en partenariat avec Slock.it, BanyMoon).

Des grilles vertes qui auront besoin d'une

crypto-monnaie

En 2000, le Japon s'est posé comme précurseur de ces *smart marketplaces*, en développant un système de valorisation de l'énergie verte produite par des coopératives citoyennes locales. Lorsque les membres de ce réseau, pour la plupart, des ménages modestes, produisent 1 kilowatt-heure (KwH) d'énergie verte, ils peuvent normalement le revendre entre 75 et 100 yens sur le réseau électrique national ou régional, soit 60 à 90 centimes d'euro. Cette possibilité légale fait suite aux nombreuses campagnes politiques de promotion des énergies renouvelables locales (panneaux solaires, petite éolienne, petite centrale hydraulique) et a été fortement renforcée après l'incident nucléaire de Fukushima, en mars 2011.

Un groupe de citoyens japonais décide alors de profiter de cette initiative énergétique pour développer une monnaie locale complémentaire, le WAT (pour 1 kWh). À l'époque, le système proposé est révolutionnaire : décentralisation des serveurs de la monnaie complémentaire sur quelques ordinateurs, pas de cotisation d'inscription au réseau d'échange de la monnaie, administration pair-à-pair des transactions les plus complexes. La monnaie WAT est imprimée sur un papier ou un petit ticket et les modestes coûts d'impression sont pris en charge par les entreprises partenaires, trop heureuses de pouvoir profiter de la publicité acquise par leur soutien affiché à une telle initiative.

Dans le système WAT, n'importe quel particulier peut produire des WAT, mais la réputation de chaque personne joue sur la faisabilité d'un tel processus et l'acceptation des unités de monnaie émises. La confiance des usagers en la pertinence des acteurs du système monétaire est ainsi, comme à l'habitude, au cœur du système monétaire complémentaire. L'adhésion au système WAT se fait par la simple acceptation des tickets WAT comme monnaie d'échange, d'où l'extraordinaire rapidité de sa propagation au Japon. Cette monnaie complémentaire compte aussi une dimension politique forte, avec une vocation à accomplir la révolution de l'économie sociale et solidaire.

Le WAT, comme de nombreuses autres monnaies complémentaires, s'inscrit donc dans une volonté de résoudre un problème particulier : isolement des personnes âgées (système *Furei-Kippu* au Japon),

chômage (système LETS [*local exchange trading system*, système d'échange local] au Canada) ou encore dégradation de l'environnement (système WAT au Japon). En France nous avons choisi un système de certificat : les certificats d'économies d'énergie (C2E). Ils aident à financer des travaux visant à obtenir des économies d'énergie. Ce sont des foyers qui peuvent les vendre à des « obligés » qui sont des fournisseurs d'énergie. Ces producteurs ou distributeurs doivent racheter ces certificats pour prouver qu'ils financent correctement la réduction de consommation. Nous avons choisi un système centralisé qui aurait pu être traduit par une monnaie décentralisée.

Par l'entreprise du développement d'une nouvelle monnaie, complémentaire à la monnaie nationale, la blockchain joue donc un rôle de premier plan dans la transformation de la société contemporaine et dans l'émergence de nouvelles solutions.

L'Internet des objets, un pari gagnant

Cette extension de la blockchain à d'autres champs que son espace originel, celui de la crypto-monnaie bitcoin, épouse les formes de l'Internet des objets (*Internet of things*, IoT). Il s'agit en effet de prolonger l'utilisation d'Internet dans l'usage quotidien d'objets physiques, d'où l'accumulation de bases de données et l'importance de la mobilisation de la technologie blockchain dans la gestion de ces immenses répertoires numériques. La *data analysis*, c'est-à-dire le travail d'analyse et de filtrage des données massivement récoltées, interroge davantage chaque jour sur ses usages pervers, voire antidémocratiques, d'où la nécessité d'une transparence accrue dans ces opérations.

L'Internet des objets croise en effet la route de la technologie blockchain en accompagnant techniquement les ambitions des contrats intelligents : ouverture et fermeture d'une serrure de porte ou de voiture, lancement d'un programme d'une machine à laver, lancement d'un programme d'enregistrement de vidéos, etc. L'objet remplace ainsi l'être humain dans la négociation transactionnelle, ce qui accélère la rapidité des échanges mais souligne aussi les nouvelles problématiques juridiques d'engagement contractuel de ces nouveaux contrats

numériques. Une plateforme comme Slock.it met donc en œuvre l'Internet des objets.

En 2015, deux géants industriels, IBM et Samsung, se sont prêtés au jeu en lançant *Autonomous Decentralized Peer-to-Peer Telemetry* (Adept), une série d'équipements connectés inscrits dans le prolongement des récents développements de l'Internet des objets. Cette gamme de produits sert désormais de base de données commune à des milliards d'équipements connectés répartis dans le monde entier, à laquelle des plateformes comme BitTorrent, Telehash ou encore la blockchain Ethereum permettent d'accéder. Pour le journaliste Erik Haehnsen, c'est l'émergence d'une nouvelle « démocratie des équipements ».

Christian Comtat, directeur de l'Internet des objets chez IBM France, voit dans cette décentralisation de l'intelligence domotique la première étape vers les nouvelles consommations de demain : « *Prenons l'exemple d'un lave-linge. Grâce à Smart Contract, celui-ci va commander la lessive qui sera livrée automatiquement afin de ne pas être en rupture de stock. On peut imaginer d'organiser ainsi une délégation de paiement contractualisée. Le propriétaire sera, bien sûr, averti de chaque transaction. De même, selon le contenu du contrat, le lave-linge pourrait gérer sa maintenance en avertissant le réparateur de l'usure des pièces à changer.*

« *La blockchain et les contrats automatiques permettent de constituer un réseau domotique décentralisé sur lequel les différents équipements de la maison passeront des transactions afin d'orchestrer les priorités de consommation électrique dans l'objectif de réduire la consommation finale d'énergie. Tout ceci peut être réalisé sans une intelligence centralisée. Il reste à régler un certain nombre de problèmes, souligne-t-il toutefois. À commencer par les aspects juridiques des contrats automatisés et de la délégation de paiement*[39]. »

Dans son chef-d'œuvre *Ubik*, l'écrivain de science-fiction Philip K. Dick décrit un personnage qui essaye d'ouvrir la porte de son propre appartement. Échec. La porte reste obstinément fermée et exige : « *Cinq cents, s'il vous plaît.* » L'homme sort « *un couteau en acier inoxydable du tiroir à côté de l'évier* », et entreprend de démonter le verrou de sa porte. Tandis que tombe la première vis, la porte l'interpelle : « *Je vous poursuivrai en justice.* » À quoi le personnage

répond : « *je n'ai jamais été poursuivi en justice par une porte. Mais je ne pense pas que j'en mourrai.* » Il semblerait qu'aussi dans ce domaine Philip K. Dick fut visionnaire et qu'il décrit ici ce qui pourrait devenir la version inquiétante de l'Internet des objets complété par la blockchain.

Transformer l'entreprise grâce à la blockchain

En 2016, pour ne pas manquer le tournant de la blockchain, le groupe PwC a développé une plateforme d'analyse des effets de la technologie blockchain sur les stratégies entrepreneuriales, avec des propositions de solutions concrètes pour ses adhérents. Cette plateforme propose ainsi douze items de solutions, de l'éducation, à l'évaluation, en passant par la collaboration et la production industrielle, pour améliorer l'expérience d'entreprise et révolutionner les pratiques de travail. Après deux années de compilation de solutions innovantes, la plateforme est fière d'annoncer plus de 1 000 services ancrés sur la technologie blockchain.

PwC promet de répondre à quatre questions que se posent les entreprises contemporaines : Quelles sont les unités de mon entreprise susceptibles d'innover prochainement ? Où se trouvent les innovations pertinentes dans la chaîne de valeur de mon entreprise ? Comment accompagner cette innovation et développer les technologies nécessaires ? Quelle stratégie adopter pour allier cette politique d'innovation et ma stratégie entrepreneuriale ? Un véritable cahier des charges pour une révolution 2.0 des entreprises du secteur.

Le nouveau défi technologique de cette plateforme est l'inter-opérabilité des solutions techniques proposées, alors que la blockchain Bitcoin est lentement mais sûrement rattrapée par d'autres blockchains publiques et privées. Cette inquiétude technologique explique l'enthousiasme récent pour les technologies sidechains de transfert des données d'une blockchain à une autre. Plus qu'un élément de vente, cette interopérabilité des logiciels de la blockchain est donc un élément de différenciation dans le choix des produits mobilisés par les entreprises dans leur processus de transformation.

La filière FinTech, un horizon pour la blockchain

L'industrie des services financiers est la première concernée par les révolutions technologiques de la blockchain, en particulier dans la transformation des modes de travail. La blockchain transforme en effet plus que le système, elle propose au client une nouvelle expérience sans intermédiation de la banque et, pour pouvoir se mettre à niveau, les banques traditionnelles ont besoin de développer une nouvelle palette de services à proposer à leur clientèle. Selon une étude du cabinet de conseil McKinsey de 2016, 10 à 40 % des revenus actuels des banques seraient mis en péril par cette concurrence de la blockchain.

La compensation et le règlement sont les deux premières applications de la blockchain dans les FinTech (technologies financières). Selon un rapport du cabinet Santander de 2015, un gain de 20 milliards de dollars par an pourrait être réalisé au niveau mondial. La mobilisation des nouvelles technologies pourra, en effet, réduire les coûts engendrés par le système D+3, selon lequel un règlement peut être exécuté sous trois jours au maximum. En l'état, ce mécanisme commande des dépenses en matière de services client et de systèmes de compensation en cas d'ennuis techniques. L'entreprise Digital Asset Holdings de Blythe Master, une personnalité engagée du secteur, propose ainsi de réduire ces coûts avec des serveurs de données hyper-distribués, plus sécurisés parce que plus ouverts encore.

