LES APPLICATIONS DE LA BLOCKCHAIN ?

Par Fabienne Marquet, Philippe Rodriguez, Hadrien Szigeti, Pierre Manenti, Philippe Dewost, Stéphane Marchand

Août 2017

- **Philippe Dewost** (Caisse des Dépôts et Consignations)
- **Philippe Rodriguez** (auteur de « La révolution Blockchain », éditions Dunod)
- **Pierre Manenti** (Collaborateur parlementaire au Sénat)

Animé par **Stéphane Marchand**, Rédacteur en chef Paris Innovation Review

Fabienne Marquet, Vice-présidente X-Sursaut

Je suis ravie d'être parmi-vous ce soir pour ma première intervention et d'introduire la réunion de ce soir qui traite du sujet de la Blockchain ; et je remercie tout particulièrement Laurent Daniel pour son accueil, sa disponibilité, sympathie et accompagnement dans ma nouvelle mission au sein d'X-Sursaut.

La blockchain est une technologie qui a fait parler d'elle depuis l'essor du Bitcoin (créé en 2009), et qui aujourd'hui est un sujet qui serait **imprudent d'ignorer**. Pour précision, la blockchain est un registre public ouvert et partagé que personne ne peut falsifier, et que tout le monde peut inspecter. En effet, cette technologie qui permet de partager de l'information de manière sécurisée sans tiers de confiance, devrait bouleverser **les usages et la chaîne de valeur dans bien des secteurs économiques,** en réduisant les coûts et en permettant de nouveaux marchés. Plus généralement, certaines organisations cherchent à comprendre comment la blockchain (la technologie sous- jacente au bitcoin) pourrait fournir une alternative crédible à l'infrastructure procédurale, organisationnelle et technologique indispensable au maintien de la confiance à l'échelle institutionnelle. Ces travaux exploratoires en sont encore au stade primaire ; toutefois, leurs conséquences pourraient être profondes.

Tout comme Internet a réinventé la communication, la blockchain pourrait transformer la façon de gérer les transactions, les contrats, et plus généralement le concept de confiance ; autant d'éléments indispensables au bon fonctionnement des entreprises, des gouvernements, et de la société. Pour autant, le

développement de cette technologie soulève des questionstechniques qui restent à résoudre. Au- delà de problèmes de scalabilité (de la technologie blockchain actuelle), il faudra aussi s'assurer que les promesses de diminution des coûts sont réelles, et que les acteurs vont s'y mettre vite, sachant qu'aujourd'hui les systèmes de paiement fonctionnent plutôt bien, et que tout casser pour remplacer par des systèmes blockchain prendrait beaucoup de temps car on ne part pas de zéro, les infrastructures de réseau sont très complexes. Enfin, c'est beaucoup de grands changements en perspective… Bon débat !

Stéphane Marchand : Nous sommes là pour parler de la Blockchain. C'est l'un des mots les plus prononcés de France. C'est aussi un des mots sur lesquels on dit le plus de choses et de bêtises. Je voyais pendant l'introduction des visages de nos experts se froncer : c'est bon signe car si nous ne sommes pas d'accord entre nous ca veut dire que le débat va être intéressant. Donc de quoi parle-t-on et quelles sont les applications intéressantes de la blockchain ? les opportunités et les risques ? et pour nous tous quand est-ce qu'on va « croiser la blockchain » et qu'elle va intervenir dans nos vies d'une manière tangible ?

Philippe Devost : Pour démarrer avec des questions très simples est-ce qu'il y en a parmi vous qui se disent qu'ils n'ont rien compris à la blockchain ? (nombreuses mains levées) Qui pensent être des experts de la blockchain ? (1 ou 2) Qui ont des bitcoins ? des Ethers ? (quelques uns) Je vais vous rassurer c'est normal de n'avoir rien compris car on est probablement devant l'un des sujets intellectuels les plus compliqués de ce début de millénaire et notamment pour nous Français car on a plusieurs maladies génétiques dont une s'appelle Descartes. On aime bien réduire les sujets compliqués dans les concepts les plus simples possibles. Quand ca peut tenir en un phrase ou faire une une de journaux c'est encore mieux. C'est ce qui nous conduit à lire 80% de bêtises dans la presse.

