1

Dix ans d'histoire

Born on the Internet

L'Internet a changé le monde, mais aussi l'être humain lui-même dans sa façon de se représenter le monde. Le cyberespace n'est pas un simple prolongement de l'espace physique. Il tend à s'autonomiser. Même si les données se trouvent physiquement dans des serveurs, même si le fournisseur d'accès est soumis à la juridiction d'un État, l'expérience de l'internaute est faite d'avatars, d'absence de frontières, d'un grand sentiment de fluidité.

Une chose est restée bien peu fluide sur Internet : l'argent. En ligne ou, pire encore, en situation de mobilité, la carte à puce reste malgré quelques améliorations d'un usage peu pratique et très peu sûr. Fondamentalement, les monnaies légales, dont la gestion est centralisée et surveillée par un système hiérarchique, sont peu compatibles avec la logique en réseau de l'Internet.

Il est faux de penser que Bitcoin serait né en 2008 du fait de la violente crise financière de cette année-là. Elle a pu précipiter la publication de la solution. Mais le problème était ancien, et la genèse de bitcoin s'étend sur presque vingt ans.

On en trouvera dans *La monnaie acéphale* un historique complet, mêlant tâtonnements techniques, déboires financiers et construction d'une idéologie. Ceux qui veulent éviter l'aspect technique des choses se focalisent sur son versant idéologique. La *Déclaration d'indépendance du cyber espace* de Barlow en 1996 ou le *Cyberpunk Manifesto* de Kirtchev en 1997 sont vraiment des textes à méditer. On dit moins qu'avec le temps, les craintes soulevées dans le milieu au départ très restreint des cypherpunks allaient s'avérer de mieux en mieux fondées. Il faut aujourd'hui, pour parler d'idéologie en ce qui concerne la défense de la vie privée, être soi-même trempé d'une bonne dose d'idéologie sécuritaire. Or, celle-ci structure désormais tout le discours politique et légitime tant la surveillance financière que celle des échanges sur Internet.

À chaque nouvel attentat, un tour de vis est donné, restreignant les droits de chacun sur son propre argent, avec un texte voté si vite qu'on voit bien qu'il était prêt d'avance. Ceci fait bon ménage avec la lutte anti-blanchiment ou contre la (petite) fraude fiscale. Tout converge vers l'obligation pour tout intermédiaire, voire pour tout commerçant, d'identifier de façon de plus en plus précise son client. On promeut par tous les moyens y compris répressifs, une société sans cash. D'autre part et toujours depuis 2001 les lois (*Patriot Act* aux États-Unis, LSQ en France) ciblent les nouvelles technologies liées à l'Internet décrites comme potentiellement criminelles.

Les racines de Bitcoin

Parler d'idéologie libertarienne en ce qui concerne les racines de Bitcoin est donc à la fois vrai et réducteur : au train où vont les choses, les bourgeois libéraux du siècle dernier seraient aujourd'hui considérés comme de dangereux anarchistes.

Mais les *cypherpunks* n'étaient pas les seuls à réfléchir à un mode de paiement nouveau. Tout en maintenant son contrôle sur les paiements en ligne, le monde bancaire cherchait lui aussi la monnaie techniquement adaptée au nouvel âge numérique. Au sein même de la Citibank, une petite équipe inventa une forme de cash électronique que les banques commerciales pourraient émettre comme elles créaient de la monnaie scripturale en consentant des crédits.

Si l'on regarde maintenant les choses d'un point de vue technologique, les diverses propositions et expériences s'appuyaient sur des travaux de cryptographie datant parfois des années 1970. L'horodatage d'un document numérique par inscription dans une chaîne cryptographique fut proposé au début des années 1990. En 1997, Adam Back proposa, pour gêner les spammeurs d'e-mails, le Hashcash, aujourd'hui connu comme le principe de la « preuve de travail » dans le système bitcoin : à défaut de prouver son identité ou son innocence, un participant d'un réseau peut fournir la preuve que sa participation est d'un coût suffisant pour être jugée sérieuse.

