

# LES NOUVEAUX ÉQUILIBRES DE LA CONFIANCE

ENTRE ALGORITHMES ET CONTRAT SOCIAL



FONDATION  
**Mines-Télécom**

La Fondation de l'IMT



# ÉDITORIAL

Juin 2017

L'IMT a contribué à ce tout dernier numéro des Cahiers de Veille de la Fondation Mines-Télécom, en coproduisant son séminaire interne de début d'année, sa conférence large public après l'été, et bien sûr ce cahier.

Dans le cadre des missions et de la stratégie de l'IMT, les écoles de l'Institut bénéficient d'une large autonomie scientifique, pédagogique et de recherche pour mener leurs activités en lien avec leurs écosystèmes. Elles se rassemblent autour de certaines thématiques transversales.

Ces grands sujets donnent l'occasion à la Fondation Mines-Télécom et ses partenaires de réaliser un tour d'horizon des nombreuses recherches menées dans les écoles de notre réseau.

Fortement transdisciplinaires, ces cahiers visent à présenter aussi bien les points techniques que les grands enjeux sociétaux, les questions de droit et les questions d'éthique, les fondements économiques comme les réflexions philosophiques.

La confiance, dont on voit l'importance essentielle dans un monde où la quantité d'interactions s'est considérablement accrue, interroge –selon les pays et les cultures– notre rapport aux autres et au monde.

Pour la Fondation Mines-Télécom, la confiance est aussi le lien primordial entre mécènes et bénéficiaires, au cœur de l'acte du don, et le ciment de cette relation mutuelle et durable.

Dans nos écoles, des enseignants-chercheurs de champs disciplinaires différents –philosophie, sociologie, informatique, droit– questionnent les nouveaux équilibres et les nouvelles formes de la confiance à l'ère numérique. Certains de leurs travaux sont mis en exergue ici. Je vous souhaite une excellente lecture de ce 9<sup>e</sup> cahier.

**Christian Roux**

*Directeur de la recherche et de l'innovation de l'IMT*

# SOMMAIRE

## 3. Reconstruction de la confiance

*Faire et avoir confiance*

*L'explosion des transactions*

Interroger la confiance :

une question très actuelle

Qu'est-ce que la confiance ?

*La confiance, socle de la société*

*Un réducteur de complexité*

*Dynamiques de la confiance*

*Réparer et instaurer la confiance*

La confiance en transition

## 9. La confiance à l'ère numérique

*La perte de crédibilité des médias*

*Le rôle des réseaux de confiance*

Blockchain, le protocole de la confiance ?

*La blockchain est une technologie*

*Les blocs de la blockchain*

*La recherche du consensus*

*Les blockchains programmables*

*Où réside la confiance dans la blockchain ?*

Les moments de confiance

*La santé : la confiance au quotidien*

*Gestion des données personnelles*

*La vie privée en mutation*

Considérations économiques

*Jeux de la confiance*

*Risques économiques*

*La commodité confiance*

*Désintermédiaire les plate-formes*

*La confiance, un nouveau bien commun ?*

## 22. La confiance dans les groupes humains

*La technologie peut-elle tout ?*

*L'apprentissage de la responsabilité*

*Le choix des gouvernances*

*L'immuabilité est-elle définitive ?*

La confrontation au réel

La confiance libérée



## Reconstruction de la confiance

Au marché, nous discutons avec ce primeur bio que l'on connaît depuis quelques années et en qui on a toute confiance aujourd'hui. Ses produits sont bons, généreux, de bonne qualité. Nous n'avons pas vérifié toute la chaîne de production car nous avons confiance dans le label Agriculture biologique qui en certifie la provenance, la qualité et la traçabilité, et dans le respect de certaines normes. Après la pesée, nous payons le prix demandé car nous savons que la balance n'est pas truquée – elle est d'ailleurs contrôlée de temps à autres par les services de l'État. L'exactitude des poids et des mesures est un des socles de confiance les plus anciens, qui a permis le développement des transactions commerciales. De son côté le commerçant est assuré d'être payé, soit par la monnaie qu'on lui tend, soit par la carte de paiement d'un organisme bancaire, et la transaction peut s'effectuer. Puis nous nous dirigeons vers un autre marchand qu'un ami nous a recommandé. Après tout, il n'est pas possible de tester tous les commerçants du marché, et la confiance peut se déléguer aussi.

### L'explosion des transactions

Nous vivons également à l'ère numérique dans un monde où la quantité d'interactions quotidiennes s'est considérablement accrue, que ces transactions s'effectuent en face à face ou en ligne, sous notre entier contrôle ou par le biais d'algorithmes. Alors que nous sommes de plus en plus informés et de plus en plus conscients de partager un destin commun, des scandales révélés par des lanceurs d'alerte, ou de fausses informations émises par des sites peu fiables, nous font douter d'un modèle de confiance ancien – celui où elle est externalisée dans des autorités tierces – qui ne serait peut-être plus soutenable.

« Aie confiance... Crois en moi... »

Quand on demande autour de soi ce que le mot *confiance* évoque, ce sont souvent les paroles doucereuses du serpent Kaa qui reviennent en mémoire. À la recherche de repères dans un monde mouvant et inintelligible pour lui, le petit d'homme est prêt à s'abandonner sans méfiance. La confiance nous renvoie en effet souvent à l'enfance, cette période où *« la confiance naît du lien – les tout premiers liens, les liens avec les parents et les proches »* rappelle l'essayiste Michela Marzano, auteure de *Éloge de la Confiance*, *« l'expérience faite pendant l'enfance d'un point d'appui »* sur lequel nous construirons en partie notre vision du monde et des autres.

### Faire et avoir confiance

Dès le matin, c'est en toute confiance que nous sortons de chez nous pour vaquer à nos occupations, et avec un certain degré de confiance que nous laissons notre habitation derrière nous, porte fermée à double tour ou restée ouverte selon les lieux et les époques. Notre confiance en nous, dans la bienveillance des autres, dans la bonne marche du monde, nous fait avancer presque sans crainte et sans risque.

## Interroger la confiance : une question très actuelle

### Les freins de la confiance

- 47% Le fait que mes données personnelles puissent être consultées par quelqu'un d'autre
- 22% L'usurpation de mon identité
- 11% L'utilisation de mes données personnelles à des fins commerciales

La confiance dans le numérique atteint un niveau historiquement bas, selon le 5<sup>e</sup> baromètre de la confiance des Français dans le numérique, présenté en octobre 2016 par l'ACSEL, la Caisse des Dépôts et La Poste. Seulement 37% (-3 points) des personnes interrogées affirment avoir confiance.

Alors que dans notre quotidien la confiance facilite nos actions, notre époque est plutôt empreinte d'une certaine défiance. L'état général de la confiance est régulièrement mesuré au travers de nombreux « baromètres de la confiance » qui permettent d'en suivre l'évolution. L'Institut Gallup pose ainsi la question suivante chaque année depuis 1973 aux Américains : « *Voici une liste d'institutions dans la société américaine. Pouvez-vous me dire quelle confiance vous placez dans chacune d'entre elles ?* » En juin 2015, l'enquête a révélé que la confiance aux USA avait chuté à un plus bas historique sur toutes les grandes institutions, excepté pour le militaire et les PME. Cette crise de confiance, qui trouve ses racines dans la crise économique de 2008, s'étend à présent à tous les domaines : politique, social, éducatif, médiatique, agricole... La confiance se maintient cependant dans deux groupes humains : la famille et la communauté.

À la suite de cette crise économique, des chercheurs de champs disciplinaires différents – philosophie, sociologie, informatique, droit – se sont penchés à nouveau sur la confiance, apparue comme une notion en « requestionnement » possible. Ce thème de recherche avait

été peu exploré en France, et de nombreux textes sur la confiance étaient proposés par des chercheurs en ayant une perception qui pouvait ne pas correspondre immédiatement à celle que nous avons en France. C'est là en effet un des points essentiels pour aborder le sujet : selon les pays et les cultures, la confiance ne s'élabore pas de la même manière, et les mots qui la désignent peuvent apporter des nuances déterminantes : c'est le cas entre la confiance-assurée (*confidence*) et la confiance-décidée (*trust*). Ces visions différentes expliquent pourquoi des systèmes fondés sur la notation poussée des autres sont plus acceptables ailleurs.

Plongeant ses racines dans la sphère privée, évoluant au cours du temps et selon les cultures, liée aux champs économiques et juridiques, la confiance est aujourd'hui régulièrement mise à mal par les abus d'utilisation de nos données personnelles, secouée par les avancées des technologies numériques dans un contexte de mondialisation et de risque d'uniformisation des pratiques, bouleversée par une accélération du temps qui ne permet plus de la construire à pas raisonnables. Il conviendrait de la réparer ou de la restaurer, mais avant tout il faut la comprendre.

## La confiance : trust et confidence

Un seul terme en français semble vouloir contenir toutes les formes de confiance, quand les anglo-saxons ont su faire une distinction, et disposent de deux mots différents. Ce choix met en lumière l'existence de deux mécanismes simultanés, qui sont des mécanismes de réduction de l'incertitude. Il y a d'un côté *confidence*, et de l'autre *trust*.