À l'identique, les activités de paiement ont connu une véritable évolution, de même que les systèmes d'identité digitale et de reconnaissance cryptographique. Les prêts de personne à personne (P2P) se sont ainsi accrus de manière extraordinaire au cours des dernières années, particulièrement dans les pays en développement, à l'initiative de plateformes portées par la technologie blockchain, telles que Abra ou Bitbond. Sur un continent comme l'Afrique, en pleine croissance démographique et économique, ces systèmes d'échange facilités sont une clé de développement durable des sociétés. Demain, dans les pays industrialisés ou dans les grands émergents, les échanges n'auront plus lieu entre les hommes mais entre les machines directement, sans l'aval de leur détenteur, ce qui nécessite donc de

créer des protocoles de reconnaissance des identités déléguées.

La digitalisation des actifs

La transformation de la finance sous l'influence de la blockchain passe aussi par une évolution des systèmes de gestion d'actifs. Selon un rapport de Capgemini et de la Royal Bank of Canada de 2014, la moitié des multimillionnaires au monde utilisent aujourd'hui des outils numériques pour gérer leur fortune, ce qui impose une évolution des milieux financiers. Cette tendance s'inscrit dans un mouvement de fond, touchant de manière plus large l'ensemble des clients de CSP+, ménages aisés ou très aisés, multi-équipés de smartphones, ordinateur portable, tablette, télévision intelligente, souhaitant être connectés en permanence. Or, jusqu'à présent, les banques privées répondaient peu ou mal à cette demande d'une offre financière digitale.

« *La gestion d'actifs a déjà connu une grande transformation avec les techniques quantitatives dans les années 1990*, souligne Jean-François Boulier, président du directoire d'Aviva Investors France, *puis l'application des produits dérivés dans les années 2000, et s'il est exact que le big data va nous apprendre davantage sur les comportements des consommateurs, il ne va pas pour autant révolutionner les processus actuels*[40]. »

Les gains importants de la FinTech relèvent, pour l'essentiel, de la transformation de la gamme des clients. Avec la révolution numérique, un public de masse s'est passionné pour la finance « facilitée », engageant néanmoins des sommes moins importantes que les clients habituels. Cet afflux soudain de clients assure une rente nouvelle pour les milieux financiers internationaux, alors que les coûts de suivi restent, eux, limités. L'optimisation des données et le développement des robots numériques (*robo-advisors*) permettent en effet un traitement efficace et rapide des demandes, sans intervention humaine.

Ces plateformes de conseil financier automatisé connaissent une sorte d'âge d'or, car elles proposent simplement de répéter des décisions d'investissement réussies, opérées par un panel de gestionnaires talentueux. Basées sur des algorithmes mathématiques relativement simples, ces machines fonctionnent donc seules,

apprenant de leur observation des gestionnaires humains, à l'image de l'ordinateur Joshua dans *Wargames* (1983). En France, de jeunes pousses se sont implantées dans ce secteur fructueux, tels Fundshop ou Marie Quantier, avec des niveaux de frais très faibles et une transparence accrue.

La titrisation blockchain

La titrisation, c'est-à-dire la technique de transfert d'actifs financiers sous forme de titres financiers, est un autre de ces processus financiers en mutation sous l'effet de l'émergence des technologies blockchain. Depuis la crise économique et financière de 2008, elle connaît un ralentissement de son activité, par manque de confiance des acteurs du marché. En dépit de la mise en œuvre de nombreuses autorités de régulation, elle ne reprend que lentement son activité et la mobilisation de la technologie blockchain apparaît comme un facteur de sa relance à court terme.

La blockchain ouvre en effet le champ à une titrisation élargie, puisque tout un chacun pourra désormais émettre des titres de propriété échangeables dans n'importe quel domaine de biens, de l'art à la restauration. Un particulier pourra donc, à terme, titriser un tableau d'artiste, sur la base d'un contrat intelligent permettant l'accès du détenteur de tout ou partie des titres à l'œuvre physique soit dans un lieu public, par exemple un musée, soit dans un lieu privé auquel le contrat lui donnera accès par une serrure débloquée. Le spécialiste Artprice a ainsi annoncé avoir engagé des démarches pour développer une blockchain à moyen terme.

Les avantages de cette titrisation blockchain sont doubles : pour l'individu, elle assure la permanence, l'intégrité et l'inter-opérabilité de ses actifs et de sa réputation, en plus de lui permettre de gagner la valeur de biens aujourd'hui en dehors du marché de la titrisation ; pour la superstructure de titrisation, elle garantit la transparence et la résilience des mécanismes de distribution de valeur et de gouvernance au sein de son organisation. En outre, la blockchain enregistre l'historique des transactions de titrisation, mais assure aussi la validité de ses opérations, « minées » par des millions d'ordinateurs, tous

connectés au réseau.

La réussite de cette révolution reposera, d'abord, sur le fonctionnement des initiatives de financement participatif (*crowdfunding*), qui permettent dès aujourd'hui de participer financièrement à un projet par l'entremise de plateformes numériques. Popularisées par des initiatives célèbres dans les années 1990, comme le groupe de rock Marillion (1997) ou la communauté française Tela Botanica (1999) et par le développement de plateformes dédiées comme My Major Company (2007), ces démarches sont de véritables structures de construction de la confiance. La blockchain a, elle aussi, su générer d'importants investissements sur le fondement de ces activités, ce qui prouve sa transformation en une technologie stable et reconnue. Philippe Dardier, qui dirige Alternativa, la première bourse alternative pour les PME, voit dans la blockchain des possibilités étendues pour pouvoir faciliter le financement des petites entreprises en utilisant une digitalisation des titres qui deviendraient cessibles dans des nouvelles bourses d'échanges plus simples à contrôler et donc à sécuriser.

Selon Chris Skinner, auteur de *FinTech by the Numbers* (2016), sur 30 milliards de dollars investis dans le secteur des FinTech en 2015, 30 % ont été consacrés à améliorer les solutions de paiement, 25 % à développer les plateformes de financement participatif, et 20 % aux prêts P2P. La génération Y, née entre le début des années 1980 et le début des années 2000, est la première touchée par cet engouement dans la métamorphose du secteur des activités financières. Il génère aussi une véritable concertation au sein des entreprises spécialisées, réunies par exemple au sein de France Fintech, une structure réunissant plus de 60 acteurs français. Il attire enfin l'attention des pouvoirs publics, ainsi la Banque de France, présente à l'appel du forum FinTech R:Evolution, organisé en mai 2016 à Paris, qui a réuni plus de 500 acteurs du monde entier.

Dans l'actualité récente, en France, en vertu de la Loi relative à la transition énergétique pour la croissance verte (LTCV) d'août 2015 et depuis le 1er juillet 2016, les sociétés locales de développement de projets d'énergie renouvelable peuvent ainsi appeler à la participation financière des collectivités territoriales et/ou des particuliers dans le financement des installations. Cet encadrement juridique du

financement participatif écologique fait suite à l'émergence de nombreuses plateformes dédiées comme Lumo, Enerfip ou GreenChannel et la technologie blockchain pourrait assurer sécurité et transparence à ces initiatives intéressantes.

Blockchain et assurances, un étrange mariage

À l'identique de l'adaptation du secteur bancaire, le secteur de l'assurance cherche à épouser les nouvelles technologies numériques et les outils de la blockchain. Le développement d'un système assurantiel sans intermédiaire, sous la forme de contrat intelligent, fait en effet directement concurrence aux entreprises historiques de ce secteur. L'assurance pair-à-pair est, en fait, déjà une réalité sur le Net, avec des structures comme Friendsurance (en Allemagne) ou Inspeer (en France), et les acteurs historiques injectent massivement de l'argent dans la technologie blockchain pour assurer l'adaptation de leur système. En 2016, Axa a ainsi investi 55 millions de dollars dans la start-up Blockstream pour développer son offre « blockchain » d'assurances.

La révolution numérique dans l'industrie de l'assurance pose des questions encore plus profondes. Le big data permet en effet de collecter massivement des données sur les assurés et sur les risques. Par exemple, il permet de cibler avec davantage de précision les personnes à risque élevé et/ou les activités à risque élevé. Le développement de l'Internet des objets accroît encore cette dynamique de concentration de l'information et de définition de profils types des assurés. En conséquence, face à la multiplication des offres et dans une logique de baisse concurrentielle des prix, les entreprises historiques du secteur des assurances sont tentées de s'appuyer sur l'analyse des données pour proposer des offres tarifaires modulées.

En France, cette mini-révolution inquiète beaucoup les assureurs historiques. Elle conduit lentement à une personnalisation du coût du risque, alors que le modèle d'assurance tricolore répartissait auparavant ce coût sur l'ensemble des assurés. En d'autres termes, alors qu'hier tous les assurés payaient une cotisation égale et que l'assureur couvrait

les quelques assurés engagés dans un accident, demain l'assureur pourrait faire payer plus à une personne dite à risque et moins à une personne sans risque. Cette évaluation des profils serait basée sur l'analyse de données collectées comme les accidents passés, votre consommation, votre vitesse de conduite, etc. Dans un système où l'assurance est obligatoire, cette évolution de la gamme des prix assurantiels peut conduire à placer des personnes à bas revenu dans l'incapacité de souscrire à une assurance.

En outre, l'émergence d'une offre d'assurances de pair-à-pair pose des questions juridiques. Dans ce nouveau modèle collaboratif, le pouvoir décisionnel est transmis aux assurés, par exemple dans la répartition du capital non utilisé en fin d'année, au choix redistribué entre les assurés ou « stocké » en vue de frais prévisionnels dans les années à venir. La non-territorialisation de ces systèmes assurantiels pair-à-pair pose la question des juridictions devant lesquels mener un recours.

La blockchain en politique, les couleurs primaires

Les ambitions démocratiques et politiques de la blockchain, à travers son rêve de transparence, devaient forcément nous amener à réfléchir aux applications politiques de cette technologie. Dans une société en crise permanente, marquée par une forte remise en cause des institutions politiques et par une défiance durable à l'égard de la classe politique, le retour au pouvoir individuel a soulevé une vague de questionnements. Les origines culturelles et historiques de la blockchain ont, en outre, participé à lier la technologie blockchain et l'appel à un renouveau du système politique.