Première bêtise qui a été dite tout à l'heure : la blockchain n'est pas une base de données. La Blockchain ne sert pas à stocker de l'information. Pour le reste le mieux c'est de raisonner par analogie. Internet a été et est encore aujourd'hui une infrastructure qui s'est développée beaucoup plus vite que l'on imaginais, qui connecte à peu près 4 à 5 milliards de gens et autant de machines, et d'ici 15 à 20 ans le nombre de machines connectées sera vraisemblablement d'un ordre supérieur. Mais Internet fondamentalement est une infrastructure neutre, et qui ne sait faire qu'un seule chose d'une manière incroyablement efficace c'est copier de l'information. Lorsque j'envoie un email ce que je fais c'est faire une copie d'un texte : la copie arrivera dans la boite mail du destinataire mais la version originale restera dans la mienne. Quand on gère des sujets assez compliqués on est content d'avoir gardé une copie du message qu'on a envoyé ! Si j'envoie une photo de mon smartphone, c'est pareil : d'une image je vais en faire deux.

Amusez vous maintenant à remplacer intellectuellement email ou photo par un billet de banque et vous vous apercevrez qu'on a immédiatement un problème. Internet n'est absolument pas fait pour gérer des contenus qui ont vocation a être uniques, à être identifiés et à ne pas être dupliqués. L'industrie des medias qui a fait un saut formidable sur Internet il y a 25 ans en fait aujourd'hui les frais. L'industrie des medias souffre aujourd'hui parce qu'Internet n'est pas fait pour maintenir l'intégrité d'une information unique tout au long de sa vie. Lorsque je vous montre ce billet nous n'avez même pas besoin de mobiliser votre intellect pour savoir que ce billet est unique. Si maintenant je tends ce billet à Philippe et qu'il le prend devant vous tous il est évident qu'une transaction vient de s'opérer. Il est implicite que ce billet a changé de main vous en êtes tous convaincus. Ce billet qui est sorti de ma poche n'existe pas en double dans ma poche. Il n'y a pas une banque centrale dans la poche gauche de mon pantalon. Et c'est cette confiance implicite dans la transaction qui vient de s'opérer et dans toutes les

autres qui fait que tout le système économique fonctionne. C'est un implicite absolu. le seul doute qui subsiste c'est de savoir s'il me le rendra à la fin du débat !

Une fois que vous avez compris que les sujets de Blockchain s'appliquent au monde des transactions et non plus au monde des informations vous avez fait un grand pas, puisque la question est bien de savoir opérer un grand nombre de transactions à travers un réseau, et notamment un réseau de machine exactement comme Internet. A quelques petites différences près.

La première différence c'est que pour opérer ces transactions on ne fait appel qu'à des machines, du moins dans les Blockchain les plus connues, qui sont les blockchains publiques, et notamment celle qui tourne depuis huit ans sans avoir jamais été compromise, Bitcoin. Sur cette Blockchain les opérateurs qui certifient et enregistrent vos transactions dans des grands livres ouverts sont des machines. Et tout est fait pour que ce ne soit que des machines. Et comme Philippe Rodriguez l'a dit un jour, le système de preuve de travail par lequel les machines vérifient et certifient vos transactions c'est l' « anti-Captcha ». Le Captcha (Completely Automated Public Turing test to tell Computers and Humans Apart) est un test qui est là pour s'assurer que « *ce* » qui est devant l'écran ou du service à ce moment là est un humain. La preuve de travail dans le Bitcoin c'est exactement l'inverse : c'est la garantie qu'aucun humain à aucun moment n'a pu toucher à votre transaction.

Donc quand vous dites la blockchain est une infrastructure de confiance ca va assez loin culturellement parlant, parce que ca veut dire qu'on est dans une défiance absolue vis à vis de l'humain. Il faut le relier à son contexte car c'est important avec les choses complexes : la Blockchain du Bitcoin apparaît quelques mois après la chute de Lehman Brothers, à un moment où l'on n'a jamais eu aussi peu confiance en l'humain. Et ce pour deux raisons. D'abord une raison formulée depuis quelques millénaires par les Romains : « errare humanum est ». L'humain