Prenons un exemple. Nous nous levons chaque matin en faisant confiance à la monnaie. Nous avons confiance dans le système monétaire qui ne va pas s'écrouler du jour au lendemain. Il s'agit d'une confiance de temporalité longue,

confiance dans le système social dans lequel nous vivons. En anglais, on emploiera le mot *confidence*. En français on peut parler de *confiance assurée*\*. Ayant décidé de faire un investissement, l'achat d'une voiture, nous prenons le temps d'écouter les arguments du vendeur. Nous avons été sensible auparavant à la publicité sur le véhicule, et plusieurs avis d'amis nous avaient poussé à envisager cet achat. Nous avons examiné les risques, et nous sommes décidé. Le mécanisme en jeu, qui s'est déroulé à une échelle individuelle, est de type *trust*, ou *confiance décidée*. « Cette distinction conceptuelle est pro-

posée par le sociologue allemand Niklas Luhmann en 1988 », rappelle Armen Khatchatourov, Télécom École de Management (voir ci-contre). « *La confiance assurée est très liée au contrat social, nous dit Luhmann. Notamment, la confiance dans le système politique relève de cette confiance confidence, alors qu'accorder sa confiance à tel ou telle candidat.e, c'est de la confiance décidée, du trust.* » Si ces deux formes de confiance servent à diminuer l'incertitude, elles le font de manière différente. Dans le premier, *confidence*, c'est l'aspect système qui prévaut. « *Comment cela s'agence-t-il ? Il y a un équilibre,*

\* retrouvez les mots du lexique page 27

## Qu'est-ce que la confiance ?

Éminemment ancrée en nous depuis l'enfance, servie à toutes les sauces au risque d'endormir notre vigilance, présentée tour à tour comme le fondement de nos réussites ou le creuset de nos incertitudes, la confiance fait et a fait l'objet de nombreuses réflexions qui ont produit autant de définitions, selon les disciplines, ou selon qu'il est fait référence aux relations interpersonnelles ou aux relations organisationnelles, et ce serait une gageure que de vouloir en énoncer une qui les engloberait toutes. Une approche multi-dimensionnelle est préférable pour la cerner.

« vit », ce qui signifie : « Quand on ne le connaît pas, *l'homme est un loup pour l'homme.* » Pour Marzano, suivant en cela Montesquieu, à *l'origine*, l'homme n'est pas poussé par la crainte mais par le désir de vivre ensemble. En tronquant la citation de sa prémisse, Hobbes veut affirmer que l'homme est un loup pour l'homme à *l'état naturel*, et qu'il faut donc placer sa confiance en son souverain. On voit ici se dessiner un premier équilibre à maintenir, entre la possibilité d'accorder sa confiance à l'autre quel qu'il soit, et la nécessité de déléguer sa confiance à un tiers construit à cet effet.

Les leviers de la confiance

- 29% Le fait que le site (la marque, l'entreprise, etc.) soit connu
- 24% Les labels de confiance
- 17% Les avis des internautes

### La confiance, socle de la société

En cherchant à en visualiser la portée dans notre quotidien, on prend vite conscience du risque ou de l'angoisse qu'il y aurait à son inexistence ou à sa faible présence dans la société humaine. La confiance est en effet une des conditions qui permet notre « vivre ensemble ». Michela Marzano en démontre le lien à partir de l'expression reprise par Hobbes, que l'on croit bien connaître : « *L'homme est un loup pour l'homme* », extraite de la Comédie des Ânes (Plaute). Le texte complet dit en réalité : « *Lupus est homo homini, non homo, quom qualis sit non no-*

Pour le sociologue allemand Georg Simmel, la confiance est « *l'une des forces de synthèse les plus importantes au sein de la société.* » Elle est le ciment qui fait à la fois prendre ensemble des matériaux étrangers, et les lie dans la durée. « *Sans la confiance des hommes les uns envers les autres, la société tout entière se disloquerait – rares, en effet, les relations uniquement fondées sur ce que chacun sait de façon démontrable de l'autre, et rares celles qui dureraient un tant soit peu, si la foi n'était pas aussi forte, et souvent même plus forte, que les preuves rationnelles ou même l'évidence ! – de même, sans la confiance, la circulation monétaire s'effondrerait.* »



*une conjonction pendant laquelle les deux marchent ensemble. Que se passe-t-il si on perd d'un côté ou de l'autre ? Si par exemple la confiance diminue, c'est le désarroi social. Il faut tenir les deux ensemble. »*

Le modèle anglo-saxon offre une autre différence : la confiance y est réputée maintenue par l'énergie des deux parties en présence, ou bien par celle de la communauté. Cela explique la réussite de systèmes comme eBay, où la confiance émerge de la communauté, et non de tiers extérieurs à la communauté.

Ce cahier de veille a bénéficié des travaux de recherche des membres de la Chaire **Valeurs et Politiques des Informations Personnelles**, dont le **deuxième Cahier de recherche** (octobre 2017), après les Identités numériques en 2016, traite des **Marques et labels de confiance**. Citons notamment **Claire Levallois-Barth**, maître de conférences en droit à Télécom ParisTech, qui coordonne cette chaire, **Patrick Waelbroeck**, professeur en sciences économiques à Télécom ParisTech, **Maryline Laurent**, professeure en sciences de l'informatique à Télécom SudParis, tous trois cofondateurs de la Chaire, et **Armen Khatchatourov**, ingénieur de recherche à Télécom École de Management et docteur en philosophie de la technique.

Autour d'une équipe pluridisciplinaire de chercheurs de Télécom ParisTech, Télécom SudParis et Télécom École de Management, la Chaire traite des aspects juridiques, techniques, économiques et philosophiques qui concernent la collecte, l'utilisation et le partage des informations personnelles ainsi que leurs conséquences sociétales. Elle bénéficie du mécénat de l'Imprimerie Nationale, de BNP Paribas, d'Orange, de LVMH, de Dassault Systèmes et d'un partenariat conclu avec la CNIL et la DINSIC.

 [www.informations-personnelles.org](http://www.informations-personnelles.org)

transparence / ouverture

durée de la relation

réputation

partage des valeurs

expériences passées

compétence

intérêts convergents

équité

interdépendance

respect des engagements

absence d'opportunisme

crédibilité

fiabilité

loyauté

disponibilité

cohérence, constance

sécurité

## Un réducteur de complexité

« La confiance est un mécanisme de réduction de la complexité sociale », développe le sociologue allemand Niklas Luhmann dans un livre éponyme de 1968. Nous devons nous résoudre à un certain degré de « faire confiance » parce qu'il est impossible de maîtriser toute la complexité d'une situation. « D'un certain point de vue », précise Michela Marzano, « les êtres humains aspirent tous à vivre dans un monde certain et stable, dans un univers où la confiance et la bonne foi déterminent la conduite de ceux qui les entourent : ils souhaitent pouvoir compter sur les autres, prévoir leurs comportements et avoir des points de repère. » En procédant ainsi, nous sommes amenés à prendre des risques, qu'il faut essayer d'évaluer selon de multiples paramètres.

## Dynamiques de la confiance

Comment la confiance s'établit-elle ? Elle est en mouvement perpétuel, à l'échelle des individus comme des sociétés. Georg Simmel la relie à l'information : « celui qui sait tout n'a pas besoin de faire confiance, celui qui ne sait rien ne peut raisonnablement même pas faire confiance », et ces passages

d'information entre acteurs font souvent appel à la théorie des jeux. Elle n'est jamais acquise – « La confiance se gagne en gouttes, et se perd en litres » écrit Jean-Paul Sartre – elle ne se décrète pas et ne peut être exigée. Elle n'est pas symétrique : faire confiance à quelqu'un ou quelque chose n'implique pas que la réciproque soit vraie, et Michela Marzano ajoute : « elle place d'emblée celui qui fait confiance dans un état de vulnérabilité et de dépendance. » Elle n'est pas nécessairement transitive non plus : si l'on a confiance en A qui a confiance lui-même en B, notre confiance en B peut en découler ou n'avoir pas d'objet, selon les sujets et selon nos rapports avec A.

Enfin, selon que la confiance en jeu est de type confiance-décidée ou de type confiance-assurée, une première distinction s'opère entre les deux sur « le rôle attribué à l'attitude rationnelle des acteurs », explique Armen Khatchatourov. « En contexte de confiance-décidée, c'est la décision en connaissance de cause, ou en tout cas en évaluation rationnelle de risque, qui importe. Pour la confiance-assurée, nous sommes en présence de mécanismes institutionnalisés, de l'interaction dans laquelle le choix rationnel cède la place à une

## Quelques dimensions de la confiance

La transparence fait-elle la confiance ? Elle en est certainement une composante mais ne saurait en être le critère central pour la construire. De même, la confiance en un système technique ne peut être réduite à la sécurité qui y est appliquée. Dans un article de 2011, Anne-Marie Gagné relève dans la littérature scientifique les différentes dimensions de la confiance selon les domaines de recherche : psychologie, sociologie, sociologie des organisations, sciences économiques, marketing...