Pour François Dorléans, fondateur de la start-up française Startumn, la blockchain est ainsi une technologie idéale pour accompagner le développement du vote sécurisé : « *Un vote est une transaction critique : celle-ci doit être exécutée rapidement par le réseau. Pour ce faire, on ajoute des frais de transaction pour rémunérer les mineurs (à l'origine de la sécurisation du vote). Ceux-ci commencent par traiter les transactions qui comportent le plus de frais, puis traitent par ordre*

décroissant les transactions suivantes. Si le réseau est saturé au moment où l'on envoie un vote, les mineurs vont avoir tendance à reporter ce vote vers les blocs suivants. En conséquence, l'idée est de mettre des frais de transaction de l'ordre de 10 centimes d'euro (selon le cours du bitcoin) pour être à peu près sûr que le réseau va traiter le vote.

« *L'administrateur du vote (qui peut être une association, ou une entreprise organisant une assemblée générale avec ses actionnaires, voire un État) place sur un protocole spécifique […] autant de jetons qu'il y a de suffrages exprimés. Il transmet ces jetons à l'ensemble des votants, qui ont accès à un portefeuille électronique (un wallet) pour contenir ces jetons. De leur côté, les candidats possèdent une urne numérique – concrètement, un wallet, avec une adresse publique. Quand le votant émet son jeton de vote, il transfère à la fois les bitcoins qui comportent les frais de transaction, et la métadonnée qui représente le vote. À l'issue du vote, le candidat gagnant est celui qui a reçu le plus de jetons.*

« *Pour parachever cette architecture, une carte électorale digitale (concrètement, une clé cryptographique) est nécessaire pour s'assurer que celui qui se présente à son wallet est bien le propriétaire de ce wallet. Une partie de la clé est publique, l'autre privée : on peut dresser le parallèle dans le monde bancaire traditionnel avec le RIB, que l'on peut communiquer à n'importe qui, et le code PIN, qui ne doit pas être partagé*[41]. »

Cette solution du vote électronique permettrait, sans aucun doute, de lutter contre l'abstention massive de nos concitoyens, en facilitant le processus du vote (suppression des déplacements et vote en quelques clics) et en diminuant son coût de mise en place (quelques centimes contre une moyenne française de 5 euros). Cette évaluation financière doit toutefois être contrebalancée par trois considérations d'ordre général : le coût des transactions varie en fonction du cours de la monnaie électronique, la vitesse des transactions est limitée par l'architecture de la blockchain, variable d'une blockchain à l'autre, et la carte électorale digitale est susceptible d'être victime d'un piratage.

Quant à l'hypothèse de stocker la clé cryptographique de la carte électorale digitale sur un support physique, par exemple une lettre adressée à chaque électeur (ainsi que le protocole Remotegrity le

propose), cette démarche suppose des coûts postaux supplémentaires d'envoi des informations aux électeurs. Elle assurerait néanmoins une protection adéquate contre les possibles corruptions de vote. En tout cas, cette démarche a l'avantage d'interroger nos systèmes de vote et de faire réfléchir aux possibilités techniques d'une nouvelle forme d'élection. Ajoutez à cela qu'une telle astuce numérique permettrait de mieux préserver notre environnement en diminuant la production de papier et vous aurez toutes les raisons d'appeler de tous vos vœux à cette révolution politique.

Les limites du vote en ligne

Ces promesses démocratiques du vote en ligne ne laissent pas tous les observateurs unanimement enthousiastes. Barbara Simons, ancienne présidente de l'Association for Computing Machinery (ACM) et membre de la Commission nationale sur le vote par Internet du président Bill Clinton, le vote en ligne est confronté à deux défis de taille : sa sécurité, en pratique son incapacité à être reconnu comme entièrement sûr, et sa contrôlabilité, en l'espèce la difficulté à « recompter les votes » alors que les dernières élections présidentielles américaines ont donné lieu à des procédures de remise en cause des votes de certains États. « *L'envoi de votre vote via votre téléphone ou via votre ordinateur de bureau sur le serveur, ou en sélectionnant les options d'un système de vote automatisé de votre téléphone serait, en effet, bien plus simple pour les électeurs*, reconnaît-elle volontiers. *Mais ce système ne garantit pas l'enregistrement correct de votre vote ou même un enregistrement quelconque. En tant qu'électeur, nous n'avons pas accès au serveur ou au réseau sur lequel notre vote est envoyé. Et lorsqu'il faut recompter les votes, aucune trace papier n'est alors possible* » explique un article de Cryptos.net[42].

La blockchain offre pourtant la possibilité de résoudre cette problématique du contrôle des votes, grâce à une base de données transparente. Le logiciel Scantegrity (développé en 2008) propose ainsi de vérifier la validité d'un vote grâce à un système de sécurité basé sur le contrôle des votes enregistrés. Dès mai 2008, David Chaum, un de ses inventeurs et une personnalité déjà rencontrée, en a d'ailleurs fait

l'éloge dans un papier consacré aux nouvelles formes du vote numérique, appelant à sa mise en pratique rapide. Lors de l'opération de recomptage, le votant dispose d'un code de confirmation pour attester que son vote n'a pas été modifié au cours de la procédure électorale.

En 2009, lors des élections municipales de Takoma Park, aux États-Unis, dans le Maryland, cette solution a été mobilisée pour la première fois afin de corroborer les premiers résultats d'un vote local. L'utilisation de Scantegrity a été un tel succès qu'elle a été de nouveau mobilisée en 2011. Deux autres logiciels, Prêt à Voter et Punchscan, sont venus compléter les avancées de Scantegrity, intégrant de nouvelles problématiques techniques, comme la nécessité de respecter l'ordre des candidats dans la présentation électronique des listes, afin de ne pas créer de biais de « vote pour le premier candidat », ou encore le système d'échantillon aléatoire de vérification de la validité des votes.

Un outil au service de la démocratie liquide

Le nouveau souffle démocratique porté par la révolution blockchain a redonné vie au projet de démocratie liquide (*liquid democracy*), porté par la Commune de Paris, à la fin du XIX^{e} siècle. En effet, dans une démocratie directe, le citoyen vote directement pour choisir le décideur, comme à l'occasion des élections présidentielles françaises. Dans une démocratie représentative, le citoyen vote pour un représentant, lequel vote ensuite pour élire le décideur – c'est le cas des élections présidentielles américaines. Dans une démocratie liquide, le citoyen peut faire le choix soit de voter directement pour le décideur, soit de déléguer son autorité démocratique à un représentant, chargé d'élire le décideur.

Au niveau des représentants, un pouvoir de re-délégation permet d'élire un super-représentant, considéré comme un expert par ses pairs. Le décideur est donc élu par la combinaison des votes des citoyens électeurs, des représentants électeurs et des super-représentants électeurs. Une variante technique est l'élection de super-représentants du fait du vote des citoyens électeurs, ce qui ramène à l'assemblée des citoyens la décision de confier un pouvoir suprême à un super-

représentant. La fluidité de ce système politique et sa capacité à adopter des règles politiques mouvantes expliquent son nom de démocratie liquide.

Dans la démocratie liquide, deux éléments distinguent clairement le système politique de celui de la démocratie représentative : la durée du mandat et son cadre. Chaque élection d'un représentant ou d'un super-représentant est ainsi unique en son genre parce qu'elle fixe des règles uniques. La durée du mandat est facultative puisque les électeurs peuvent, à tout moment, rappeler le représentant ou le décideur et entamer un nouveau processus d'élection. Quant à l'étendue de ses pouvoirs, elle est définie lors du vote, avec un champ d'action variable d'une élection à l'autre, y compris pour les mêmes fonctions.

Pour Connor O'Day, spécialiste de la question, il ne fait aucun doute que la démocratie liquide peut s'appuyer sur la technologie blockchain pour être appliquée dans les régimes politiques modernes : « *Ethereum a la capacité d'être la colonne vertébrale de ce protocole décentralisé et de confiance porté par Internet. Historiquement, la démocratie liquide n'a pas réussi à se développer à une grande échelle, car il est très dur de s'assurer qu'une seule personne ne vote pas plusieurs fois* [pour le décideur et, en même temps, pour le représentant censé porter sa voix]. *C'est ce que l'on appelle une attaque Sybil, dans laquelle un utilisateur peut créer plusieurs identités pseudonymiques, qui se font au détriment de la création d'un système politique honnête. Imaginez si la démocratie liquide pouvait s'appuyer sur Facebook, rendant plus complexe la création de faux comptes qui faussent le système*.

« *Sur Ethereum, cependant, certains des meilleurs programmeurs travaillent aujourd'hui à créer un système d'identité cryptographique et de réputation hypersécurisé. Tout en protégeant les informations personnelles des utilisateurs et sans violer leur intimité. Il est donc possible de créer un protocole de vote décentralisé qui peut résister à des attaques Sybil, en requérant simplement des vérifications basiques sur la réputation des utilisateurs tout en protégeant leur anonymat*[43]. »

Dans cet esprit, une initiative d'identité numérique unique, telle que celle proposée par Onename, acquiert un sens nouveau. Sur la blockchain Ethereum, l'apparition du logiciel ConsenSys vise à nourrir ces rêves de démocratie renouvelée, en intégrant des données aussi techniques que des mécanismes de gouvernance avancée, d'allocation

de budget, de comptabilité transparente, de vote des actionnaires, etc. Cette structure de gouvernance est, par exemple, celle appliquée au modèle de The DAO, dans lequel l'absence de consensus mène à la partition de la société en deux groupes distincts.

Plusieurs exemples pratiques montrent la fonctionnalité de la démocratie liquide, appuyée sur l'usage de la technologie blockchain. Le logiciel Adhocracy permet ainsi de mettre en avant des débats sur des thèmes précis, d'organiser un vote sur un ensemble de proposition, ou encore de mettre en œuvre un classement des propositions de la plus appréciée à la moins appréciée, toujours dans cette dynamique de la recherche de la solution politique la plus consensuelle. À l'identique, le logiciel LiquidFeedback, programmé par des membres du Parti pirate allemand et rendu public en 2009, sert aux conventions nationales de Partis pirates en Allemagne, en Autriche, en Suisse, en Italie, ou même au Brésil.