— et même le Polytechnicien — parfois se trompe dans ses calculs. Mais il y a un autre comportement de l'humain qui pose un problème c'est que de temps en temps certains humains — en général un petit nombre — ont une fâcheuse tendance à se mettre d'accord dans le dos de tous les autres en vue de les trahir, de les enfumer, de détourner leurs biens, etc. C'est contre ca au départ que la Blockchain apparaît, et il faut garder ca à l'esprit tout le long de ce qui va pouvoir être dit dans le débat. Les Blockchain publiques sont des infrastructures qui sont neutres et dont l'objectif est de sécuriser de bout en bout des transactions de manière décentralisée sans jamais faire intervenir un humain dans les mécanismes qui sécurisent les transactions. Et pour s'assurer qu'aucune de ces machines ne peut être manipulée par un humain, la preuve de travail est une gigantesque loterie entre des machines qui vont exécuter des centaines de millions de calculs pendant une dizaine de minutes ayant pour objectif tout en consommant pas mal d'énergie de trouver la première une propriété crytographique particulière, et de lever la main en disant « j'ai trouvé ! ». Là le réseau s'arrête et vérifie en un rien de temps que l'opération qui a été effectuée par la machine qui a gagné est la bonne. L'analogie qui est utilisée est celle du Sudoku : comme l'écrit Philippe Rodriguez dans son ouvrage, la preuve de travail est *« une énigme mathématique complexe à résoudre dont la vérification est, elle, relativement simple. Prenons l'exemple d'un Sudoku à 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. »*

Dans les Blockchains publiques celle qui est la plus controversée c'est celle de Bitcoin. La meilleure manière de comprendre pourquoi c'est à nouveau une comparaison : la Blockchain de Bitcoin est comme un autoroute qui aurait été déployée il y a 8 ans et sur laquelle il n'y aurait jamais eu aucun accident. Pourquoi alors est-ce si controversé ? C'est justement parce que au péage et dans les stations services vous avez la mafia, du traffic de drogue, du car jacking, de l'essence

frelatée… Ce sont à nos interfaces entre cette infrastructure et le monde réel que la plupart des problèmes se produisent, tout simplement disent les ultra-libertarien parce que c'est là que des humains interviennent : ceux qui vous échangent des Euros contre des Bitcoins ou des Ethers, ceux qui gèrent le stock de clés privées, qui du coup peuvent être assez facilement corrompus. Gardez bien cela à l'esprit : l'infrastructure elle est neutre exactement comme Internet. Et je vous rappelle qu'au début du Minitel qui était le prototype Internet français, la plupart des usages qui ont tiré la consommation et le déploiement étaient des usages considérés aujourd'hui de manière consensuelle comme réprouvables voire illicite. C'est exactement la même chose aujourd'hui avec la Blockchain.

Stéphane Marchand : Le grand bonheur avec la blockchain, et c'est le gage de sécurité, c'est que jamais aucun humain n'y a de responsabilité. Cela peut inquiéter pas mal. Pierre Manenti, vous vous êtes intéressé à la manière d'accompagner juridiquement et politiquement la blockchain, pour qu'elle rende des services aux êtres humains. Racontez nous comment vous envisagez la choses, comment vous travaillez, comment vous raisonnez.

Pierre Manenti : On a eu une présentation assez complète de ce que pouvait être la blockchain. Pour bien en comprendre les enjeux il faut s'imaginer qu'elle repose sur 3 piliers, qui la caractérisent en tant que technologie numérique et permettent d'apporter de l'innovation à différents secteurs de la vie de tous les jours, comme l'énergie, la monnaie ou encore la politique. En fait, tous sont des secteurs qui reposent sur des échanges. La monnaie existe mais pas pour soi : l'argent est là pour permettre de réaliser des échanges entre des individus. Ce que la blockchain a changé c'est d'opérer une révolution des échanges.

Le premier pilier sur lequel repose cette technologie c'est la transparence : la blockchain c'est un grand livre de comptes qui est public. Tout le monde peut voir les transactions, savoir d'où elles viennent, ce qu'elle contiennent, et c'est la

première rupture des échanges. Jusqu'à présent, les échanges étaient secrets. On négociait entre soi. On n'avait pas besoin de dire ce qu'on faisait. Désormais on a un besoin de transparence, à la fois dans l'espace public et dans la vie des entreprises. Et la première chose qu'on a voulu réglementer c'est ce qu'on appelle la RSE (Responsabilité Sociétale des Entreprises), en Anglais CSR (Corporate Social Responsibility). On a déterminé qu'à partir d'aujourd'hui les entreprises avaient la responsabilité d'être transparente vis à vis de leurs actionnaires et de leurs clients.

Deuxième chose qui qualifie la blockchain et qui en fait une technologie futuriste, c'est son sérieux et sa sécurité optimisée. Les échanges, on pouvait les influencer : la mafia, le vol, les conflits litigieux. La blockchain, elle, repose sur les algorithmes, et pour citer Philippe Rodriguez, aujourd'hui on ne fait plus confiance aux institutions, parce qu'elle sont corrompues et détenues par des êtres humains — personnalités politiques, grands dirigeants, et grands financiers sur qui on jette l'opprobre — par contre on fait confiance aux chiffres. Les chiffres sont neutres. Et c'est justement la neutralité apportée par la blockchain : les échanges ne sont plus des échanges entre des humains, mais entre des ordinateurs, des machines qui n'ont pas d'intérêts personnels, qui ne peuvent pas être corrompues.