## La confiance, mécanisme de réduction du risque

La crise de confiance contemporaine est également une perte de confiance dans l'avenir, dans le progrès et dans les technologies. À IMT Atlantique à Nantes, la sociologue Sophie Bretesché rappelle que « le développement exacerbé de la technologie apporte des formes de défiance, sur les ondes, les OGM, les nanotechnologies... ». Elle y coordonne la chaire « Risques émergents et technologies : De la gestion technologique à la régulation sociale ». Le risque est en effet une donnée centrale de nos sociétés, que l'on songe au risque nucléaire, au risque que fait peser le terrorisme sur les démocraties, à ceux qui touchent à la santé, à l'environnement... « La science est un instrument de mesure et de gestion du risque, si les connaissances minimales nécessaires à la compréhension des situations à risques et des alternatives envisageables sont acquises par les individus. Or, la société du risque est devenue un lieu de méfiance généralisé où les profanes, et parfois même les experts, doutent et remettent en question les fondements sur lesquels elle s'est construite. » Dans ce contexte, la chaire étudie les modalités de régulation du risque entre les pouvoirs publics, le savoir scientifique et la sphère citoyenne.

*habitude socialement acquise.» La dynamique des comportements futurs apporte une deuxième distinction entre ces deux types de confiance, qui se tiennent. « Avec la confiance-assurée, l'échec d'une action particulière est attribué aux facteurs extérieurs, sur lesquels l'acteur n'a que peu de prise. S'il s'agissait de confiance-décidée, il est attribué au comportement et aux mauvais calculs de l'acteur par lui-même. »*

### Tout ne se réduit pas au calcul

Tous les calculs ne sont pas rationnels, et il persiste une part de subjectivité. Pour commencer, la confiance ne se mesure pas (facilement) rappelle Michela Marzano : « *en dépit de tout, la confiance ne dépend pas directement de notre volonté d'avoir confiance : elle n'est pas le fruit d'une connaissance objective ; elle ne se fonde pas sur des standards quantifiables.* » Pour Diego Gambetta et Russel Hardin, poursuit-elle, la confiance se définit comme « *un certain niveau de probabilité subjective, ce qui devrait permettre à un individu de croire que l'autre accomplira ce qu'il attend de lui. Faire confiance à quelqu'un signifierait dès lors envisager la possibilité d'une coopération.* »

Avoir et être digne de confiance sont alors liés, dans des intérêts enchâssés entre les deux parties. La confiance repose « *sur le fait que mes propres intérêts sont enchâssés dans les intérêts de l'autre : elle dépend du fait que le bénéficiaire de ma confiance conçoit mes intérêts comme étant partiellement les siens.* » Les boucles de rétroaction de cette confiance interdépendante rendent encore plus difficile un calcul de risque rationnel. Pour Georg Simmel, il existe un « *moment autre* » qui complète le moment cognitif où la confiance se crée, reliant ainsi la confiance et la foi, qui comble la part d'ignorance qu'on a dans la partie en face. Comment alors, si la foi est en jeu, évaluer les preuves de confiance, et déterminer les déviations à un comportement habituel ?

### Délégation de confiance

Le caractère dynamique de la confiance et son rôle de facteur de réduction de la complexité ouvrent la possibilité d'une répartition dynamique dans le temps et dans l'espace des « *briques de confiance* ». Suivre le conseil d'un ami pour aller chez tel primeur au marché, et ne pas en faire soi-même l'évaluation, c'est accepter de construire son « *capital confiance* » à partir de l'observation de celui d'un tiers. Désigner une personne de confiance en tant que patient est un acte fort de délégation de sa volonté, puisqu'on peut aller jusqu'à remettre sa vie entre ses mains.

Un acteur joue un rôle particulier dans cette construction : le *tiers de confiance*. Il représente l'idée que lorsque deux entités ont des difficultés à se faire confiance, elles peuvent avoir recours à un tiers en qui elles placent leur confiance, ce dernier pouvant assurer à l'une ou l'autre des parties, le moment venu, qu'il leur est possible d'effectuer une transaction en toute confiance.

Les difficultés à se faire confiance peuvent être de natures très diverses. Il peut s'agir tout simplement de deux acteurs qui ne se connaissent pas du tout et veulent interagir sans avoir à passer par une longue période de mise en confiance. Le tiers joue là un rôle d'accélérateur de création de confiance. La difficulté peut surgir des bases techniques de la relation de confiance, par exemple lorsqu'il y a obligation qu'une tierce partie détienne un bout de la convention secrète d'une solution de chiffrement. Elle peut découler de la nécessité de rendre disponibles et exploitables à tout moment des documents, le tiers jouant ici un rôle de conservateur. Enfin, l'une ou l'autre des deux parties peut être désireuse de conserver une certaine méfiance envers l'autre, et le tiers opérera comme un pare-feu qui évite de s'exposer trop largement, et ne délivrera au demandeur que les justes données nécessaires de l'autre.

### Réparer et instaurer la confiance

Bien qu'il n'existe pas en droit de définition explicite de la confiance, rappelle Claire Levallois-Barth, on retrouve cette notion dans de nombreux textes juridiques. L'abus de confiance est par exemple présent en droit pénal, la fidélité dans le mariage est liée à la confiance réciproque des époux, la personne de confiance est définie dans le code de la santé publique. La loi n° 2004-575 pour La Confiance dans l'Économie Numérique utilise le terme explicitement dans son titre. Cette loi, qui vise à réglementer l'usage du numérique dans un climat de confiance, se réfère surtout à la dimension de sécurité, notamment dans le cadre des échanges électroniques, des obligations des prestataires et de la valeur juridique des écrits électroniques.

À l'origine, le droit intervient pour protéger la partie faible, et vient réparer une confiance trahie et sanctionner –abus de confiance en droit pénal, perte de confiance en droit du travail... Concernant la protection des données personnelles, la confiance est entendue notamment à travers le principe de loyauté, lui-même non défini et laissé à l'appréciation du juge. Ce principe inscrit dans la loi Informatique et Libertés de 1978, transposition de la directive européenne 95/46/CE, qui sera elle-même remplacée le 25 mai 2018 par le Règlement Général sur la Protection des Données. Le numérique –une pratique encore jeune et en perpétuelle invention– ne pouvant se lier à une confiance-assurée sociale spontanée, le droit dans ce domaine évolue et déplace le curseur de la confiance vers l'individu et plus de confiance-décidée. « *De plus en plus* », explique Claire Levallois-Barth, « *on passe à un droit dont l'objectif devient la régulation du marché, en particulier du marché intérieur numérique, on cherche à instaurer la confiance du consommateur qui est une condition préalable pour assurer une dynamique favorable à l'économie numérique.* »

## La confiance en transition

La pionnière de l'économie collaborative Rachel Botsman rapporte un moment de vérité qu'elle a vécu un jour en repensant aux serviettes de bain laissées négligemment par terre dans sa chambre d'hôtel en la quittant. Elle se faisait la réflexion qu'elle ne se serait pas comportée comme cela chez un hôte Airbnb, qui la noterait et qu'elle notait. Celle pour qui la confiance sera la nouvelle monnaie du XXI<sup>e</sup> siècle, soulignait à quel point cette serviette jetée par terre pourrait ruiner sa capacité à faire de futures transactions dans le cadre de l'économie collaborative en construction. Elle poursuivait en mettant l'accent sur la manière dont les algorithmes, ici ceux de notation interpersonnelle, pouvaient avoir un impact direct sur notre comportement de tous les jours. « *Un nouveau monde de la confiance émerge, celui où elle réside dans les mains des individus, et plus dans celle des institutions.* »

Cet exemple illustre la deuxième ligne de partage entre confiance-assurée et confiance-décidée relevée plus haut. « *La boucle de rétroaction sur nos comportements futurs se resserre, la confiance reposant de plus en plus sur les conséquences des actions des individus* », observe Armen Khatchatourov. Un changement s'opère sous nos yeux. Il se forme un déplacement vers plus de *trust*, vers l'individu. À l'extrémité, ce *trust* devient pur calcul de risque. On peut raisonnablement faire l'hypothèse que le numérique prolonge et accentue cette tendance. D'ailleurs, « *si l'on exa-*

*mine les règlements européens sur les données des personnes, et ceux sur les identités numériques* », poursuit le chercheur, « *on voit dans les versions anglophones que le terme confidence n'apparaît pas, et il ne s'agit pas là d'un problème de traduction, mais bien d'une mise en visibilité de la tendance actuelle.* » S'il y a une crise de la confiance aujourd'hui, porte-t-elle d'abord sur la confiance-assurée ou sur la confiance-décidée ? Si les politiques publiques ou les initiatives privées doivent renforcer la confiance dans le numérique, de quel aspect faut-il prendre soin ?

La transformation numérique apporte à la fois des capacités pour établir ou renforcer la confiance – systèmes de recommandation, gestion d'e-réputation, engouement pour le *fact checking* –, des moyens pour accélérer les phénomènes de défiance – théories du complot, partage de rumeurs – mais également des possibilités de redéfinir durablement les rapports de confiance au sein du corps social. Les chemins possibles ne sont pas anodins. La blockchain par exemple, conçue à l'origine pour des personnes qui ne se faisaient pas totalement confiance, supprime les mécanismes traditionnels de confiance par la mécanique froide de son protocole et de ses algorithmes. Ce faisant, elle pourrait bien atrophier notre capacité d'humains à savoir faire confiance, un risque dont il faudrait se garder.