Cette application de démocratie liquide permet en effet de créer des groupes de dialogue au sein d'une plateforme numérique, de mettre en place des votes autour des propositions émergentes et de déléguer son vote à une tierce personne, un représentant, ou à un expert technique, une sorte de super-représentant. Cette délégation du vote ne s'inscrit pas dans la durée et peut être reprise au cours du débat, en cas de contradiction avec le représentant/super-représentant, ou après le débat sur un autre vote. Pour adhérer, le participant doit simplement créer un pseudonyme et s'inscrire aux groupes de discussions. Dès lors qu'une proposition atteint au moins 10 % d'intérêt de la part des membres du réseau, elle est mise au vote avec une visée, au choix, informative, suggestive, directive ou même décisionnelle.

Revenir à une démocratie vivante

Cette transformation politique portée par la révolution blockchain nous ramène à l'échelon local ou territorial. Contre les super-structures institutionnelles, politiques, économiques et sociales désincarnées, nous avons besoin de retrouver le sens humain des choses. Cette recherche de la proximité s'applique d'ailleurs à l'ensemble des champs de la vie contemporaine : achats locaux pour des logiques de traçabilité

des produits, démocratie locale et numérique pour des raisons d'impact concret des élus sur la vie quotidienne, etc. Nous éprouvons le besoin de voir pour croire, de pouvoir toucher et débattre, voire critiquer, pour accepter notre délégation de souveraineté à un représentant élu.

Alors que nous nous engageons vers davantage d'individualisme et de repli sur soi, le numérique, les réseaux sociaux et la blockchain nous invitent à communiquer davantage. La technologie blockchain, contrairement à des réseaux sociaux comme Facebook ou Twitter, parvient à recréer du lien politique parce qu'elle demande d'adhérer à un ensemble de valeurs. En souscrivant à l'adoption d'une monnaie commune, crypto-monnaie ou jeton, l'utilisateur de la blockchain rejoint une communauté numérique. Derrière son anonymat, il construit une personnalité avec des prises de position publiques et des relations sociales.

Elle nous fait aussi échanger avec des inconnus, confronter nos idées, nouer des alliances de vues et lancer des entreprises communes, alors que les réseaux sociaux « traditionnels » ont plutôt tendance à recréer notre confort personnel avec une communauté d'amis connus, dont nous partageons déjà les états d'esprit. Bref, la blockchain reconstruit l'espace public théorisé par Jürgen Habermas. Elle forme un réseau d'échanges d'avis et d'opinions, un jardin commun cultivé par tous, une méga-structure sociale et politique dématérialisée, que la démocratie liquide aide à se réaliser en luttant contre les dictatures de pensée ou la coercition.

Des plateformes comme DemocracyOS, PublicVote ou encore V-Initiative soutiennent ainsi l'émergence de nouveaux espaces publics numériques, où le citoyen retrouve le goût de commenter et débattre. Pour Don Tapscott, auteur de *The Digital Economy* (1994) et de *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business and the World* (2016), la blockchain transforme radicalement la démocratie : « *Aujourd'hui, les gouvernements utilisent les taxes sur les entreprises, les individus, les brevets et ainsi de suite pour fonctionner. Tout cela peut changer. D'abord, nous pouvons avoir davantage de transparence dans un sens radical du terme parce qu'un coup de projecteur* [sur notre système politique] *sera le meilleur des désinfectants. Ensuite, nous pouvons ouvrir davantage nos gouvernements, à travers les politiques de partage des données. Ce*

n'est pas vraiment de la transparence, qui parle plutôt de choisir avec qui partager les données pertinentes. Ces politiques visent à libérer des vrais atouts digitaux.

« *En créant une plateforme blockchain, nos gouvernements pourront mettre en œuvre une organisation de la société dans laquelle les entreprises, les organisations de la société civile, les ONG, les universitaires, les fondations, les agences gouvernementales et chacun des citoyens pourront utiliser ces données pour s'auto-organiser et créer ce que nous avions l'habitude d'appeler des services publics. Enfin, la troisième possibilité de changement tient dans la relation entre les citoyens et leurs gouvernements*.

« *Nous avons l'opportunité de créer un gouvernement par le peuple, pour le peuple – et plus pour l'argent ou pour les investissements massifs. Les dirigeants pourraient être élus à l'appui d'un contrat intelligent qui spécifie ce qu'ils feront quand ils seront élus, et qui gèlera automatiquement leur salaire s'ils ne font pas ce que les électeurs ont demandé mais ce que leurs bailleurs souhaitent. Plusieurs gouvernements ont dépensé des milliards et des milliards de dollars à essayer de comprendre cela. Le vote électronique basé sur un serveur traditionnel ne fonctionnera pas, parce que les citoyens n'auront pas confiance. Mais avec la blockchain, les citoyens pourront confirmer que leur vote a bien été pris en compte.* »

L'innovation démocratique en pratique

Sur le modèle des logiciels de la technologie blockchain, BitCongress entend développer ces nouvelles formes démocratiques, y compris le principe de démocratie liquide, dans d'autres lieux que l'espace public, par exemple au sein des universités. En 2016, cette start-up s'est ainsi fait connaître comme porte-parole du mouvement de gouvernance 2.0, en invitant l'Internet des objets à accroître la participation démocratique. En pratique, l'application permettait de participer à des votes ou des décisions publiques avec des outils du quotidien comme un téléphone, une tablette numérique ou encore une télécommande de télévision.

BitCongress édite ainsi des jetons « Vote » à chaque fois qu'un processus décisionnel est engagé et en expédie chez chacun de ses

membres, en s'assurant, grâce à la localisation géographique des objets connectés, que la lutte contre les opérations de multi-comptes ait bien abouti. Le processus de vote est ainsi « payé » par l'envoi du jeton « Vote » au réseau et les données d'identification des utilisateurs restent confidentielles, autant que faire se peut. L'entreprise applique aujourd'hui ces propositions démocratiques au système politique, mais aussi à d'autres enceintes décisionnelles comme les entreprises ou les universités.

En 2016, plusieurs initiatives se sont créées pour offrir un service permettant de « parier » sur le résultat mesurable d'un événement, sans passer par une autorité centrale, comme un organisme de pari. Ces « marchés de prédiction » (*wisdom markets*) utilisent la blockchain pour décentraliser ces opérations et les rendre dignes de confiance. La plateforme Augur s'est illustrée dans ce domaine mais récemment a également démarré Gnosis, établi sur la blockchain Ethereum. La vision complète serait que Gnosis verse une sorte de salaire de conseil à ceux des utilisateurs qui savent le mieux prédire les résultats d'événements économiques ou politiques. Aujourd'hui, ils constituent une innovation majeure face aux études d'opinion plus conventionnelles.

Dit autrement, la révolution blockchain en vue de l'établissement d'une démocratie liquide appelle à la mise en œuvre d'organisations autonomes et décentralisées et de business models acentraux. Se coordonner à plusieurs, de manière consensuelle, sans autorité centrale, ce sont les trois étapes de l'émancipation individuelle promise par la blockchain. Ce que cette technologie consacre, c'est aussi l'immuabilité et l'irrévocabilité des décisions, enregistrées dans les blocs numériques, une sorte d'histoire consacrée des échanges, insusceptible d'être modifiée par le truchement d'un être humain.

La blockchain, un chantier de pionniers civiques

Parmi les très nombreux cas d'usage de la blockchain, de la crypto-monnaie à la finance rénovée, de la gouvernance d'hier aux nouvelles formes d'organisation de la société d'aujourd'hui et de demain, l'idée forte de cette transformation de nos modes de vie et de comportement

est dans une révolution radicale de l'esprit. Les programmateurs de la blockchain ne sont pas seulement de simples informaticiens, ingénieurs ou techniciens, ce sont de véritables révolutionnaires, hérauts d'une nouvelle forme de vie commune.

En septembre 2016, à l'occasion du lancement du site Make.org, j'ai eu l'occasion d'avoir une discussion à ce propos avec son fondateur, Axel Dauchez, ancien patron de Publicis France. Cet entrepreneur cherchait à comprendre comment la blockchain pourrait rendre son infrastructure moins corruptive et plus transparente. Nous avons eu des échanges passionnants sur les nouveaux outils numériques à disposition et leur pertinence dans la recherche de l'irréprochabilité de la politique. Le lien entre décideurs et citoyens peut ainsi être refondé par davantage de décentralisation du pouvoir décisionnel.

Le mouvement 577 pour la France de Jean-Christophe Fromantin cherche à résoudre cette équation civique en donnant la chance à chaque citoyen de se présenter et d'être élu aux élections législatives. Pas d'investitures partisanes, mais une liste d'étapes à franchir (comme les étapes d'un jeu vidéo) : mise en place d'équipes, réunion de souscripteurs, etc. Le premier candidat à remplir tous les objectifs préalablement fixés est investi par le mouvement. Ce système brillant est l'un des premiers à transposer l'acentralité de la blockchain à la vie politique.

Tous ces innovateurs, coiffés d'un bonnet phrygien numérique, veulent inventer une nouvelle façon de se comporter en société. Ils lèvent le voile sur le mystère de certains secteurs d'activité. Le politique sera désormais tenu par sa parole, à l'appui d'un registre d'engagements de sa campagne. L'électeur pourra, lui, intervenir davantage dans le débat public grâce à des outils d'intervention numérique et à un système de « reprise en main » de son vote. Le banquier sera, enfin, forcé de tenir sa comptabilité publique et transparente, afin que l'utilisation de l'épargne soit orientée vers des entreprises à haut rendement financier mais aussi politique et social.