Et enfin le troisième qualificatif de la blockchain, c'est l'autonomie : jusqu'à présent il y avait toujours un régulateur. On a évoqué tout à l'heure la banque centrale, c'est à dire un acteur central qui surveille tout ce qui se passe. Ca vaut pour la monnaie mais aussi pour l'énergie, les transports, la consommation,… Et ces régulateurs sont là pour dire « Attention ! On surveille qu'il n'y ait pas d'excès. On surveille les comportements humains pour limiter les pratiques corrompues. » Eh bien la blockchain dit « Non, on n'a pas besoin de ce régulateur, car on peut fonctionner de manière autonome en faisant confiance non plus aux dirigeants, mais à tous les individus. » Et là, tout à l'heure on a dit avec l'analogie du Sudoku

que pour vérifier qu'une transaction était valide, il fallait que des centaines de milliers d'ordinateurs réfléchissent à cette même opération. Aujourd'hui, c'est la banque centrale qui fait le Sudoku tout seul puisque c'est à elle qu'on fait confiance. La blockchain dit « Oui mais cette banque centrale, c'est un humain ou du moins c'est contrôlé par des humains, donc je ne suis pas sur qu'on puisse lui faire confiance, alors tout le monde va faire le Sudoku, comme ca même si l'un d'entre nous est corrompu ou a intérêt à donner un faux résultat, tous les autres pourront donner le bon résultat. »

Voilà les trois critères qui ont fait émerger la blockchain : être plus transparent, plus sécurisé, et plus autonome. Je vous raconte tout cela, car il y a eu de multiples changements dans différents secteurs comme la démocratie. On ne fait plus confiance aux personnalités politiques, et l'on a envie d'une nouvelle forme de démocratie, ce qu'on appelle une démocratie plus liquide dans laquelle la relation entre le citoyen et l'élu est beaucoup plus simple. Exemple : aux Etats-Unis une loi donne à un collectif de citoyens le droit de déchoir un élu de son statut s'il ne respecte pas un certain nombre d'engagements. C'est ce que permettrait la blockchain : faire qu'un collectif d'utilisateurs de la blockchain invalide une décision prise par un élu.

Deuxième secteur d'innovations : celui de la santé. Depuis la réforme de la loi santé de 2016, vous avez tous un dossier médical personnel, auquel chaque médecin peut accéder et dans lequel il y a toutes vos informations de santé : les médicaments que vous prenez, les accidents médicaux que vous avez pu avoir, et aujourd'hui vous ne savez pas trop qui a pu avoir accès à ce document. Qu'est ce qui vous empêche de penser qu'un médecin malhonnête pourrait vendre ce document à une entreprise pharmaceutique. Le blockchain permet d'apporter transparence et sécurité des données, puisque les données sont cryptées et enregistrées sur une base de données, on ne peut plus y accéder sans votre

consentement. Donc pour qu'un médecin puisse accéder à vos données il faut sa clé d'entrée et la vôtre, un peu comme lorsque vous déposez à la banque un bien précieux, et que vous avez deux clés, celle du banquier et la vôtre.

Troisième secteur d'innovations, l'énergie : jusqu'à présent vous aviez un fournisseur national d'énergie qui produisait et vous vendait de l'énergie. Aujourd'hui avec la révolution technologique de l'énergie et la promotion des énergies vertes, vous pouvez avoir des panneaux solaires sur votre maison, et vous deviez jusqu'à maintenant revendre à EDF l'excédent d'énergie que vous produisez et que vous ne consommiez pas. Ensuite, EDF en tant que régulateur national le revendait à qui en avait besoin. La loi a changé en 2015 — et cela permet de montrer comment la loi vient en complément de la technologie blockchain — pour permettre, si vous produisez de l'énergie, de la vendre à vos voisins dans votreimmeuble ou votre lotissement. Et la loi de 2017 permet maintenant de la vendre au niveau du quartier, et vous n'avez même plus besoin d'en informer le régulateur national. Vous êtes libres de faire ce que vous voulez avec votre énergie, et la vendre au plus offrant, au prix que vous souhaitez. La blockchain permettrait de faciliter et d'accélérer ces échanges, en faisant le lien entre les besoin de votre voisin et vos capacités de production d'électricité.