Histoire d'une image détournée  
(page ci-contre)

### Bibliographie & lectures complémentaires

Éloge de la confiance, Michela Marzano, coll. Pluriel, 2012

La confiance. Un mécanisme de réduction de la complexité sociale, Niklas Luhmann, *Economica*, coll. « Études sociologiques », 2006

Confiance et familiarité – Problèmes et alternatives, Niklas Luhmann 1988 (traduction dans le n°108 de la revue *Réseaux*, <https://goo.gl/IqTuHz>)

Les moments de la confiance. Connaissance, affects et engagements, Albert Ogien et Louis Quéré, *Economica*, coll. « Études sociologiques », 2006.

La confiance dans tous ses états, Éric Simon, *Revue française de gestion*, n° 2007/6

La confiance et le soupçon. Faire des relations publiques à l'ère de l'entreprise « responsable », Anne-Marie Gagné, 2011

The Changing Rules of Trust in the Digital Age, Rachel Botsman, October 20, 2015 <https://goo.gl/B37QVG>

En janvier 2017 est diffusée sur Twitter une image présentée comme ayant été faite par le spationaute Thomas Pesquet lors de sa sortie dans l'espace. Il s'agit en réalité d'une œuvre de l'artiste Robert Jahns, faite en 2012 à partir d'un véritable cliché de l'astronaute Akoshido Hoshide. Las, l'image se propage rapidement sur les réseaux sociaux, et il faudra plusieurs jours avant que l'information de sa véritable provenance n'en rattrape sa trajectoire. Malgré ces explications, il se trouvera de nombreux internautes pour dire : « oui, mais cela aurait pu être lui ». Ici, l'image est faussement attribuée. Ailleurs, ce sont des images délibérément fausses, voire des vidéos, avec des voix approchantes, qui semblent en tout point réelles. Si le phénomène n'est pas nouveau, la différence est que la technique est aujourd'hui suffisamment convaincante pour jeter le trouble et la suspicion. Ne plus avoir confiance dans le réel qu'on perçoit de ses propres sens pourrait être le grand risque de ce XXI<sup>e</sup> siècle.

# La confiance à l'ère numérique

qui ont été pris lorsqu'on leur accordait confiance sont encore plus grands. Le phénomène ne concerne d'ailleurs pas que les textes, mais également les images, les vidéos et même les publicités.

## Le rôle des réseaux de confiance

Notre entourage sur les réseaux sociaux contribue fortement à notre niveau de croyance dans les faits. Il a été ainsi montré, à travers plusieurs expériences récentes sur ces réseaux, que c'est la confiance, ou la défiance, qu'on a dans la personne qui partage une information, qui importe plus pour nous faire adhérer, que la confiance, ou la défiance, que l'on porte dans la source média elle-même. Le design de ces réseaux a également sa part d'influence. Sur Twitter par exemple, autant le partage –sans même y ajouter un commentaire– est très facile, autant les corrections ultérieures ou l'arrêt d'une diffusion de tweet qui ne serait plus pertinent sont quasi impossibles. Il est également très facile de fabriquer de faux tweets, fausses informations ou propos faussement attribués à quelqu'un, et par leur diffusion massive les parer de tous les attributs de la vérité... alternative. Enfin, les algorithmes de ces réseaux contribuent à enfermer l'individu dans une bulle, ou lui ôtent toute velléité à chercher à s'en échapper en accaparant son attention, avec le risque que l'individu se prive des échanges d'information qui engendrent la confiance.

La redistribution des articulations de la confiance entre confiance-assurée et confiance-décidée s'est déjà produite au cours de l'histoire, notamment lors de la naissance de l'imprimerie qui a contribué à affaiblir l'importance des règles quotidiennes issues du religieux, en mettant les connaissances à disposition d'un plus grand nombre et en facilitant leur circulation. Aujourd'hui, c'est encore la question de la production et de la diffusion des savoirs et de l'information, lors d'un changement d'ère, qui fait bouger les équilibres de la confiance.

## La perte de crédibilité des médias

De tous les facteurs minant la confiance, la multiplication ces dernières années de ce qui est communément appelé *les fake news* est le plus préoccupant. La confiance se construit en effet sur la circulation d'informations aptes à réduire la méconnaissance que l'on a de l'autre. Si ces informations sont erronées, les prises de décision qui en découlent sont vouées à échouer, et les risques

Face à ces dégradations des mécanismes de la confiance, la réponse peut aller d'un plus grand effort commun des journalistes et de leur lectorat à vérifier les faits et à identifier ce qu'est une source fiable, jusqu'au choix d'une réponse purement technique consistant à consigner les faits dans un grand registre infalsifiable, qui ferait référence à tout instant pour établir la véracité originelle d'un document.

## Blockchain, le protocole de la confiance ?

**une technologie, dite *trustless* :** la confiance est reportée sur la partie algorithmique et en aucun cas sur les utilisateurs

**de stockage et de transfert :** dans une base de données (distribuée, non modifiable), qui forme le registre des transactions, le grand livre de comptes

**d'actifs immatériels :** la crypto-monnaie bitcoin à l'origine

**de manière transparente :** publique et librement accessible, au moins par ses utilisateurs

**sécurisée :** construite sur un protocole de consensus résistant aux attaques

**protocole :** règles de fonctionnement

**consensus :** moyen de s'accorder sans passer par un vote

**fiable :** impossible à effacer et indestructible, inaltérable

**non modifiable :** horodatée, infalsifiable. On parle d'*immutabilité*.

**sans intermédiaire :** distribuée entre ses participants, pas de tiers de confiance

**distribuée :** pas d'organe central de contrôle. Différents exemplaires du registre existent simultanément sur différents ordinateurs (les nœuds)

La blockchain (publique) par ses caractéristiques techniques

Comme la confiance, la blockchain est multiforme et les mots qui la décrivent ont un sens précis. Le lecteur qui découvre la blockchain est invité à s'emparer de ces mots avant de se reporter à la figure expliquant le mécanisme général d'une blockchain bitcoin page 19.

S'assurer qu'un document (une image, une vidéo, un permis de conduire, un reçu fiscal...) existait sous une forme précise à une date donnée en consultant un registre infalsifiable est à portée de main. Un tel registre existe en effet depuis début 2009. Il s'appelle la blockchain, a été créé à l'origine pour offrir les bases techniques d'une *crypto-monnaie*, et a été appliqué depuis à bien d'autres domaines. Comme toute technologie de rupture, on en entend souvent parler comme d'une solution magique, et à son invocation tout semble dit, alors que rien n'a été dit. Le concept est en effet plus complexe qu'il n'y paraît, et entraîne parfois des discours embrouillés, ce qui est paradoxal pour une technologie qui se donne comme objectif de rétablir la confiance et la transparence dans les échanges.

La blockchain serait-elle le protocole de la confiance à l'ère numérique ? Offre-t-elle toutes les garanties d'une base technique servant à (re)créer la confiance ? Comme pour cette dernière, adoptons une approche pas à pas à travers les multiples dimensions de la blockchain pour nous en assurer.

### La blockchain est une technologie

La blockchain est une technologie, qui assure le stockage et le transfert d'actifs immatériels, de manière transparente,

sécurisée, fiable, non modifiable et sans intermédiaire. Cette technologie offre un caractère tangible à un actif numérique, associe cet actif à un compte (sous une identité pseudonyme, voir page 19), et permet le transfert de cet actif –ou transaction– de son détenteur à une autre personne en assurant que le transfert a effectivement lieu (le destinataire possède l'actif et le précédent propriétaire ne le possède plus), sans qu'aucune fraude ne soit possible.

C'est le projet Bitcoin d'échange de crypto-monnaie pour lequel elle a été conçue à l'origine qui a rendu populaire la blockchain, et sa longévité a permis de démontrer sa grande fiabilité. On compte en juin 2017 plus de 600 crypto-monnaies, dont les différences viennent du schéma d'actions réalisées –le protocole– lors de la formation puis la validation d'une transaction entre les utilisateurs. Il est donc nécessaire de préciser le protocole employé lorsqu'on parle d'une blockchain donnée.

### La blockchain bitcoin

À l'origine de la création de la blockchain bitcoin se trouve le besoin de disposer d'un système de monnaie électronique pair-à-pair dont les utilisateurs n'auraient pas de raison de se faire confiance. Le système est dit « *trustless* », reflétant

Le minage, une activité de création de confiance déportée

La blockchain bitcoin met en œuvre une crypto-monnaie. Chaque transaction (transfert de monnaie) doit être certifiée valide (pour interdire des paiements sans solde, ou doubles...) et ce sont des utilisateurs particuliers qui en sont responsables. Les transactions en attente de validation sont réunies dans des blocs (limités à une taille de 1Mo pour la blockchain bitcoin, soit 2000 à 3000 transactions). Pour que les transactions

d'un bloc soient validées, il faut vérifier par la connaissance des transactions antérieures et la concordance avec les comptes faisant les transactions que les transactions sont réalisables. Ce travail qui consiste à certifier certains éléments (l'authenticité des transactions, l'identité des parties, etc.) sans avoir recours à un intermédiaire de confiance ou à une autorité centrale est également un des éléments de sécurité du système.