En novembre 1998, le chercheur en informatique Wei-Dai publia un papier décrivant une monnaie électronique anonyme permettant des transactions directes et formulant l'idée d'émettre de la monnaie pour compenser le coût supporté par les participants au système afin de fournir leur « preuve de travail ». Et vers 2005 Nick Szabo, un génie touche à tout, proposa le *bit-gold*, un système de création de « preuves de travail » difficiles à produire et donc rares, échangeables comme des unités monétaires. Toutes ces expériences sur le papier furent les prémices du fameux *whitepaper* qui, lui, connut une implémentation.

Un ou des pères ?

Le mystérieux Satoshi Nakamoto n'était donc ni le seul ni le premier. Révélé en novembre 2008 à un tout petit nombre de passionnés et d'initiés, Bitcoin allait rester de très longs mois en couveuse. Dix ans après, on peut voir comment un protocole libre, ouvert et sans autorité centrale a réussi à échafauder un modèle de société assez mouvant, sur un spectre social et intellectuel large, et comment il a obtenu l'adhésion de publics hétérogènes. Ce fut un long chemin, dont les premières étapes, que fort peu de gens ont parcourues, se fondent dans un récit mythologique.

L'absence de géniteur est un bon mythe fondateur. Qui est celui qui a signé Satoshi Nakamoto le livre blanc *Bitcoin: A Peer to Peer Electronic Cash System*[1]? Il prétendait être un Japonais de 37 ans qui aurait travaillé sur ce projet depuis 2007. Le 3 janvier 2009, il sortit la première version du logiciel de Bitcoin et en créa les premières unités, à raison de cinquante bitcoins toutes les dix minutes, largement pour lui seul durant quelque temps. En décembre 2010, il publia un dernier message sur le forum qu'il avait créé, puis désigna comme successeur un informaticien diplômé de Princeton, en lui donnant, pour prévenir le réseau en cas de problèmes graves, une clef d'alerte qui devait être révoquée plus tard. Enfin, en mai 2011 il fit savoir : « je suis passé à autre chose et je ne serai probablement plus là à l'avenir ». Laissant alors orphelins tous les passionnés qui continuèrent le projet.

Parmi toutes les hypothèses, on rencontre des noms de précurseurs, mais aussi d'informaticiens virtuoses comme Hal Finney, décédé aujourd'hui, qui échangea la première transaction en bitcoin avec Satoshi et fut aussi le premier à écrire en deux mots le terme « block chain ». Le nom qui revient le plus souvent est cependant

1. Bitcoin : un système de cash électronique de pair à pair.

celui de Nick Szabo (SN à l'envers). Une équipe universitaire ayant comparé le *White paper* de 2008 aux publications de treize suspects a désigné Szabo comme l'auteur « principal » du document de 2008. Car rien n'indique que le fondateur soit un individu unique.

Aucun consensus n'existe à ce sujet et il y a quantité d'hypothèses douteuses ou farfelues. Le fait que le magot de près d'un million de bitcoins accumulé au commencement par le créateur soit resté intact depuis l'origine accrédite diverses rumeurs et peut étayer l'hypothèse que le créateur est mort, ou bien que la clef a été partagée entre plusieurs personnes, dont une qui a pu la perdre ou mourir.

Tout ceci est plutôt mal perçu de l'extérieur de la communauté. Mais, de l'intérieur, on ressent positivement l'absence du père. Bitcoin ne pourrait être ce qu'il est aujourd'hui sans sa « disparition ». La gestion du code est totalement horizontale. Chacun peut travailler sur une amélioration du protocole Bitcoin et la proposer à tous. Tout se fait par réputation. D'autres blockchains ont un créateur connu, dont le poids intellectuel et financier peut se faire sentir. Les supporters de Bitcoin tiennent à cette distinction : sans créateur identifié, la communauté et sa monnaie sont vraiment décentralisées. Et ici le mot décentralisé est important, car certains ont plus de poids que d'autres, mais pour trouver un consensus, il faut que de nombreux pairs y trouvent leur compte.