Ces applications aux relations sociales des êtres humains se trouvent parfaitement exprimées dans la transformation des réseaux sociaux. Steemit, par exemple, est un réseau social décentralisé, qui n'est pas géré par une société (comme Facebook ou Google+) mais par un collectif d'utilisateurs. Cette communauté gérante a pour principal

objectif que la création de valeur soit également partagée entre tous les membres de la communauté numérique. Il s'agit du premier réseau social décentralisé et autonome. C'est un espoir formidable pour tous ceux qui se questionnent sur la façon dont les géants du numérique prennent possession de nos données personnelles et les exploitent.

La communauté blockchain apparaît ainsi comme l'embryon d'un nouveau vivre-ensemble. La série américaine *Halt and Catch Fire* (2014-2016), consacrée à l'histoire des premiers ordinateurs personnels, cherche à retranscrire cet état d'esprit, en peignant les dessous de la communauté Mutiny, une des premières à se former physiquement et numériquement. Les blockchains proposent finalement un mode de vie sociale alternatif aux sociétés contemporaines et remettent en question le postulat de Francis Fukuyama, selon lequel la fin de la guerre froide aurait signé « la fin de l'histoire » et l'adoption d'un modèle culturel unique.

En 1989, cet économiste et philosophe américain avait en effet développé, dans *La Fin de l'histoire et le dernier homme* (*The End of History and the Last Man*), la théorie d'une fin de l'histoire humaine, avec la conclusion de la guerre froide. La victoire de la démocratie libérale américaine sur le communisme soviétique marquait la fin d'un combat des idéologies et, de fait, un arrêt de la progression de l'histoire humaine. Pour Fukuyama, la fin de l'histoire était aussi l'ouverture d'un nouveau chapitre, celui de la fin de l'homme, demain transformé sous l'influence des biotechnologies et de la machine humaine, bref du transhumanisme. La blockchain semble montrer que le modèle dominant au début des années 1990 n'a plus lieu de régner et que l'humanité tend à l'avènement d'un nouveau modèle économique, social et culturel.

Au fond, ce que la blockchain propose à travers ses nombreux usages, c'est de redistribuer les choses : redistribuer les données pour davantage de transparence dans les systèmes de gouvernance, redistribuer les outils d'intervention dans la sphère publique pour davantage de démocratie, redistribuer le contrôle sur les décisions pour davantage de consensus, etc. Ce retour au consensus et au commun sait séduire les entreprises, car il personnalise les services à l'aide des données collectées et offre donc des expériences uniques à chacun des utilisateurs. Les outils digitaux n'ont pas fini de changer notre quotidien

et il semble que tout le monde veuille désormais embarquer à bord de ce navire futuriste.

La blockchain et les grandes transitions

« Vous ne pouvez pas arrêter des choses comme le bitcoin. Elles vont se propager partout et le monde devra forcément s'y ajuster. Nos gouvernements devront s'y ajuster. »

JOHN MCAFEE, 2013

Avec la technologie blockchain, nous laissons derrière nous un monde centralisé et jacobin. Le mode de fonctionnement de ce monde institutionnel est la bureaucratie : une organisation du travail dont l'action est encadrée, motivée par la loi. La dérive de la bureaucratie, qu'elle soit dans les institutions de la finance, de la démocratie, est devenue l'objet d'un rejet contemporain. Mais nous pouvons changer les choses, en allégeant nos institutions et leur bureaucratie, par des algorithmes créateurs de confiance…

Penser le monde autrement et interroger cette logique des relations humaines, c'est un peu réaliser une nouvelle révolution copernicienne. C'est abandonner une vision hiérarchique de haut en bas (*top down*) pour épouser les formes d'une vision renversée, de bas en haut (*bottom up*). C'est encore se demander si l'univers tourne toujours autour de la bureaucratie ou s'il existe de nouveaux centres de gravité pour nos sociétés. Et si oui, lesquels ? Aujourd'hui, notre culture, nos comportements et nos habitudes, mais aussi nos systèmes d'éducation célèbrent cette centralité, ce rapport à l'autorité suprême, construit pas à pas depuis plusieurs siècles, et nos logiciels de fonctionnement ont donc beaucoup de peine à évoluer. Développer des solutions, c'est donc relever de nouveaux défis. C'est se débarrasser des oripeaux de l'histoire, d'une sorte d'obscurantisme involontairement accepté, pour

s'engager dans un nouveau chemin.

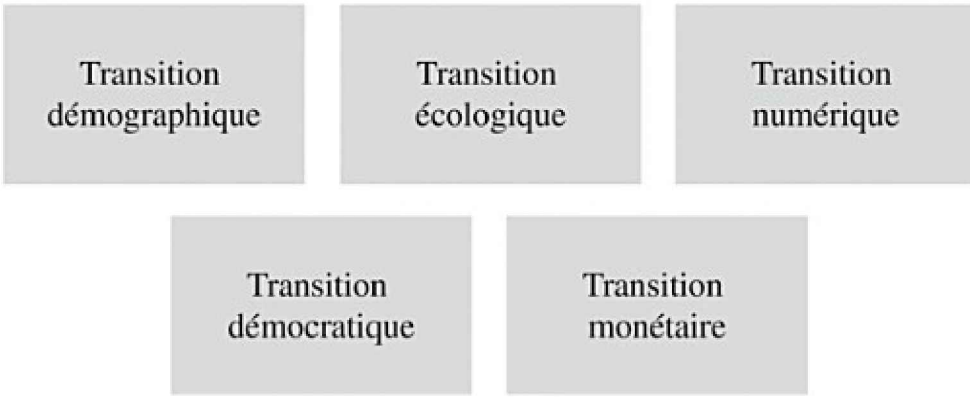
Avec la fin de la guerre froide et la première décennie du XXIe siècle, les communautés humaines ont commencé à développer de nouvelles formes de gouvernance, dans lesquelles l'autogestion est un mode de vie et de développement. Elles ont renversé les dernières dictatures pour consacrer le citoyen roi, cet individu, centre de toutes les attentions économiques et sociales. L'exploitation déraisonnée des ressources naturelles et le réchauffement climatique ont en effet posé les limites d'un modèle capitaliste, poussé à outrance, et les récents développements diplomatiques autour de cette question de l'avenir de notre planète invitent à mettre en œuvre de nouvelles formes de partage. Le nouveau siècle sera donc celui des communs, des connaissances et des richesses partagées.

L'émergence d'une économie du partage, et auparavant le Web 2.0, cet Internet collaboratif, outil partagé, enrichi de la connaissance de chacun, en est le fier témoignage. Le développement effréné des encyclopédies en ligne, comme Wikipédia, marque le commencement d'une nouvelle relation de l'homme à l'humanité, dans lequel chacun participe à la construction d'un héritage commun des savoirs et des pratiques. L'émergence de forums mondiaux de discussion, comme 4chan, ou de communautés numériques, comme les cypherpunks ou les Anonymous, célèbre aussi la naissance d'une nouvelle forme d'identité, numérique et transnationale, humaine plus que civilisationnelle. Notre monde entre ainsi progressivement dans une nouvelle ère.

Cette révolution de la blockchain s'inscrit dans une dynamique d'ubérisation de nos sociétés. Apparue en 2014, sous la plume de Maurice Lévy, patron de Publicis, l'« ubérisation » désigne le processus de transformation d'un secteur économique sous l'influence des nouvelles technologies, mais aussi l'émergence d'une économie pair-à-pair et de services à la demande. Des monuments historiques du siècle passé se sont ainsi effondrés en quelques années, incapables de s'adapter à ces ruptures technologiques : le photographe Kodak, les encyclopédies Larousse, etc. L'usage massif du mobile ou des plateformes de services à la demande accélère cette tendance au tout numérique et invite à se doter de tous les outils à disposition, notamment la technologie blockchain, pour préserver notre économie et

lui faire épouser les contours de l'économie collaborative et de l'innovation numérique.

Figure 2 Les grandes transitions de notre société



Machine créatrice de confiance et accélératrice des liens humains, la technologie blockchain est un catalyseur de cette révolution des mœurs. Elle célèbre l'individu et l'acentralité, elle repose la transparence et la confiance comme règles fondamentales des échanges humains, bref elle remet l'homme au centre des préoccupations humaines, ainsi que le mouvement humaniste l'avait fait aux XIV^{e} et XV^{e} siècles. En même temps, elle remplace aussi l'intermédiation d'un tiers humain par le seul usage des mathématiques. Elle participe donc à l'affirmation du « second âge de la machine », prophétisé par Erik Brynjolfsson, et elle invite nos outils numériques à communiquer entre eux pour mieux satisfaire nos désirs. Elle pose, finalement, les bases d'un nouvel âge de la robotique, consacrée dans son rôle dans les sociétés humaines.

À la recherche de la confiance perdue

La quête de la technologie blockchain ne repose pas, au fond, pas sur la création d'une nouvelle forme de confiance. Elle part plutôt à la recherche d'une confiance perdue et devenue une sorte de Graal mythique pour nos sociétés modernes. Avec l'émergence des technocraties et les récents scandales monétaires et financiers, la confiance s'est érodée. Qui voudrait, aujourd'hui, confier ses économies

à Lehman Brothers ou à Bernard Madoff ? Qui tolérerait un retour politique de Jérôme Cahuzac ? Qui saluerait l'émergence d'une société de contrôle absolu sans penser, avec inquiétude, aux dérives soulignées par George Orwell, dès le milieu des années 1940 ? Les chevaliers de la blockchain sont ainsi engagés dans une aventure épique.

Les faits nous obligent à considérer deux faces d'une même réalité : liberté et sécurité vont de pair. Il est évident qu'avec une grande liberté viennent de grandes responsabilités. Dans le même temps, il est évident que les décisions prises rapidement au nom de la sécurité peuvent vite devenir liberticides. Ces réflexions connaissent une actualité criante, dans le contexte d'état d'urgence, décrété en novembre 2015. C'est là que la blockchain peut avoir un rôle à jouer, pour instaurer une société basée sur la protection de nos données et sur leur distribution limitée et régulée

Dès les premiers travaux universitaires des années 1970 et 1980, la blockchain s'est donc inscrite dans la nécessité de ré-inspirer confiance dans un contexte global d'inquiétudes généralisées et de méfiances réciproques. La théorie des contrats intelligents de Nick Szabo s'interroge ainsi sur la capacité d'un document numérique à acquérir une valeur juridique et morale identique à celle de son équivalent papier. Les récents développements juridiques de la monnaie bitcoin ou des contrats intelligents montrent que ce champ est encore en pleine évolution et que l'acceptation et la popularisation de ces nouvelles technologies seront conditionnées par une reconnaissance légale et politique de leurs valeurs.