Puis le bloc doit être lié à tous les blocs précédents, cette liaison créant l'historique des transactions et l'infalsifiabi-

l'idée que la confiance réside entièrement dans l'algorithme qui sous-tend le protocole.

Le registre construit par la blockchain est un livre des transactions. Il ne conserve pas l'état des soldes de chaque utilisateur, mais l'historique complet des transactions –ici, des échanges atomiques de monnaie, et dans le cas général, de *jetons* ou *tokens*– qu'ils ont effectuées, et cet ensemble est manié dynamiquement pour représenter «l'état actuel du système», les transactions modifiant cet état interne. La confiance dans la véracité du registre s'établit si une majorité des utilisateurs –organisés en un réseau de machines, ou nœuds– s'accordent sur cet état interne, ce qui se fait par la recherche d'un consensus. La confiance ne résulte en effet pas d'une autorité chargée de maintenir le registre des transactions.

Pour établir l'état interne suivant, celui qui prend en compte les dernières transactions, validées, un certain type d'utilisateurs, appelés mineurs (voir ci-dessous), doivent résoudre un défi mathématique dont la complexité a été étudiée pour interdire les fraudes. Leur travail accompli doit obtenir l'assentiment des autres utilisateurs, c'est pourquoi l'on parle de consensus distribué, un consensus de l'ensemble des nœuds sur l'état du réseau. Nul

intermédiaire n'est présent, nul tiers de confiance n'est nécessaire, aucune information centrale n'est utile. Chaque utilisateur peut vérifier l'état interne du registre de manière indépendante et arriver à la même conclusion que les autres utilisateurs.

Le système a la particularité d'être résistant à la censure, la blockchain bitcoin –publique– ne nécessitant pas d'autorisation préalable pour l'utiliser (voir en page 2 les caractéristiques des blockchains qui n'ont pas l'attribut «publique»). Chacun peut diffuser dans le réseau toute *transaction conforme au protocole* en vue de l'inclure dans la blockchain. De même, chacun peut participer à la mise à jour du registre, en procédant au minage. Enfin, la seule chose possible est d'ajouter des (blocs de) transactions au registre. En vertu du protocole il est impossible –ou extrêmement coûteux en terme de ressources nécessaires– de supprimer des informations qui y sont inscrites.

### Les blocs de la blockchain

Toutes les transactions en cours (elles sont en attente d'être validées) sont regroupées au sein d'un bloc de transactions, qui va avoir pour but de se lier aux blocs précédents, formant ainsi une chaîne (un chemin linéaire jusqu'au premier bloc créé, Bloc Genesis, le 3 janvier

Lorsqu'un de ces *constructeurs* de bloc, appelés mineurs, déclare avoir résolu le défi, tous les autres utilisateurs de la blockchain bitcoin peuvent vérifier avec peu de puissance de calcul que ce travail de vérification est correct. Pour que le bloc soit effectivement ajouté à la chaîne –ce n'est pas au mineur de se permettre cette action, et il n'a aucun moyen de prédire qu'il sera choisi– une grande majorité des utilisateurs de la blockchain doit donc valider que l'opération de minage est correcte et réelle, et le mineur choisi touche une récompense, son travail ayant été prouvé.

### Les généraux byzantins

La blockchain est réputée être une technologie de rupture, notamment parce qu'elle apporte pour la première fois la solution à un problème de gestion de confiance dans un environnement non fiable et asynchrone, dit «problème des généraux byzantins». Il s'agit de coordonner la confiance de généraux (les utilisateurs de la blockchain) pour qu'ils se mettent d'accord (consensus, voir page 2) sur un plan de bataille (vérifier la validité des transactions) alors que certains sont des traîtres (ils frauderaient par exemple en effectuant une double dépense).

### L'attaque des 51%

Le système blockchain est construit pour maintenir sa fiabilité même si une part minoritaire de ses utilisateurs envoie des informations erronées dans le but de contourner la vérification de la double dépense. Chaque nœud doit d'ailleurs faire l'hypothèse que tout le reste du réseau est défectueux ou frauduleux. Cependant, si un utilisateur disposait de plus de 50% de la puissance de calcul nécessaire à faire le travail de minage, il pourrait aisément bloquer de nouvelles transactions, dépenser ses actifs plus d'une fois et procéder à d'autres malversations, s'accaparer le travail de minage des autres, en un mot prendre le pouvoir sur la blockchain.

Assez rapidement des mineurs isolés n'ont plus eu aucune chance de résoudre le défi par eux-même, et se sont regroupés en pools, eux-même absorbés en grandes «fermes de minages», la plupart situées en Chine. La puissance de calcul nécessaire pour prendre le pouvoir n'est également plus aujourd'hui accessible à un pool de mineurs, et ces derniers n'auraient pas intérêt à joindre leurs efforts pour l'atteindre car ce serait ruineux. Les mineurs sont en effet rémunérés pour leur travail (en bitcoins) et ont intérêt à protéger le système. Un élément de sécurité supplémentaire...

lité du registre. Pour qu'un tel bloc de transactions soit ajouté à la blockchain –ce qui signifie qu'il a été validé et les transactions qu'il contient avec– le protocole bitcoin exige que cette liaison ait une forme suffisamment précise et rare pour ne pas être trouvée sans un calcul conséquent, et les utilisateurs particuliers chargés de la trouver doivent pour ce faire résoudre un défi mathématique complexe de cryptographie, nécessitant une puissance de calcul très importante. La forme de liaison est rare pour éviter que le système soit submergé de nouveaux blocs simultanés.

2009 à 18h15). Une fois lié, le bloc ne pourra être délié. Modifier son contenu a posteriori sera immédiatement détecté lors de l'ajout des blocs suivants, car c'est son contenu lui-même qui a servi, lors du défi mathématique complexe, à créer la liaison avec les blocs antérieurs jusqu'au premier, et ce de manière unique. Le bloc contient également son horodatage de création.

La formation de nouveaux blocs – on parle de découverte, à l'issue du processus de minage, puisque l'un des mineurs va découvrir la solution du défi mathématique lancé – se fait selon l'ensemble précis de règles inscrites dans le protocole, qui sont conçues pour protéger la blockchain de toute attaque visant à l'altérer frauduleusement, et également pour atteindre rapidement un consensus lorsque par exemple des ramifications de la blockchain pourraient surgir et qu'il faut faire un choix (elle doit rester linéaire).

### L'infalsifiabilité via les signatures

Un élément de sécurité au niveau de chaque utilisateur assure que personne ne peut effectuer une transaction au nom d'un autre. Les transactions sont

en effet signées, de manière unique, selon le principe de la cryptographie asymétrique, robuste et éprouvé, avec un couple de clés publique et privée qui est créé à l'ouverture d'un compte bitcoin (la clé publique est le numéro de compte, ou adresse du compte). Il faut bien sûr que la clé privée ne soit ni perdue (auquel cas les bitcoins de l'utilisateur lui seront à tout jamais inaccessibles), ni révélée. Ces clés privées doivent donc être stockées sur un disque dur externe, et non pas confiées à une plate-forme tierce, ce qui irait à l'encontre du principe de non centralisation (certains l'ont fait dans le passé, et l'ont parfois payé par le vol de leurs bitcoins).

### La recherche du consensus

Un consensus est la procédure qui consiste à dégager un accord sans procéder à un vote formel. Le mécanisme de consensus est essentiel dans le système blockchain car il permet de s'assurer de la véracité du registre et des opérations qui y sont effectuées, sans nécessité de confiance préalable entre tous les acteurs impliqués. On retrouve du reste ce souhait de consensus à plusieurs niveaux. Le premier d'entre eux se produit quand une majorité de

nœuds du système reconnaît qu'un bloc de transactions a été miné dans les règles de l'art et accepte qu'il soit le prochain bloc de la chaîne.

Le second concerne les évolutions possibles d'un protocole. Les utilisateurs d'une blockchain sont très attachés au protocole qui la définit, puisqu'ils l'ont choisie pour ses qualités aptes à créer la confiance par l'algorithme, et à rendre les services qu'ils en attendent. Cependant, il peut arriver qu'une limite technique se fasse jour, ou qu'une erreur de programmation perturbe la belle mécanique. Il existe par exemple une discussion régulière sur la nécessité ou non d'augmenter la taille des blocs de la blockchain bitcoin, et donc le nombre de transactions pouvant être traitées à chaque occasion. On touche là des questions de gouvernance informelle, et en observant les discussions, on constate que les développeurs centraux (Bitcoin Core) font toujours référence auprès des mineurs.

### Les blockchains programmables

D'autres blockchains ont été créées, pour gérer des crypto-monnaies selon des protocoles légèrement différents,

## Passer à l'échelle pour créer un système auquel on croit

Pour qu'une nouvelle technologie soit largement adoptée, elle doit être crédible à plusieurs points de vue. Elle doit notamment être simple d'emploi pour des non-experts, le besoin qu'elle remplit doit être clair, ses bénéfices d'usage doivent être manifestes, ses liens avec les technologies antérieures être sans couture s'ils doivent exister.