Qui qu'il ait été, il est peu probable que Satoshi Nakamoto ait réellement voulu faire fortune. Parmi les critiques superficielles contre son invention, il y a l'idée que ce serait une simple pyramide de Ponzi. Les premiers adeptes de cette monnaie s'en seraient gavés à bon compte et seraient aujourd'hui archi-milliardaires grâce à la naïveté des suiveurs. Ceux qui écrivent cette sottise (en se servant de logiciels ou de navigateurs qui, eux, ont fait des milliardaires parfaitement identifiés) sont trop mal informés.

Qui acheta pour mille euros de Bitcoin en 2009 ?

Presque tous les journaux ont introduit une fois le sujet en notant plus ou moins amèrement que « celui qui aurait acheté pour mille euros de Bitcoin en 2009 » pourrait se régaler aujourd'hui. Évidemment, nul n'a acheté de bitcoin en 2009, et rarissimes sont ceux qui le firent en 2010, pour la bonne raison qu'il n'existait aucune plateforme réellement accessible au grand public. Pendant près d'un an, le bitcoin fut sans valeur aucune. C'était un jeu entre quelques dizaines de geeks. Et comment ceux-là mêmes, qui n'ont pas acheté le moindre bitcoin quand il a connu sa première notoriété avec la crise chypriote de 2013, auraient-ils été capables de prendre un tel risque en février 2011, lorsqu'il atteint enfin, après deux ans de vie, la parité avec le dollar ? De tels rêves de grandeur financière flattent l'ego de ceux qui les poursuivent et n'ont ni la cervelle ni les tripes nécessaires à de pareilles aventures.

La pizza la plus chère de l'histoire est un autre mythe, abordé dès l'introduction de cet ouvrage. Elle incorpore le même anachronisme que la description de Bitcoin comme un Ponzi : quelqu'un qui imaginait le cours actuel du bitcoin en aurait-il échangé 10 000 contre deux pizzas ? Pour la communauté, la pizza partagée chaque 22 mai est un rite festif. Une sorte de nouvelle fête populaire du cyberespace, comme l'est le Pi Day pour les mathématiciens.

S'il existe peu de milliardaires datant de 2009, c'est aussi que des centaines de milliers de bitcoins ont été considérées comme des jouets obtenus au cours d'expériences informatiques ou ludiques. Ils ont été oubliés, les clés privées ont été mal notées ou mal conservées. Les applications ont été mal entretenues, les matériels changés. Quand les médias ont signalé la première hausse des cours, bien des gens se sont aperçus qu'ils avaient perdu un trésor. Un informaticien

britannique avait accumulé 7 500 bitcoins sur un disque dur qu'il a jeté ensuite. En novembre 2013, il se mit à fouiller sa maison en tous sens, puis la décharge de son pays… mais son disque dur y gît toujours sous des tonnes de déchets.

Une étude très détaillée de 2014 mesurant ce phénomène sur une période de 18 mois où le cours du bitcoin avait connu 4 000 % de hausse estimait le nombre des bitcoins perdus à 3,9 millions sur les 13 millions déjà minés alors. On y trouve des adresses contenant jusqu'à 70 000 bitcoins, mais surtout un grand nombre d'adresses en contenant 50. Des gens qui ont miné quelques heures ou quelques jours ont touché une récompense alors sans valeur et ont arrêté le jeu. On trouve des comptes qui semblaient vivre et qui un beau jour sont devenus inertes. Enfin, on trouve des millions d'adresses ne contenant que quelques millièmes de bitcoin : des adresses expérimentales, qui ont servi à des démonstrations ou à des essais. Bitcoin est donc bien moins concentré financièrement qu'on le dit. Et les milliardaires sont venus plus tard.

Une adolescence turbulente, entre *Silk Road* et tempête chypriote

Sorti de l'enfance, Bitcoin eut une adolescence rebelle complaisamment rappelée. Pas une présentation de Bitcoin qui n'en fasse son plat de résistance, voire le menu tout entier. Rappelle-t-on chaque jour que les premiers à émettre du papier-monnaie furent des crapules ?