Dernier exemple d'apport de la réglementation dans le domaine des véhicules électriques : aujourd'hui on promeut des véhicules plus autonomes et verts, c'est à dire moins polluants et plus intelligents, mais qu'il faut recharger. L'ex-ministre de l'environnement, Ségolène Royal, avait mis en place un plan de déploiement de bornes de recharge électrique, c'est à dire que l'Etat-Institution a décidé de mettre partout sur le territoire des bornes pour recharger les voitures reliées au réseaux d'énergie. Or une proposition de loi qui devrait être discutée prochainement vise à ce que des individus via leur production individuelle d'énergie solaire puissent directement alimenter ces bornes de recharge. C'est à dire que demain votre

maison sera directement connectée à une borne de recharge dans la rue, devant chez vous. Et là se pose une question technique non-résolue : comment l'individu qui se gare devant chez vous vous payera pour l'électricité consommée depuis vos panneaux solaires. Première option : la redevance. C'est la situation actuelle. L'Etat vous payera tous les mois une somme fixée d'avance, et si la consommation dépasse cette somme tant pis pour vous. Deuxième solution qui commence à être réfléchie : via la blockchain, un contrat vous lie à n'importe quel utilisateur de véhicule, et si cet individu veut s'approvisionner sur la borne il lui faut un portefeuille numérique avec des bitcoins qu'il aura créé en quelques clics, et il pourra payer avec son téléphone ou pourquoi pas avec son empreinte digitale, et là, la loi est importante pour débloquer tous les problèmes technologiques et juridiques qui freinent le déploiement de l'internet des objets. La loi n'est donc pas là pour encadrer, mais joue le rôle d'outil de développement et d'accompagnement de la blockchain.

Pour aller plus loin dans la blockchain on aura besoin de fixer son cadre juridique, et les lois seront donc essentielles à son développement à moyen terme.

Philippe Devost : sur le dernier point mentionné, la loi a effectivement un rôle majeur dans l'organisation et l'encadrement des interfaces. Je voulais également vous proposer un autre cas d'usage qui va éclairer tous les exemples qui ont été cités. Quand on fait des transactions dans le monde actuel, en général, vous regardez avant ce dont le parties disposent et peuvent engager dans la transaction — ce que chacun a sur compte bancaire — avant d'opérer la transaction — un décrément de l'un des comptes et un incrément de l'autre. Aucun argent ne circule : c'est juste un jeu d'écriture. Il y a des chambres de compensation qui vérifient que tout cela fonctionne bien. Dans la blockchain on se pose une question complètement différente sur la transaction. La question devient « A qui appartient ceci ? » et « A qui est-ce que cela appartient maintenant ? » comme si à chaque

passage d’un billet de main en main chacun de ses dépositaires temporaires l’horodataient et le signaient avant de le transmettre. La blockchain vous permet donc de retracer l’historique d’un actif unique de bout en bout depuis sa création. C’est une nouvelle manière de regarder les transactions.

Par analogie avec les trois piliers cités par Pierre Manenti, Satoshi Nakamoto quand en 2008 il publie son manifeste et instancie le premier noeud quelques mois plus tard, il est en fait le premier à combiner de manière absolument géniale et unique trois technologies qui sont connues depuis des dizaines d’années. La première est celle des réseaux décentralisés de pair à pair, qui démarre avec la DARPA et Internet il y a 25 ans, continue avec le protocole Torrent — qui est aussi un protocole neutre dont les usages ont rendu la réputation sulfureuse — ou Skype ou le SETI — Search for Extra-Terrestrial Intelligence, première expérimentation de crowdsourcing de puissance de calcul à très large échelle menée il y a un vingtaines d’année. La deuxième invention est très ancienne : c’est un moine franciscain à Venise en 1494 qui invente la comptabilité en partie double, même s’il y a débat sur le sujet. C’est donc une invention Européenne qui structure le commerce mondial et les registres standardisés qui enregistrent toutes les transactions passées dans le monde depuis au moins un demi millénaire. Et le troisième objet c’est un actif cryptographique — un jeton de valeur — qui ne doit sa valeur aujourd’hui qu’au fait qu’un jour des gens ont estimé que ca valait le coup de l’échanger contre des Dollars ou des Euros. Mais au départ c’est un actif cryptographique unique, divisible au cent-millième dans le cas de Bitcoin, qui circule le long du réseau en étant utilisé soit comme valeur de transaction — comme « monnaie » d’échange même si ce n’est pas une monnaie — soit comme marqueur d’un transaction qui n’a rien à voir avec la valeur transférée en utilisant le champ de méta-données, comme dans un SMS, dans lequel on ne peut inscrire qu’un message court comme le code cryptographique unique de ce à quoi se réfère la transaction. En général on utilise une fonction crytographique de