La blockchain bitcoin ne remplit pas tous ces critères. Le temps de minage d'un bloc est fixé à 10 minutes, et pour parer à certains risques de dédoublement de la chaîne lors de sa construction, une transaction est considérée effectivement passée quand elle a été enterrée sous 6 blocs, soit une heure avant de bénéficier effectivement de ses bitcoins et faire soi-même une transaction sur cet acquis. Cette condition crée un frein important pour développer des usages plus dynamiques, et bien que ce rythme de 7 transactions par seconde

en moyenne ne soit pas un problème pour ses utilisateurs, la blockchain bitcoin ne peut rivaliser avec le rythme de transactions sur des systèmes de type cartes de crédit, dont certains ont des pics évalués à 20 000 transactions par seconde.

De plus, le travail des mineurs est excessivement consommateur en énergie, même en s'effectuant sur des processeurs optimisés pour ces opérations. Les chiffres ne peuvent aller en s'améliorant puisque le protocole implique que la difficulté, et donc la puissance de calcul nécessaire, aille croissante avec le temps. La technologie blockchain bitcoin est donc réputée peu écologique, et son passage à l'échelle, en l'état actuel de son protocole, n'est pas envisageable. D'autres blockchains ont paramétré leur protocole de manière différente pour pallier ces freins : dans Ethereum par exemple, chaque bloc est validé en 14 secondes environ. Ces blockchains sont destinées également à d'autres types d'usage. L'équilibre doit se faire entre performances, usages et sécurité.

ou encore pour gérer d'autres types d'actifs. L'une d'entre elles, Ethereum, a été proposée en 2014 par un passionné de bitcoin, Vitalik Buterin, qui a eu l'idée d'étendre le principe de la blockchain à une blockchain dite « programmable », au sens où ses transactions sont liées à des programmes autonomes capables d'exécuter automatiquement des conditions définies en amont. Il y a toujours une crypto-monnaie dans la boucle, l'ether, mais ce qui importe est la nouvelle capacité apportée par ces « *smart contracts* » de déclencher automatiquement les termes d'une relation commerciale – la livraison d'un colis une fois une certaine date passée, ou l'ouverture d'une porte d'un logement pour déposer ce colis – sans que les partenaires n'aient besoin d'apprendre à se faire confiance. La confiance recherchée ici est la garantie que les termes du « contrat » ne pourront pas être modifiés. Attention cependant à ce terme de « contrat », car celui-ci n'a rien de juridiques, pour l'instant.

Il s'agit là du troisième cas d'usage de la blockchain, après les transferts d'actifs et la référence à un registre. L'intérêt de cette nouvelle capacité est également de lier la blockchain au monde réel, et notamment aux objets connectés, dont les actions et la sécurité des données qu'ils créent et manipulent pourraient bénéficier d'un regain de confiance. Le protocole de la blockchain bitcoin n'est en revanche plus adapté, car son système de consensus par ce qu'on appelle la preuve de travail (*proof of work*, celui des mineurs qui triment à résoudre leur défi cryptographique complexe) est trop consommateur de ressources énergétiques et de temps. C'est pourquoi Ethereum a prévu, dans sa feuille de route vers ce que Vitalik Buterin imagine être le futur ordinateur mondial, d'adopter une autre preuve : la preuve d'enjeu.

### D'autres preuves pour le consensus

D'autres moyens existent pour établir le consensus entre les utilisateurs sur

l'état interne de la blockchain, d'autres types de preuve. La preuve d'enjeu (*proof of stake*) se réfère à ce qui est en jeu pour l'utilisateur, la part de monnaie (les ethers) qu'il possède : la probabilité qu'un nœud construise le prochain bloc de transactions sera ainsi proportionnelle au rapport entre son solde utilisateur actuel et le total de la monnaie en circulation. Là où avec la preuve de travail, investir dans un ordinateur de minage deux fois plus puissant permet de construire des blocs deux fois plus efficacement, faire sous preuve d'enjeu un dépôt de monnaie deux fois plus important double les chances d'être sélectionné pour construire un bloc.

Il existe de nombreuses variations de ces preuves, comme la preuve d'enjeu déléguée (*delegated proof of stake*), où les nœuds qui décident sont élus, et peuvent être révoqués à tout moment. La preuve de possession donne plus de pouvoir à ceux qui conservent leur monnaie plus longtemps, la preuve d'usage à ceux qui la font circuler le plus. Ces preuves correspondent à autant de protocoles, avec leurs avantages et leurs inconvénients, dans une quête actuelle très foisonnante pour trouver les meilleurs consensus en fonction des applications recherchées, des types de participants et du niveau de rapport de confiance qu'ils possèdent ou qui se révèle à l'usage. Par ailleurs, toutes les preuves de confiance ne concernent pas que le processus de minage. Les mécanismes de preuve à divulgation nulle de connaissance sont utilisés pour les phases d'authentification et d'identification, et apportent la preuve mathématique à une entité « vérificatrice » qu'une proposition est vraie sans révéler autre chose que cette véracité.

### En résumé, où réside la confiance dans la blockchain ?

Elle réside à la fois dans le protocole et dans *les intérêts enchâssés* de l'ensemble des participants – les développeurs, les constructeurs de blocs, les

utilisateurs... – dont aucun ne peut soulever l'échec du système.

Pour susciter la confiance, la blockchain s'appuie donc sur des piliers technologiques (cryptographie asymétrique et systèmes distribués) et sociologiques (consensus distribué sans nécessiter de tiers de confiance), c'est-à-dire sur :

son architecture décentralisée qui repose sur un grand nombre de nœuds dépendant d'organisations variées. Un consensus doit toujours être atteint pour prendre des décisions, et la prise de contrôle par plus 50% des nœuds est extrêmement difficile.

sa disponibilité de service, qui découle de cette architecture composée d'une multitude de nœuds assurant la validation et le stockage de la blockchain.

ses mécanismes d'incitation attractifs, qui créent la masse critique d'un grand nombre de nœuds, issus d'organisations différentes, ce qui contribue à garantir l'indépendance et la disponibilité de la blockchain.

la traçabilité et l'auditabilité de toute la chaîne de transactions. Aucune triche n'est possible.

l'authenticité des transactions passées par pseudonyme : les transactions doivent être approuvées grâce à du matériel cryptographique de sécurité suffisante, dont le niveau de sécurité peut s'adapter avec les avancées technologiques.

la rigidification de la chaîne jusqu'à son origine, qui interdit toute altération ultérieure à quelque endroit de la chaîne.

des mécanismes d'incitation aux bons comportements et de dissuasion des mauvais comportements.

(suite page 16...)

# Une redistribution de la confiance couplant algorithmes et collectifs humains

## Suis-je bien qui je prétends être ?

Pouvoir prouver son identité est un des éléments sur lesquels une relation de confiance peut se construire. D'une vérification initiale en présence physique, à la certification par un tiers de confiance que l'entité en train d'agir correspond bien à la personne physique qu'elle représente, les moyens de valider une identité dans un contexte numérique

sont nombreux. Entre la nécessité due à des réglementations (de type *Know Your Customer* par exemple) et le respect de la vie privée, ils agissent aussi comme une arme à double tranchant. Dans le cas des blockchains publiques, les participants agissent sous *pseudonymat*, ce qui protège dans une certaine mesure l'identité réelle des personnes

impliquées dans une transaction. Des projets existent pour utiliser la blockchain dans des contextes où elle servirait également à délivrer des preuves d'identité, tout en gardant la maîtrise des éléments de preuve divulgués, leur réutilisation possible ou non par les demandeurs, la gestion des consentements et d'options de type *opt-in* et *opt-out*.

## Les phases de confiance lors d'une transaction sur la blockchain bitcoin

### Confiance faible ou forte

En informatique, on distingue deux formes de confiance selon les garanties apportées par les preuves de confiance et leur résistance à la falsification. Il y a en effet une différence entre le besoin de savoir si tel vendeur sur une plateforme livre dans les temps ce qu'on lui commande, et l'assurance que tel contrat signé numériquement entre deux entités aura une valeur juridique le moment venu.

Dans le premier cas, une confiance faible construite sur les éléments de réputation, et sur des techniques d'ana-

lyse comportementale permettant de détecter des déviations par rapport au comportement habituel, est suffisante. Dans le second, les techniques de cryptographie, associées à la confiance dite forte, sont nécessaires.

L'irruption des données massives, des techniques d'apprentissage machine, et la coopération de la multitude sont en passe de changer la donne. Les techniques d'analyse comportementale tous azimuts par des algorithmes survitaminés, couplées à des incitations vers

tout un chacun à attribuer des notes et des scores à ses voisins, sont les bases d'une nouvelle forme d'établissement collectif de la confiance qui peut dériver facilement vers la surveillance de masse. Là encore, l'outil créé pour améliorer la confiance numérique est à double tranchant, et les équilibres qui seront trouvés dépendent de notre prise en compte des nouveaux équilibres de la confiance entre êtres humains.