Le mariage de la cryptographie et de la technologie blockchain répond aux mêmes ambitions, dans la mesure où il consacre l'anonymat des utilisateurs dans une société numérique où l'information circule de manière libre, publique et rapide. Contre l'étalement de la vie privée, accéléré par le déploiement des nouvelles fonctionnalités des réseaux sociaux, la blockchain invite à davantage de prudence et de parcimonie dans la communication des informations privées. Elle assure une sorte de discrétion numérique, essentielle à certaines activités, comme les échanges financiers et bancaires, alors que le Net apparaît plutôt comme un appareil de divulgation massive, encore mal contrôlé, de l'ensemble des informations.

Le postulat de la blockchain est, pourtant, somme toute assez simple. En désintermédiant les échanges, c'est-à-dire en supprimant le recours à un tiers dans un échange, comme la banque, elle comble un trou de sécurité et limite les assomptions de confiance. Dans un échange à deux personnes, la source d'une duperie est plus facilement identifiable que dans un échange à trois ! Dès lors que ce troisième acteur n'est plus un être humain mais une organisation accueillant un ou plusieurs employés, la confiance est encore plus difficile à fonder et l'information n'a que davantage de possibilités de fuiter.

La technologie blockchain est ainsi inscrite dans la continuité des travaux économiques de la théorie des jeux de Nash. La confiance s'installe dès lors que la présence d'un tiers de confiance disparaît ; elle ne nécessite que la relation entre deux êtres humains, dotés d'une parfaite connaissance de l'ambition et de l'histoire de leur partenaire. La confiance *a priori* dans les institutions a été endommagée par les grands scandales de ce début de siècle, ce que leur médiatisation a davantage encore assuré. La confiance *a priori* dans les individus a, pour sa part, toujours de beaux jours devant elle. L'individu solitaire ne semble pas, dans son essence, avoir tendance à abuser d'un pouvoir qu'il ne détient pas forcément. Mais c'est la communauté d'individus qui sera, demain, le réceptacle de ce que sont aujourd'hui les institutions : un marqueur sociétal de confiance.

La révolution blockchain, une rébellion contre les institutions ?

Pour Nick Szabo et les autres pères fondateurs de la technologie blockchain appliquée au domaine de la monnaie, l'enjeu principal de la cryptographie est donc d'accompagner la privatisation de la monnaie. Dans la lignée des aspirations des crypto-anarchistes, cette révolution technologique a bouleversé les conceptions fondamentales de notions sociétales occidentales, comme l'identité et l'individu, la propriété ou encore le contrat. A-t-elle pour autant procédé, comme la révolution russe de 1917, à un nouveau partage de terres ? A-t-elle participé à un retour à l'humain appelé des vœux des altermondialistes ?

La monnaie a besoin d'un gage de « sérieux » pour assurer son

fonctionnement. Elle ne peut exister comme outil d'échange sans qu'elle soit appuyée sur un étalon sûr : une institution sérieuse, une valeur gardée en coffre, comme de l'argent ou de l'or, ou encore une parfaite transparence des informations sur ses actifs. La digitalisation de la monnaie offre, en effet, cette dernière possibilité : puisque la monnaie est dématérialisée, sa valeur de gage peut l'être tout autant à condition que les investissements réalisés soient relativement sûrs. Qui dit sûr dit donc observable par tous ! Elle n'a ainsi pas besoin de centralité puisque sa valeur de gage (ses actifs) est elle-même décentralisée. Ses bases de données peuvent en conséquence être décentralisées et mises en ligne publiquement.

Face à la crise financière internationale et à ses excès de corruption, les grandes institutions monétaires ont doublé ou triplé leur armée de représentants : plus de régulateurs, plus de médiateurs, plus de structures en charge d'administrer et de surveiller les principaux flux internationaux. Ces hyper-structures sont-elles le garant d'une nouvelle sûreté de la finance internationale ? À en croire les derniers sondages de l'opinion, pas du tout. Elles inspirent, tout au contraire, davantage de mépris à l'égard d'une bureaucratie sans visage et sans nom.

Saurons-nous, pour autant, briser les chaînes de la bureaucratie ? J'ai la conviction que la technologie blockchain est le moyen d'y parvenir. L'affranchissement du citoyen des institutions régulatrices semble être l'horizon de transformation de nos démocraties modernes. Cependant, nos États auront-ils la capacité de mener à terme les réformes nécessaires à l'adoption de la rupture technologique de la blockchain, la si médiatique disruption ? L'immobilisme de la situation actuelle invite à penser tout le contraire, mais la foi des informaticiens et ingénieurs en cette nouvelle technologie est inébranlable.

La blockchain peut déchaîner les forces fondamentales de nos sociétés. Elle peut nous libérer de règlements contraignants, d'usages dépassés, de relations desséchées. En organisant un nouveau partage de l'information, elle peut nourrir une liberté retrouvée, une confiance ressuscitée, bref aider à refonder un nouveau pacte social entre les hommes. Elle reposera, alors, sur le fruit d'un travail humain collectif, d'un échange renouant avec la simplicité d'une relation entre deux individus, mais peut-être aussi entre deux machines. Quel meilleur protecteur de nos libertés fondamentales que les mathématiques ? Quel

plus froid et impartial applicateur de nos règles que la machine codée pour ce seul usage ?

Vers une transformation monétaire

Nous sommes longuement revenus sur les tenants et les aboutissants de la monnaie numérique bitcoin, nouvelle valeur internationale d'échange, fondée sur la technologie blockchain. Cette monnaie 2.0 repose essentiellement sur une croyance profonde en la capacité du numérique, science appliquée des mathématiques, à restaurer la confiance de nos concitoyens dans les systèmes financiers et monétaires. Cela pose un véritable problème de base : comment imaginer que les Européens, démoralisés devant les échecs à répétition de l'euro, aux mains d'un système centralisé, s'affichent en faveur d'une monnaie décentralisée et, du moins le pensent-ils pour la plupart, mal supervisée ?

Cet exercice politique demande à consacrer l'indépendance du bitcoin. Ce que la technologie blockchain condamne, par-dessus tout, c'est le manque de transparence du microcosme technocratique. Dans l'antichambre du pouvoir, pas de nom, pas de visage, seulement des hommes et des femmes en charge de l'avenir des pays. Ce sentiment d'échappement du pouvoir par le haut est devenu insupportable pour nos contemporains. S'ils se sentent toujours le besoin d'être guidés, ainsi que l'écrivait Alexis de Tocqueville, ils souhaitent aussi s'affranchir de leur condition, retrouver leur souveraineté nationale[44].

Cette révolution politique et monétaire est, bien entendu, inquiétante pour le système établi, le bien nommé *establishment*. Imaginez la panique que peuvent susciter les annonces à répétition en faveur de la marche inaltérable vers une désintermédiation des échanges ! Dans un système devenu si complexe que la règle technocratique est l'instrument de contrôle typique de l'individu, désemparé par des obéissances dont il ne comprend parfois même pas le sens, la mise en œuvre d'une nouvelle architecture monétaire est un véritable appel d'air démocratique. Elle est aussi un ennemi dangereux pour la finance internationale.

La transformation monétaire de nos économies n'est pourtant qu'au

début de ses prouesses. J'en veux pour preuve que des monnaies comme le bitcoin ou l'ether se présentent aujourd'hui seulement comme des monnaies complémentaires à nos systèmes monétaires. Dans des niches thématiques, elles parviennent cependant à s'affirmer pleinement, par exemple sur le segment des monnaies locales ou sur celui des financements dédiés à la transition écologique. Ces monnaies numériques sont aussi l'occasion unique de développer de nouveaux modèles économiques et sociaux (économie circulaire, économie de proximité) et de renforcer les solidarités locales.

Une remise en cause des équilibres numériques

Cette révolution des mentalités est uniquement possible parce que l'homme s'est doté de nouveaux outils, au premier rang desquels l'informatique. Pourtant, en dépit des avancées fantastiques acquises au cours de cette révolution numérique, le Web ne fonctionne pas ou ne fonctionne plus comme il le devrait. C'est son inventeur, Sir Tim Berners-Lee, qui fait ce constat terrible et ne cesse de le répéter, martelant ces propos critiques dans ses différentes interventions publiques, à la télévision ou dans la presse. S'il rapproche les hommes, le Net crée aussi le matériau de nouveaux secteurs de l'économie fortement discutables.

Les données produites, à chaque heure, à chaque minute, à chaque seconde, dans l'enregistrement de nos activités et de nos comportements numériques sont devenues la matière première d'une économie d'analyse des données. Les nouveaux géants du numérique fondent ainsi leur développement sur une activité d'exploitation de nos vies privées. Pour Sir Berners-Lee, comme pour beaucoup d'autres analystes de cette situation parmi lesquels je me situe, cette nouvelle relation au numérique est viciée. Il faut donc mettre en œuvre de nouveaux systèmes d'identification, à la fois stables et sûrs, pour assurer aux utilisateurs du Net l'anonymat, lorsqu'ils le souhaitent, et l'identification, lorsqu'ils désirent un service personnalisé.

Ces idées sont principalement portées par le bras armé de Sir Berners-Lee : la World Wide Web Foundation. En 2013, le collectif « Web We Want » (« Le Web que nous voulons ») s'est inscrit dans

cette démarche de recherche et de défense d'un Internet plus démocratique, « *promouvant les droits de l'Homme, avec un accès gratuit et une gouvernance partagée* ». Présente sur le terrain dans une soixantaine de pays, cette initiative entend faire du Net un bien public, outil de liberté d'expression et de justice sociale. En pratique, elle propose des « mini-bourses » à « *ceux qui agissent pour le futur du Web* », afin de financer l'innovation démocratique dans les technologies numériques[45].