La *Silk Road* fonctionnait depuis février 2011 sur le modèle des places de marché en ligne qui ne font que mettre en rapport acheteurs et vendeurs, mais elle gérait aussi une activité de séquestre temporaire des fonds lui permettant d'arbitrer d'éventuels litiges. Il faut bien dire que la vente de drogue (avec 13 000 références de

stupéfiants, jusqu'aux plus violents) assurait la majeure partie des revenus du site. On y trouvait aussi des armes, des faux papiers, des logiciels malveillants et bien des choses *off-limits*. Enfin, le site offrait un forum où les membres pouvaient échanger leurs conseils sur la façon la plus discrète de recevoir leurs colis.

Les trafics de drogue sur le Net n'avaient pas attendu Bitcoin, mais le règlement des transactions restait en 2009 le maillon faible des activités illégales dans les *darknets*. Que les acteurs des marchés illégaux aient compté parmi les premiers utilisateurs du bitcoin s'explique alors aisément. La *Silk Road* ouvrit un boulevard non seulement à ceux qui voulaient interdire Bitcoin, mais aussi à ceux qui rêvent de contrôler l'Internet et ses profondeurs invisibles.

Lorsque le 2 octobre 2013, le FBI appréhenda Ross Ulbricht, la presse reprit les chiffres du rapport public mais en préférant les retranscrire en dollars. Or, sur les 33 mois de fonctionnement de la *Silk Road*, le bitcoin était resté deux ans autour de 10 dollars avant de décoller, de commencer le mois d'octobre 2013 à 100 dollars et de le terminer à 200 dollars. La conversion du bilan de la *Silk Road* au prix du moment de la fermeture (130 dollars) contribua à lui donner une importance spectaculaire. Entre sa création en février 2011 et juillet 2013, la *Silk Road* aurait en réalité vu passer un peu plus de 1,2 million de transactions, pour un total de 9,5 millions de bitcoins, générant 600 000 bitcoins de commissions pour le site. Ce sont ces deux derniers chiffres en bitcoin qui, abusivement convertis en dollars se sont transformés en 1,2 milliard de ventes et 80 millions de commissions.

Le 1,2 million de transactions sur la *Silk Road* est à comparer au total de 6,9 millions de transactions enregistrées depuis l'origine jusqu'au 2 octobre 2013 sur la Blockchain. Soit une proportion de 17 % ou un peu moins si l'on pense que bien des transactions

ont eu lieu en « compte *Silk Road* ». Les 600 000 bitcoins gagnés par le site représentaient environ 5 % des bitcoins existants en octobre 2013. Il est donc incontestable que ce marché illicite a joué un rôle dans l'économie du bitcoin. Pas de quoi cependant étayer l'identité remarquable « bitcoin = drogue » qui va être répétée ensuite durant des années. Quelques mois plus tard, Bitcoin allait traverser une nouvelle tempête avec la faillite de la plateforme MtGox. Elle avait été créée des années auparavant pour échanger des cartes du jeu *Magic The Gathering*. Ayant découvert Bitcoin dès 2010, son créateur la spécialisa dans cette nouvelle monnaie, puis la revendit en mars 2011 à un informaticien français qui s'était installé au Japon en 2009, Mark Karpelès. En quelques mois le nombre des clients était multiplié par vingt. Deux ans plus tard, et malgré le très grand nombre de plateformes créées, MtGox représentait 70 % des volumes d'échange sur le bitcoin, qui commençait son ascension. Plus dure fut la chute.

Mark Karpelès a probablement été dépassé par sa croissance, et n'a pas réussi à embaucher des gestionnaires expérimentés. Les incidents se multiplièrent. En février 2014, il dut suspendre les transactions, puis mettre MtGox en faillite. En avril, le liquidateur annonça un trou de 850 000 bitcoins manquants ou volés. Karpelès plaida le piratage. Faillite ou arnaque ? On peut imaginer une négligence transformée par un trop long silence en délit caractérisé, une manipulation tentée pour gagner du temps, ou un Ponzi pur et simple.

Par la suite, on retrouva 200 000 bitcoins, mais il apparut que les premières disparitions dataient de 2011, soit avant le rachat au créateur, qui aurait conseillé à Karpelès de garder la chose pour lui. On finit par penser qu'une bonne partie des bitcoins disparus n'aurait jamais existé, et que MtGox aurait aussi manipulé le cours à la hausse avec des robots.