### Les mots de la confiance...

des racines *\*kred* et *\*bheid*, qui ont donné en grec *πειθω* (*peithō*, persuader, faire croire par des mots), *πίστις* (*pistis*, foi) et en latin *fides*

### croyance

le moment cognitif où on saute le pas, on se met à croire

en germanique : (*ga*)-*trauan* (avoir foi)

en hindi : *bharodâ* et *wiśwaś*, le préfixe *bhar* renvoyant à l'idée de « tout » et *wiś* à celle de « complétude »

en latin : *confidere*, de *cum* (avec) et *fidere* (se fier)

avoir **foi**  
**fidélité**

### crédit

donner crédit à

*Treue* (fidélité), *Trauen* (faire confiance, unir)

*Vertrauen* : confiance, à la fois une disposition et une action. Le préfixe *ver* porte une idée de réciprocité

se fier à quelqu'un ou quelque chose

“ s'abandonner à, se confier, parler avec confiance

“ bonne foi // attendre quelqu'un avec confiance // confiance en la providence

Alicia (pseudonyme A) désire acheter (transaction) quelque chose à Basile (pseudonyme B) en réglant en fractions de bitcoins.

Alicia chiffre sa transaction avec sa clé privée *faite pour cette transaction* et l'émet sur le réseau blockchain bitcoin. Tous les nœuds savent que A a émis une transaction et peuvent grâce à la clé publique associée de A vérifier qu'il s'agit bien de A, et que A peut payer...  
#trans 482169 010001100100...



Manon, Mario et Max sont des utilisateurs particuliers, appelés mineurs, qui vont officialiser les transactions. Ils prennent connaissance des transactions en attente et les réunissent dans un bloc de quelques centaines de transactions.

Ils cherchent à résoudre un défi mathématique consistant à obtenir une forme de bloc bien particulière et rare. Les bits qu'il vont ajouter au bloc pour ce faire dépendent également de la forme des blocs précédents et leur font référence (liaison).

Protection



Transaction

Authentification et Vérification

Création (structure du bloc)

Minage

Basile trouve à l'adresse de son portefeuille bitcoin le paiement d'Alicia, et la transaction de A&B est inscrite sur le registre public

Modifier le bloc plus tard demanderait encore plus d'efforts que ce que Manon a fait, car d'autres blocs arrivent par dessus toutes les 10 minutes, qu'il faudrait modifier aussi. Et tout le monde le verrait facilement.

Protection



Le bloc a été accepté et est donc lié à la chaîne des blocs précédents (Manon est récompensée en bitcoins).



Manon a réussi à construire un bloc dont la forme correspond au défi demandé. Tous les nœuds du réseau bitcoin peuvent vérifier facilement si ce travail est bien fait.



Validation par consensus

### Quelques règlements, lois et normes sur la confiance

Le règlement général sur la protection des données, applicable à partir du 25 mai 2018, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Le règlement européen eIDAS, electronic IDentification And trust Services, entré en vigueur le 1er juillet 2016, instaure un cadre européen en matière d'identification électronique et de services de confiance.

Le décret n°2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique.

La norme ISO/TC 69, «Application des méthodes statistiques» permet une mesure de la confiance et des poids et des mesures fiables grâce aux normes.

### Lectures complémentaires

Noëlle Carlin. Relation de soin, la confiance à l'épreuve du droit. Law. Université Paris-Est, 2014. French. Chapitre : Vocabulaire et grammaire de la confiance, pp 15-52

Cahiers de recherche la Chaire Valeurs et Politiques des Informations Personnelles: Identités numériques (mars 2016), Marques et labels de confiance (octobre 2017)

Ævatar, reprendre le contrôle de son identité numérique (aevatar.com)

*Trust*, le fait d'éprouver de la confiance. Pari sur le comportement coopératif d'un autre. Tristant & Yseult.

en anglais

*Reliance*, sentiment de pouvoir compter sur quelqu'un  
*Reliable*: personne fiable

*Confidence* (latin), le fait de placer volontairement sa confiance. Attente normale et socialement sanctionnée vis-à-vis des autres

confiance intime entre amis (jusqu'au XVII<sup>e</sup> siècle)

confidentialité

*confidere*: confier en dépôt, et ce que l'on confie doit rester inviolé

●●► **confidence** (latin *confidentia*) ●●●●●►

**confiance**



bienveillance // se placer dans un état de vulnérabilité, de dépendance // à quoi/ qui peut-on encore se fier? // être, vivre en confiance // attendre, dormir avec confiance...

## Santé, données personnelles, vie privée : les moments de confiance

Confier ses données de santé  
en toute sécurité

Une donnée de santé – dans le cadre de l'hôpital, ou d'un protocole médical, à ne pas confondre avec des données en provenance de dispositifs de suivi de bien-être, comme des bracelets connectés – n'est pas n'importe quelle donnée. Sa définition en cours en Europe énonce qu'«une donnée de santé est une donnée médicale et/ou relative aux déterminants généraux de la santé se rapportant à l'état de santé d'une personne concernée qui comporte des informations sur sa santé physique ou mentale passée, présente ou future, y compris des informations relatives à son enregistrement pour la prestation de services de santé.»

Tous les prototypes, projets, preuves de concept dans le domaine médical doivent prendre en compte les réglementations établies par de nombreux organismes : l'Agence européenne des médicaments, l'Agence Nationale de Sécurité des Médicaments (ancienne Afsaaps), la Food and Drug Administration, la CNIL et le Règlement Général sur la Protection des Données. Les hébergeurs de données de santé à caractère personnel sont assujettis à l'obtention d'un agrément auprès de l'ASIP Santé, l'agence française de la santé numérique.

### La santé : la confiance au quotidien

Avec l'exploitation des données de santé recueillies en masse auprès des personnes, l'utilisation de systèmes d'intelligence artificielle dans des contextes de diagnostic, y compris prédictif, et l'avènement des robots chirurgiens, pour ne citer que ces quelques exemples, la santé à l'ère numérique change radicalement de forme (voir cahier de veille Humain Augmenté 2015, pp 12-13). Du numérique bien pensé et déployé à bon escient peut *redonner confiance dans le système de santé*. Un opérateur de télécommunication comme Orange a compris très tôt qu'il devait y jouer un rôle, ce qu'il a concrétisé dès 2007 par la création d'**Orange Healthcare**. Ses activités y sont nombreuses : développement du parcours de soins, notamment la transformation digitale de l'hôpital, dont l'optimisation est un enjeu majeur, transformation digitale de l'industrie pharmaceutique, au-delà de la boîte de médicament, dispositifs médicaux communicants pour du suivi continu par le médecin, liens avec les mutuelles et assurances comme le maintien à domicile... Et, socle essentiel de la confiance numérique, proposer une réponse technique sur toute la chaîne de la sécurité des données, tant les cyberattaques sont un risque important pour les hôpitaux – comme on a pu le voir encore en mai 2017 au Royaume-Uni notamment.

La confiance est la base de la relation médicale : secret médical, accès aux soins, consentement, partage des données, suivi du traitement, désignation de la personne de confiance... Enseignant-chercheur à Mines Saint-Étienne, et auteur de *Industrialisation de la santé : Identité, biopouvoir et confiance*, **Bruno Salgues** invite à faire un parallèle utile entre divers cadres conceptuels familiers, en informatique et en théorie de l'innovation, et l'établissement pas à pas de la confiance – envers les thérapies, les médecins, les médicaments, les dispositifs médicaux, les lieux de santé. La confiance se construit en ef-

fet autour d'une certaine logique, et ce parallèle appliqué dans le cas de la santé sera également valable dans le cas de la confiance en général. Parmi ces cadres conceptuels, la théorie de diffusion de l'innovation élaborée par Everett Rogers, dont une des 5 caractéristiques est la *trialability* (capacité à être testé), c'est-à-dire la propension des futurs utilisateurs à explorer les possibilités offertes par une innovation. Par exemple, comment expérimenter l'opération que vous aurez dans quelques temps et vous y diriger en toute quiétude ? Cela peut se faire par l'accès à des patients experts qui ont subi la dite opération dans le passé, ou à l'aide d'outils numériques comme la réalité virtuelle.

Un autre paradigme proposé en 2007, l'approche GEMS (*Get, Enjoy, Maintain, Share*), fondé sur la dynamique des états de fébrilité des communautés, peut servir à expliquer la construction de la confiance en santé. L'acquisition de données (étape *Get*) est un moment crucial : si les logiciels de construction d'image peuvent différer, les informations (x,y,z,t) qu'ils reçoivent en sortie d'IRM doivent être cohérentes quel que soit le matériel. L'étape *Maintain* amène à réfléchir à la manière dont les données sont stockées et retrouvées, et notamment leurs dates de conservation, bien trop faibles aujourd'hui au regard de l'allongement de la durée de la vie.

Enfin, reprenant les travaux d'Anne-Marie Gagné (cf. tableau page 6), Bruno Salgues fait sien et propose d'appliquer à l'étude du domaine de la santé les quatre ensembles constitutifs de la confiance qu'elle a identifiés lors de son analyse des modèles de confiance (voir figure ci-contre).

### Utilisation de la blockchain en milieu médical

Le recueil du consentement des patients dans le cadre d'un essai clinique est une procédure encadrée et réglementée, qui nécessite beaucoup

## Gérer ses consentements

À savoir : la gestion de consentement ne se limite pas qu'au domaine médical. Le développement des objets communicants, et notamment des mobiles, créant des masses de données, implique d'en maîtriser finement les droits d'accès et de valorisation. L'utilisateur doit pouvoir définir qui peut précisément accéder à quelle donnée et dans quelles conditions. Il doit également pouvoir faire confiance dans le fournisseur de service lui proposant cette fonction. Une équipe de recherche d'**Orange** a ainsi développé une solution de gestion de consentement autour d'une blockchain. Démontré dans un cas d'usage médical, le service garantit par exemple au patient que chaque professionnel de santé n'a accès qu'aux données qui sont nécessaires à leur rôle.