Les récentes découvertes en matière d'intelligence artificielle permettent de se nourrir de ces bases de données gigantesques. L'aléa n'est donc pas tant technique mais plutôt moral. Le libéralisme à outrance nous a-t-il véritablement conduits à briser les dernières limites de notre intimité ? Nos concitoyens n'y semblent pas prêts et le fait que plus de 200 millions d'internautes utilisent aujourd'hui des logiciels de blocage de publicité montre que le numérique est un des derniers bastions de protection la vie privée, soumis à d'incessantes attaques. Ils sont de plus en plus conscients de la nécessité de défendre ces droits.

L'Internet des objets accompagne cette transformation de nos pratiques du Net, en connectant les éléments de notre quotidien à un immense réseau de partage des informations. Cette interconnexion de nos outils numériques participe aux grandes transitions de ce XXI^{e} siècle : transition économique, transition démographique, transition écologique et transition politique. La blockchain est à la fois un outil de manipulation des actifs digitaux (valeurs, musique, livres numériques) et un catalyseur des usages nouveaux (financement participatif, découverte numérique) tout en respectant les droits à la vie privée et les principes d'égalité.

Allons enfants de la blockchain !

La technologie blockchain signe ainsi une rupture politique dans l'agencement de nos sociétés, vers un retour du pouvoir au peuple souverain. Elle est l'instrument de re-démocratisation de nos régimes politiques, tant espéré par Marcel Gauchet ou Pierre Rosanvallon, régulièrement appelé de ses vœux par l'ensemble de la classe politique. Elle réalise en effet un retour au fondement du pouvoir

populaire, tel que la cité grecque ou les premiers révolutionnaires le concevaient. Nous avons déjà distillé cette idée au cours de notre exposé ou des parties précédentes de la conclusion de notre essai. La blockchain veut ainsi redonner le pouvoir à ses véritables détenteurs.

Dans un univers démocratique où 80 % des citoyens français (selon un sondage Harris Interactive paru en 2016) avouent ne plus avoir confiance en la politique. Le renouveau de la confiance dans le système politique est donc la première étape de réalisation de cette re-démocratisation de nos sociétés. En France, 69 % de nos concitoyens font un constat identique, affirmant que « la démocratie fonctionne mal », dénigrant la classe politique et ses représentants. Les caractéristiques de ce groupe restreint répondent en effet à toutes les critiques : un groupe d'hommes, âgés, candidats à répétition, élus multi-casquettes, tenus par des engagements divers et variés, soumis à l'influence des lobbies.

Pour David Van Reybrouck, auteur de *Contre les élections* (2014), notre démocratie évolue lentement vers trois crises certaines : la crise populiste, engendrée par une croyance aveugle en la nécessité de rénover le personnel politique, la crise technocratique, dénonçant les élites et leur gestion anti-démocratique des États modernes, et la crise des mouvements citoyens, célébrant le retour à la démocratie locale et citoyenne. La solution à ces crises démocratiques est le regain de transparence : plus de transparence dans le suivi des promesses électorales du personnel politique, plus de transparence dans l'organisation des cabinets, lieu de pouvoir de la technocratie, ou encore plus de transparence dans la relation entre l'État et les collectivités territoriales.

La lisibilité des politiques publiques, c'est-à-dire leur accessibilité par tous et à tout moment, est la condition de refonte de notre système démocratique. Des crises récentes comme le Brexit montrent en effet que, mieux informés, les électeurs auraient voté différemment. La blockchain comme instrument de transparence et de partage public des données est à même de répondre à ces défis politiques. Elle redonne aussi le pouvoir d'agir et de décider aux utilisateurs. Elle institue donc, en quelque sorte, une démocratie directe, ainsi avec le mouvement des Indignés en Espagne, révolution citoyenne aux portes de l'Hexagone.

Ces modèles existent déjà et pourront, dès demain, s'implanter et se

développer dans notre pays. En 2015, j'ai rencontré Virgile Deville, activiste de Democracy OS, et nous avons cherché, ensemble, à définir les contours de cette démocratie renouvelée en France, par l'entremise du numérique et des nouveaux outils à disposition. En dépit de ses 25 ans, il travaillait avec acharnement et passion sur ces questions depuis plusieurs années. Il a notamment été inspiré par les travaux du jeune Santiago Siri, un Argentin à l'origine d'un logiciel de supervision des votes des députés. La blockchain apparaît alors comme une sorte de « proxy » politique, servant d'intermédiaire entre le citoyen électeur et le décideur élu.

Et demain ?

Alors que le monde semble prisonnier d'une crise permanente, les aspirations de la blockchain en faveur d'une démocratie renouvelée et d'une société plus équilibrée sont un souffle d'air frais pour nos systèmes politiques. Nous ne pouvons plus seulement appeler de nos vœux le changement de nos comportements. Nous devons le réaliser pour survivre à notre propre disparition. Le monde court aujourd'hui à sa perte : réchauffement climatique, érosion de la biodiversité, montée des eaux. Certains États, comme les îles Vanuatu, sont ainsi sur le point de disparaître et cette situation criante nous rappelle que nous sommes tous citoyens d'une seule et même planète. La blockchain nous offre la possibilité de réaliser cette communauté internationale.

Cette puissance nouvelle, cette liberté retrouvée, offerte par la technologie, ne viennent pas sans grandes responsabilités sur les épaules de l'utilisateur et des infrastructures décentralisées. Bien évidemment, leur jeunesse les fera tomber dans des travers qui ne sont pas tolérables. Elles doivent donc être accompagnées pour pouvoir mieux se relever. Le libre-échange demeure une utopie et des règles de régulation devront donc être établies, sans pour autant tomber dans le travers d'« interdire les interdits ». C'est un véritable défi, mais il nous faut le relever.

Cette technologie est d'autant plus brillante que, si elle crée des nœuds de communication et d'échange au niveau mondial, elle sait aussi impulser une nouvelle dynamique à l'échelon local et territorial. En

accompagnant la création de grille de consommation et de production locale, elle accompagne l'émergence de l'économie locale. Dit autrement, la blockchain est l'argument de durabilité de nos systèmes économiques et sociaux, parce qu'elle garantit une allocation pure et parfaite des biens au niveau local.

Née avec la volonté de résoudre une énigme mathématique et un problème informatique, la blockchain est progressivement devenue une aventure humaine, accompagnant les grandes transformations de ce nouveau siècle. Cette technologie s'est imposée comme une matrice de réflexion sur le rétablissement de la confiance : comment redonner de la stabilité à nos institutions, au sens large du terme, dans un monde en crise perpétuelle. La création d'une monnaie digitale décentralisée, le bitcoin, s'inscrit pleinement dans cette démarche. Il s'agit de la première application de cet effort en faveur d'une confiance renouvelée.

Cette aventure technologique se vit, aujourd'hui, dans son application quotidienne à l'ensemble de la société : transformation de nos territoires, volonté de refonder la démocratie, révolution écologique et numérique, etc. La technologie blockchain intervient dans ces domaines en supprimant la bureaucratie et en accompagnant l'émergence d'organisations décentralisées, replaçant le pouvoir d'action et de décision entre les mains de chaque citoyen.

Demain, nous aurons donc à choisir entre de nouvelles institutions ou des algorithmes mathématiques, outils froids mais incorruptibles. C'était l'ambition de cet essai de donner à chacun la curiosité de vivre les expériences technologiques de notre époque pour pouvoir pleinement participer à ce choix.

Demain, nous aurons le choix de nous fier aux institutions humaines ou à leur extrême opposé : des algorithmes prouvant mathématiquement la confiance. Les deux se développant pour le bien commun, nous nous poserons une question essentielle : quelle entité nous apportera le plus de liberté et le plus de justice ?

Bibliographie

ANDREESSEN, Marc, « Why Bitcoin Matters », *The New York Times*, 21 janvier 2014.

ASSANGE, Julian, *Cypherpunks: Freedom and the Future of the Internet*, OR Books, 2012 (traduction française : *Menace sur nos libertés. Comment Internet nous espionne. Comment résister*, Robert Laffont, 2013).

ASSANGE, Julian, « State and Terrorist Conspiracies & Conspiracy as Governance », Satoshi Nakamoto Institute, 3 décembre 2006, http://nakamotoinstitute.org/static/docs/julian-assange-conspiracies.pdf

BAUWENS, Michel, *Sauver le monde. Vers une économie post-capitaliste avec le peer-to-peer*, Les Liens qui libèrent, 2015.

CHAMPAGNE, Phil, *The book of Satoshi: the collected writings of bitcoin creator Satoshi Nakamoto*, E53 Publishing LLC, 2014.

DAI, Wei, « b-money », blog de Wei Dai, 2001, http://www.weidai.com/bmoney.txt

DELAHAYE, Jean-Paul, « Le Bitcoin, premières crypto-monnaie », *Bulletin de la Société informatique de France*, n° 4, octobre 2014, http://www.societe-informatique-de-france.fr/wp-content/uploads/2014/10/1024-4-delahaye.pdf

DELMAS, Philippe, *Le Maître des horloges : modernité de l'action publique*, Odile Jacob, 1991.

Epicenter, podcast animé par Brian Fabian Crain, Sebastien Couture et Meher Roy, https://soundcloud.com/epicenterbitcoin

FINNEY, Hal, « Bitcoin and Me », Bitcoin Forum sur BitcoinTalk.org, 19 mars 2013, https://bitcointalk.org/index.php?topic=155054.0

FRIEDMAN, Milton, « NTU Talks with Milton Friedman », par John Berthoud, National Taxpayers Union, 1er mars 1999.

GATES, Bill, Bloomberg TV, 2 octobre 2014, http://www.bloomberg.com/news/videos/2014-10-02/bill-gates-bitcoin-is-exciting-because-its-cheap

GIBSON, William, *Neuromancien*, La Découverte, 1985 (version originale : *Neuromancer*, Ace Books, 1984).