hachage Sha256 qui la propriété que les collisions y sont pratiquement impossibles et que le changement de la moindre virgule dans le document — comme ajouter un zero ou changer une date — résulte en une empreinte de hachage radicalement différente de l'empreinte source. Vous pouvez immédiatement savoir en 2 ou 3 caractères que ce n'est pas le même document. La preuve elle-même n'est pas disponible en clair mais elle est opposable. Toute personne qui prétend pouvoir produire un document peut le prouver devant une autorité légale. Et si demain le juge le reconnaissait comme élément de preuve on aurait quelque chose qui fonctionnerait en droit des contrats.

Philippe Rodriguez, auteur de La Révolution Blockchain, « Algorithmes ou institutions à qui donnerez vous votre confiance ? », chez Dunod réagit aux propos précédents, avec toujours ce mélange d'excitation et d'inquiétude que déclenche la Blockchain.

« Dans mon livre j'essaye pour mieux expliquer la Blockchain de repartir d'un certain nombre de ses racines, et de comprendre le pourquoi plutôt que le comment. Le comment est passionnant, et l'on vient d'évoquer les algorithmes de hachage et de cryptographie. On aurait envie d'y passer des heures, mais on risquerait probablement de manquer la finalité derrière ce système qui permet de gérer des transactions décentralisées. On a aussi évoqué la loi et comment il faut l'encadrer. En fait ce n'est pas la Blockchain qui s'intéresse à la loi, c'est la loi qui s'intéresse à la Blockchain parce qu'on est dans un système conçu pour échapper à un environnement centralisé et autoritaire. »

« Premier sujet c'est l'origine politique et culturelle très importante de la Blockchain, chez les CypherPunk une communauté de « geeks » au début des années 90 qui s'intéresse au sujet de la protection de nos vies privées sur Internet, et qui imagine que dans le futur, dans une société de plus en plus digitale, un gouvernement ou un système privé pourrait menacer notre droit à la vie privée.

Pour tout vous dire au début ils ne sont pas vraiment pris au sérieux, ou font même franchement rire. On les voit plutôt comme des gens paranoïaques et introvertis. Aujourd'hui ils ne nous font plus rire du tout. L'idée qu'un jour un gouvernement pourrait lire nos emails ne fait plus rire personne depuis 2013, puisqu'on a appris que la surveillance de masse des communications Internet existait bien, et qu'elle a été dénoncée parEdward Snowden et d'autres lanceurs d'alertes. La façon dont les CyberPunk réfléchissent est très simple : leur connaissance de la cybersécurité les amène à penser que tout système dans lequel l'humain joue un rôle est peu fiable. C'est à l'opposé de ce que l'on a appris concernant la société de confiance : nous avons été éduqués dans un système qui prône l'humain comme véhicule de la confiance. Voici un premier paradoxe.

(42'00) *Il y a eu beaucoup de recherches concernant le niveau de confiance qu'on peut avoir dans un groupe. Connaissez vous Monsieur Dunbar ? C'est un anthropologue et chercheur britannique, qui a proposé une étude concernant le « nombre de Dunbar », qui vaut environ 150. Son sujet est assez simple : dans un groupe de mammifères quelle est la taille maximale pour qu'il y a un niveau de confiance suffisant ? Normalement ce nombre se situe au alentours de 15 à 20, mais pour l'être humain on arrive à une valeur atypique de 150 parce que l'on a inventé une technologie unique qui s'appelle le langage. Grace au langage on arrive à se faire confiance à 150 dans un groupe. C'est une mauvaise nouvelle pour tous les gens qui ont 6000 amis sur Facebook et pensent pouvoir leur faire confiance.*

Depuis 10.000 ans avec l'invention de l'agriculture, une nouvelle technologie va nous permettre de casser le nombre de Dunbar, et de passer de 150 à des groupes organisés de plusieurs milliers, et ensuite de plusieurs millions. Cette nouvelle technologie ce sont les institutions, qui permettent de déployer l'agriculture. Ces institutions sont toujours basées sur une croyance commune qui peut être une

religion, ou des valeurs (« Liberté, Egalité, Fraternité »), ou une croyance comme « L'Euro est une monnaie ». A partir de ces croyances on va construire des instruments qui permettent de développer l'agriculture, de créer une banque centrale, et de créer une démocratie : des villes, des Etats-Nations, puis des empires. On va créer des églises, qui sont capables d'augmenter dans des proportions gigantesques. L'église catholique est la première à atteindre le milliard d'individus. Des organisations un peu plus grosses, apportées par le numérique : Facebook a aujourd'hui 2 milliards d'utilisateurs, qui vont avoir un certain nombre de croyances communes dans leur fonctionnement.