GRAEBER, David, *Dette : 5000 ans d'histoire*, Les Liens qui libèrent, 2013 (version originale : *Debt: The First 5,000 Years*, Melville House, 2011).

HAYEK, Friederich A., *Denationalisation of Money : the argument refined*, The Institute of Economic Affairs, 1990 (3e édition), http://nakamotoinstitute.org/static/docs/denationalisation.pdf

HAYEK, Friedrich A., *Monetary Theory and the Trade Cycle*, Mises Institute, 1929.

HUERTA DE SOTO, Jesus, *Money, Bank Credit, and Economic Cycles*, Ludwig von Mises Institute, 2009 (2e édition) (traduction française : *Monnaie, crédit bancaire et cycles économiques*, L'Harmattan, 2011).

LAMPORT, Leslie, Robert SHOSTAK et Marshall PEASE, « The Byzantine Generals Problem », *ACM Transactions on Programming Languages and Systems*, vol. 4, n° 3, 1982, http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf

LEBKOWSKY, Jon et Mitch RATCLIFFE (eds), *Extreme Democracy*, 2001.

LIETAER, Bernard, *The Future of Money: Creating New Wealth, Work and a Wiser World*, Random House, 2001.

MARINI Philippe et Francois MARC, *Rapport d'information sur les enjeux liés au développement du bitcoin et des autres monnaies virtuelles*, Sénat, Paris, 23 juillet 2014, http://www.senat.fr/rap/r13-767/r13-7671.pdf

MAY, Tim, *The Crypto Anarchist Manifesto*, 22 novembre 1992, http://nakamotoinstitute.org/crypto-anarchist-manifesto/

MAY, Tim, *The Cyphernomicon: True Nyms and Crypto-Anarchy*, 1992.

MISES, Ludwig von, *The Theory of Money and Credit*, Yale University Press, 1953.

MOUGAYAR, William, *The Business Blockchain: Promise, Practice and Application of the Next Internet Technology*, Wiley, 2016.

NAKAMOTO, Satoshi, « Bitcoin: A Peer-to-Peer Electronic Cash System », 31 octobre 2008, https://bitcoin.org/bitcoin.pdf

NOIZAT, Pierre, *Bitcoin, monnaie libre !*, 2012.

PEREZ MARCO, Ricardo. « Blockhain : l'autre révolution venue du bitcoin », *Journal du CNRS*, 19 mai 2016, https://lejournal.cnrs.fr/billets/blockchain-lautre-revolution-venue-du-bitcoin

POITRAS Laura, *Citizenfour*, film documentaire, 2014.

RAYMOND, Eric S, *The Cathedral and the Bazaar*, O'Reilly Media, 1999.

STEPHENSON, Neal, *Le Samouraï virtuel*, Robert Laffont, 1996 (version originale : *Snow Crash*, Bantam Books, 1992).

SZABO, Nick, « Bit Gold », 29 décembre 2005, http://unenumerated.blogspot.fr/2005/12/bit-gold.html

SZABO, Nick, « Shelling Out: The Origins of money », blog de Nick Szabo, 2002, http://szabo.best.vwh.net/shell.html

SZABO, Nick, « The God Protocols », 1999 (1re publication, 1997), http://nakamotoinstitute.org/the-god-protocols/

TAIEB, Nassim Nicholas, « Ask Me Anything », forum Reddit, 2013.

TAIEB, Nassim Nicholas, *Le Cygne Noir*, Les Belles Lettres, 2008 (version originale : *The Black Swan: The Impact of the highly improbable*, Random House, 2007).

TAPSCOTT, Don, *Blockchain Revolution, Portfolio* Penguin, 2016.

The Economist, « The Trust machine. How the technology behind bitcoin could change the world », 31 octobre 2015, http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable

VAN REYBROUCK, David, *Contre les élections*, Actes Sud, 2014.

Notes

1. Cité dans Jon Lebkowsky et Mitch Ratcliffe (eds), *Extreme Democracy*, 2001. Voir aussi http://www.goodreads.com/quotes/13119-you-never-change-things-by-fighting-the-existing-reality-to

2. Wei Dai, 1998, liste de diffusion cypherpunks.

3. *Marianne*, « Bitcoin : l'arnaque géante sur internet », 9 septembre 2013, http://www.marianne.net/Bitcoin-l-arnaque-geante-sur-internet_a231609.html

4. Bloomberg TV, 2 octobre 2014, http://www.bloomberg.com/news/videos/2014-10-02/bill-gates-bitcoin-is-exciting-because-its-cheap, et, pour la dernière phrase, Fox News, 6 mai 2013, http://video.foxbusiness.com/v/2359385547001/?#sp=show-clips

5. « Ask Me Anything » de Nassim Nicholas Taieb sur le forum Reddit (2013).

6. https://www.youtube.com/watch?v=mlwxdyLnMXM&feature=youtu.be (14 :36)

7. *The Economist*, « The Trust machine. How the technology behind bitcoin could change the world », 31 octobre 2015.

8. Extrait du « cyphernomicon » par Tim May (FAQ de la liste de diffusion cypherpunk), http://www.cypherpunks.to/faq/cyphernomicron/chapter4.html#3

9. Idem.

10. Extrait du manifeste cypherpunk.

11. Extrait des commentaires dans http://www.jeuxvideo.com/news/438679/interview-de-guildes-sur-eve-online.htm, Jeuxvideos.com, 14 septembre 2015.

12. Forum de discussion AUCRYPTO, cité par *The Indepedent* le

15 novembre 1999.

13. Marco Polo, *Le Devisement du monde*, 1298.

14. *Forbes*, 3 novembre 2012.

15. « Gold and Monetary Conference », La Nouvelle Orléans, 10 novembre 1977, cité par Mises Institute, https://mises.org/library/free-market-monetary-system

16. Lexbase et Kramer Levin cité par l'association Bitcoin France en avril 2014, https://bitcoin-france.org/2014/04/23/analyse-juridique-et-fiscale-de-bitcoin

17. *La République des Pyrénées*, 28 avril 2014.

18. Programme des Nations unies pour le développement, *Rapport sur le développement humain 1990*, ONU. Le texte complet est disponible sur http://hdr.undp.org/en/reports/global/hdr1990 et la dernière version sur http://hdr.undp.org/en/2015-report

19. Joseph Stiglitz, Amartya Sen, Jean-Paul Fitoussi, *Richesse des nations et bien-être des individus*, préface de Nicolas Sarkozy, Odile Jacob, 2009.

20. *Forbes*, 3 novembre 2012, http://www.forbes.com/sites/jonmatonis/2012/11/03/ecb-roots-of-bitcoin-can-be-found-in-the-austrian-school-of-economics/#27560cc5f14f

21. Article L.315-1 du Code monétaire et financier transposé en 2013.

22. Blog, *Alternatives économiques*, « La fascination autour du Bitcoin et des "monnaies virtuelles" : comment les définir ? », 7 novembre 2015.

23. D'après Satoshi Nakamoto, « Bitcoin: A Peer-to-Peer Electronic Cash System », https://bitcoin.org/bitcoin.pdf

24. « My Life Inside a Remote Chinese Bitcoin Mine », CoinDesk.com, 8 juin 2015.

25. *L'Usine digitale*, 11septembre 2015.

26. Virtual School, « Smart Contrats », http://www.virtualschool.edu/mon/Economics/SmartContracts.html

27. Cité par Blockchain France suite à une conférence de Primavera de Filippi.

28. Blog de Jérôme Giustu, « Les smart contrats sont-ils des contrats ? », 27 mai 2016,

29. « La loi des DAO », CoinDesk.com, mai 2016, http://www.coindesk.com/the-law-of-the-dao/

30. Bain & Company, « Ditributed Ledgers in Payment, Beyond the Bitcoin Hype », 13 juillet 2016.

31. Cité par Aude Fredouelle, *Le Journal du Net*, 10 juin 2016 (la dernière phrase est un commentaire de la journaliste).

32. Adam Back *et al.*, « Enabling Blockchain Innovations with Pegged Sidechains », 22 octobre 20014, https://blockstream.com/sidechains.pdf

33. « Far from a mere libertarian fairy tale or a simple Silicon Valley exercise in hype, Bitcoin offers a sweeping vista of opportunity to reimagine how the financial system can and should work in the Internet era, and a catalyst to reshape that system in ways that are more powerful for individuals and businesses alike. »

34. *L'Observateur de l'OCDE*, « Fiscalité, transparence et économie mondiale », n° 267, mai-juin 2008.

35. *The Economist*, « The Trust Machine. How the technology behind bitcoin could change the world », 31 octobre 20015,

36. Guillaume Maujean, « Cette femme veut révolutionner la finance », *Les Échos Week-End*, 3 juin 2016.

37. Conférence Money 20/20, Copenhague, avril 2016.

38. Cité dans la revue sur les crypto-monnaies *The Cointelegraph*.

39. Cité dans Erick Haehnsen « La Blockchain part à la conquête de l'Internet des objets », *La Tribune*, 10 février 2016.

40. Laurent Chemineau, interview de Jean-François Boulier, « La digitalisation ne révolutionnera pas la gestion d'actifs », *L'Agefi*, 24 mai 2016, http://www.agefi.fr/fintech/actualites/video/20160524/digitalisation-ne-revolutionnera-pas-gestion-d-182780

41. Blockchain France, « Démocratie et blockchain : le cas du vote », 12 février 2016, https://blockchainfrance.net/2016/02/12/democratie-et-blockchain-le-cas-du-vote/

42. Cryptos.net, « Technologie de la blockchain ; l'avenir de la démocratie numérique ? ».

43. Sur le blog de ConsenSys, société spécialisée sur les applications de la blockchain Ethereum.

44. « Nos contemporains sont incessamment travaillés par deux passions ennemies : ils sentent le besoin d'être conduits et l'envie de rester libres. », Alexis de Tocqueville, *La Démocratie en Amérique*, 1835.

45. Voir http://webfoundation.org/our-work/projects/web-we-want/