Demain il faudra aller au delà et dépasser ce nombre de Dunbar qui tourne donc aujourd'hui autour de 2 milliards d'individus, parce que d'une part il va falloir qu'on vive dans un environnement constitué d'ici 2030 d'environ 10 milliards d'êtres humains, et d'autre part 5 à 6 intelligences artificielles avec lesquelles chacun de nous va discuter — une assistante virtuelle, nos objets connectés,… — ce qui fait pas loin de 50 milliards d'individus supplémentaires dans lequel il va falloir construire des réseaux de confiance. Est-ce que vraiment on va pouvoir baser notre confiance sur des institutions ? La question se pose. Le début de réponse que j'apporte c'est de dire qu'avec la Blockchain on a la capacité à créer de la confiance dans un système « ouvert ». C'est probablement la prochaine technologie qui va être capable de casser encore une fois le nombre de Dunbar et de passer de 2 à 60 milliards d'individus, et dans laquelle ni un Etat, ni une banque, ni un géant du numérique ne pourra être le point commun entre tous ces individus.

Pour faire quoi ? Pour faire ce qu'on a vu tout à l'heure : rendre efficace la démocratie; rendre efficace la transition écologique par ce qu'elle nécessite aussi de la confiance; rendre efficace d'autres transitions démographiques et monétaires. Dans toutes ces transitions qui nécessitent de la confiance, on peut

considérer que les organisations centralisées ne vont plus fonctionner, et que vont s'opposer des systèmes centralisés, algorithmiques comme la Blockchain, contre des organisations super-centralisées fondées sur des institutions.

Dernier exemple : c'est le cas d'un système décentralisé de monnaies qui existaient dans l'île de Yap en Micronésie. Après la deuxième guerre mondiale on a découvert dans une île des roues de pierre assez importantes de 80cm à 2,20m de haut et qui pèsent chacune plusieurs tonnes, et en étudiant la géologie de cette île on s'est rendu compte que la pierre avec laquelle était faite ces roues n'existait pas sur cette île. En visitant l'archipel on se rend compte qu'il y a effectivement une île à 6km dans laquelle on trouve cette pierre-là, et on comprend qu'elles sont extraites sur place et ramenées en pirogue sur Yap.

A quoi servent ces pierres ? Ces pierres servent à faire de la monnaie suivant un principe (encore une fois) très simple : c'est un registre ouvert comme une Blockchain. Imaginez que vous disposiez d'une pierre de 2m et que vous vouliez acheter une maison. L'ensemble de l'île — un peu moins de 1000 habitants — se rappelle que cette pierre est la pierre de votre famille. Il suffit donc de se mettre d'accord avec le propriétaire actuel de la maison que maintenant il disposera de la propriété de cette pierre. On retrouve le principe de la Blockchain, où le premier élément est de pouvoir prouver la propriété. On n'écrivait rien sur ces pierres : c'est seulement la mémoire collective de la totalité de l'île qui se rappelle comme dans un registre que cette pierre appartient maintenant à celui qui a cédé la maison. Pas besoin de banque ou de banque centrale. C'est un système dans lequel la confiance est établi par un système décentralisé commun qui est l'ensemble de la mémoire des habitants de l'île. Preuve que ces systèmes ont existé et ont fonctionné, et qu'il faut continuer à réfléchir à la façon dont ils doivent se développer.

Questions

Alain Bernard : dans le système décentralisé à 60milliards est-ce qu'il y aura encore des élections ?

PR : *On a rapidement évoqué la démocratie liquide. Je pense qu'il y a aura toujours des élections mais qu'on aura la possibilité grâce à les jetons d'une blockchain de faire vivre la démocratie différemment. L'idée d'une démocratie liquide, c'est une idée d'un vote qui ne serait pas permanent. Imaginez la réforme suivante sur l'école, qui est un bon exemple car personne n'y est jamais arrivé. Dans l'école deux systèmes s'opposent : une démocratie représentative et une démocratie directe. La démocratie liquide efface la distinction entre les deux. Imaginez que je remette des jetons à tous les citoyens et des jetons supplémentaires aux profs et aux étudiants. Imaginez que chacun doive voter pour 5 projets de lois, et faire intervenir les corps intermédiaires — syndicats et associations qui portent traditionnellement la voix des citoyens [NdlR]. On va vous demander soit de déposer directement vos jetons dans l'urne parce que vous savez ce que vous voulez et n'avez pas besoin d'un intermédiaire, soit vous allez dire « moi j'y comprends rien, je fais confiance à … » et vous donnez vos jetons à votre syndicat, votre député,… Et l'on va ainsi inverser le système démocratique et demander à chaque élu et corps intermédiaire de convaincre dans le cadre d'une réforme. Et si vous n'arrivez pas à convaincre vous n'avez pas de représentativité, pas de légitimité pour pouvoir prendre part au débat. Et si vous n'avez pas confiance dans vos corps intermédiaires vous gardez vos jetons, ou vous les donnez à votre député. Ce sont des systèmes qui pourraient à la fois apporter la confiance, mais surtout permettre de créer des consensus très forts et de la cohésion sociale, car les débat ont lieu avant et pendant l'élection. Il y a évidemment une date à partir de laquelle on ne peut plus les enlever. C'est expérimenté aujourd'hui à très petite échelle. Il ne manquait qu'une chose pour les mettre en place, c'est une*

technologie décentralisée. Remettre ses jetons dans une base centralisée, ce serait évidemment une faille, un risque pour la sécurité et la confiance dans le système.

Sylvain Cariou : vous avez parlé de la confiance et donné surtout des exemples dans le monde de la finance. En fait la blockchain dans le monde digital c'est parfait pour la confiance puisque tout ce qui est inscrit est permanent. Mais il y a aussi la capacité à inscrire dans la Blockchain des transactions d'objets physiques par exemple. Donc il y a une difficulté qui est de faire la liaison entre un objet physique et sa représentation dans la Blockchain. Donc soit on trouve des technos pour faire cela — comme avec des puces RFID non reproductibles — soit on met en place des vérifications par des organismes de contrôle et d'audit.

Vous avez également parlé des contrats dont on enregistre le hash dans la Blockchain. On peut se poser les questions : est-ce que ce contrat est bien légal ? Est-ce que les personnes qui l'ont signé étaient bien consentantes et informées ? La Blockchain peut résoudre des problèmes de confiance, mais pas dans toutes les applications. Il y a peut-être des compléments à rajouter.

PD : Merci parce que l'une des remarques qu'on me fait le plus souvent c'est : « Pourquoi la Caisse des Dépôts va là-dedans puisque c'est la mort des notaires ? ». En fait ce qu'on a oublié c'est que le notaire a la charge de s'assurer du « consentement éclairé des partis en présence », et chaque mot a son importance dans cette formule. Il y aura toujours des rendez-vous physique de signature ne serait-ce que pour s'assurer que vous n'avez pas compris de travers ce que vous signez, et que vous n'y avez pas été forcé.

PM : Sachez aussi qu'on s'est posé la question en 2016, une fois qu'un « contrat intelligent » (*smart contract*) a été signé sur la Blockchain, de la valeur de ce contrat. Certains ont dit que puisque les deux entités signataires n'ont pas de valeur juridique, le contrat n'avait pas de valeur non plus. Mais il existe une initiative qui

s’appelle *The DAO* qui a proposé de faire une société miroir en Suisse, qui enregistrera à la chambre de commerce une copie des contrats passés sur la Blockchain en présence de la chambre de commerce. L’initiative était louable, sauf qu’on s’est demandé quel était le contrat qui liait cette société miroir avec la Blockchain en soi, et qu’on n’a toujours pas de réponse aujourd’hui puisque la blockchain n’existe pas juridiquement. Deuxièmement sur l’enregistrement des transactions physiques dans la Blockchain, la société Everledger créée en 2015 s’est interrogée sur la possibilité de créer un ADN numérique pour chaque objet, et s’est concentrée sur le marché des diamants. En attribuant un code à chaque diamant, on pourra vérifier son identité lorsqu’une transaction a lieu. En Mai 2017 Everledger a débuté des négociations pour créer pour le gouvernement français un code qui irait avec chaque vin AOC ou AOP. Lorsque vous recevez une bouteille chez vous vous devez pouvoir vérifier sur un registre ouvert que la bouteille est authentique, et connaitre l’ensemble de ses caractéristiques.