➔ [goo.gl/vZCzZp](https://goo.gl/vZCzZp)

*composante attitudinale* : ouverture d'esprit, justice, disponibilité, honnêteté, bienveillance, équité, compétence et expertise perçues...

*composante relationnelle* : communication, interdépendance, continuité, fréquence, existence de routines communes

*composante organisationnelle* : structures de l'entreprise, normes, valeurs, capacités techniques, légitimité

*composante stratégique* : respect des engagements et des promesses, cohérence entre le discours et les actes

Quatre ensembles constitutifs de la confiance.  
D'après Anne-Marie Gagné, 2011, op. cit.

de délicatesse dans la relation médecin – patient, et pour laquelle l'utilisation de la blockchain pourrait apporter un gain d'efficacité et de confiance.

Les consentements éclairés sont en effet encore parfois recueillis sur papier, ce qui pose des problèmes de traçabilité et de fiabilité des données lorsqu'ils doivent être saisis informatiquement (double saisie). Dans le cas où ils sont directement saisis, bien qu'il existe un standard électronique des protocoles (eCRF, ePRO), il s'agit de documents PDF éditables qui doivent toujours être imprimés et signés. Le patient exerce toujours son consentement au protocole proposé en y apposant sa signature. Cependant, les consentements étant demandés en fin de consultation avec un médecin, la pression de l'autorité médicale peut engendrer chez le patient un sentiment de contrainte pour signer un protocole sans avoir pris le temps de bien lire les documents. Par ailleurs, la nature sensible des données impose qu'elles soient recueillies dans des conditions qui protègent la vie privée du patient. Les amendements aux protocoles sont fréquents et chaque nouvelle itération nécessite un nouveau consentement du patient. Le patient ne dispose d'aucun droit sur ses données et l'éventuelle cession de son consentement vers d'autres investigateurs ou des tierces parties. Enfin, un grand nombre d'essais cliniques ne sont pas reproductibles, en partie dû au manque de consistance des données.

Utiliser une blockchain augmente la transparence et la reproductibilité des essais cliniques : *audit trail* de l'essai, du protocole médical initial (qui ne pourra donc être modifié en chemin), gestion des consentements des patients (plus d'inventions de faux patients ou de retraits des patients gênants). La start-up française Stratum a ainsi développé à l'hôpital Hôtel-Dieu (labo épidémiologie) DocChain, un projet pilote de consentement numérique aux protocoles d'essais

cliniques avec horodatage des données des patients ainsi que des étapes du processus de consentement. Chaque mise à jour du dossier du patient (renseignement des informations personnelles, consentements...) est horodatée dans une transaction afin de créer un historique fiable, immuable et auditable des actions du patient.

La blockchain peut trouver de nombreux autres cas d'usage dans le milieu médical, et les expérimentations y font florès : l'échange de données médicales électroniques (IBM Watson et la Food and Drug Administration), la traçabilité et le suivi du matériel hospitalier et des factures, la garantie de l'intégrité des données et médicaments contre la contrefaçon (800 000 décès dus à la consommation de médicaments falsifiés dans le monde chaque année, et 15% des médicaments en circulation sont des contrefaçons), l'accès au dossier médical partagé, l'amélioration de la confidentialité des données patients...

Aux États-Unis, **Accenture** a étudié ce que le déploiement d'une blockchain (privée) par les autorités de santé pourrait apporter aux patients, et comment ce choix coïnciderait avec les objectifs visés par l'administration. Dans ce contexte américain précis, la blockchain pourrait résoudre des contraintes d'interopérabilité qui ont longtemps posé problème à l'industrie de la santé, notamment la nécessité de relier des identités de patients éparpillées et de stocker les informations de consentement. Elle offrirait un moyen pour les fournisseurs d'améliorer leur capacité à comprendre leurs patients, créant ainsi un degré plus large de confiance dans le partage de l'information médicale et une vision cohérente de l'identité des patients. Elle permettrait la création d'enregistrements de soins sécurisés et fiables, dans un dossier de soins créé par les professionnels de la santé et responsabilisant les patients par l'enregistrement de leurs décisions dans une chaîne d'événements.

## Gestion des données personnelles

Nous confions à des prestataires, des réseaux et des plate-formes d'autres données personnelles, comme les données de localisation ou d'historique de navigation, les photographies que l'on prend, les transactions d'e-commerce, les documents administratifs. Ils les analysent pour les classer, les étiqueter, en tirer des enseignements sur nos comportements ou nous proposer des services pour mieux les utiliser. La plupart du temps nous ignorons ce que ces prestataires font de nos données, et nous en ignorons même les possibilités techniques. Une asymétrie s'est installée entre eux et nous, leurs algorithmes ayant acquis un pouvoir d'influence et de maîtrise de nos comportements. Il a été démontré qu'ils peuvent même mettre les individus suffisamment en confiance pour les amener à divulguer encore plus d'informations personnelles.

Pourtant ces données personnelles ne devraient pas être réutilisables de n'importe quelle manière. Elles sont soumises à des règles juridiques, conçues pour assurer la confiance des utilisateurs dans l'économie numérique. Jusque récemment encadrées en France par la Loi Informatique et Libertés, et la directive européenne 95/46/EC, elles seront régies dès le 25 mai 2018 par le Règlement Général sur la Protection des Données, qui s'inscrit dans la continuité de la directive de 1995, tout en ajoutant de nouvelles obligations.

Aux principes clés de protection des données personnelles déjà connus (finalités, qualité et durée de conservation des données, mesures de sécurité et de confidentialité, droits de la personne concernée...) s'ajoutent de nouveaux principes (protection des mineurs, droit à la portabilité des données, *privacy by design*...) qui renforcent le droit fondamental à la protection des données personnelles et, par delà, la confiance du citoyen européen dans les nouvelles technologies. Parmi ces nouveaux prin-

cipes se trouve le principe de responsabilité (*accountability*) qui énonce qu'« à tout moment le responsable de traitement des données doit être en mesure de démontrer qu'il remplit ses obligations légales, notamment qu'il gère les risques d'atteinte aux données personnelles, et a mis en place les outils pour en garantir la protection effective. » Les éléments de démonstration attendus, constitutifs de la confiance, peuvent prendre la forme d'une politique de protection des données, d'un code de conduite ou d'un mécanisme de certification approuvés.

### Rendre lisible la confiance

La confiance numérique ne se limite pas seulement à celle du consommateur. C'est également celle du particulier (et du citoyen, voir page 9). En France, **Le Groupe La Poste** dispose auprès des citoyens d'un capital confiance construit sur deux actifs pour lesquels il est reconnu : la bienveillance et la transparence sur la finalité de ses services. Son service Digiposte est un coffre-fort numérique dédié au particulier, conçu pour rassembler, sécuriser et maîtriser son patrimoine numérique.

### Moins il y a de confiance, moins il y a d'usages

« Il s'agit de ré-équiper le particulier d'un endroit sécurisé, bienveillant, qui n'apporte pas de biais, qui n'a pas de finalité cachée, c'est-à-dire que le gestionnaire de cet espace ne profite pas d'une connaissance de ce qui y est entreposé pour vendre des services en plus. En effet, dès que la personne a un doute sur la finalité des choses, elle perd en confiance », explique Didier Louvet, Directeur de la Confiance Numérique chez Le Groupe La Poste.

Les personnes déposent dans ce coffre-fort leurs documents d'un simple glisser-déposer de leur ordinateur. Elles peuvent également confier leurs logins et mots de passe pour que leur coffre

## Délégué à la protection des données, un nouveau rôle dans l'entreprise

Pour piloter la gouvernance des données personnelles, en vertu du Règlement Général sur la Protection des Données, il est recommandé et parfois obligatoire, selon la taille des organismes, de désigner une personne qui aura en interne un rôle d'information, de conseil et de contrôle. Sensibilisant les collaborateurs aux implications juridiques de l'utilisation des données, elle diffuse la culture de la donnée dans l'entreprise. Il s'agira également pour elle de saisir et d'expliquer les mutations de la confiance à l'ère numérique, et notamment celles liées à la vie privée.

aille récupérer à leur place et en leur nom des informations telles que leurs documents fiscaux ou des données d'e-commerce. L'intérêt pour les particuliers est de disposer de sa donnée personnelle dans son coffre, de la récupérer et surtout de la réutiliser. C'est ce dernier point qui est essentiel : réutiliser la donnée pour la comprendre, pour l'analyser, pour agir et pour réagir.

## **Pouvoir maîtriser ses données augmente la confiance**

Dans un monde de plus en plus transactionnel et relationnel, il faut renvoyer la donnée à d'autres personnes, réalimenter son écosystème... Tout est mis en œuvre pour fluidifier cette (ré)utilisation de la donnée, car fluidifier l'utilisation *contrôlée* de ses données personnelles contribue à augmenter la confiance dans les outils numériques qui la gèrent.

### Transitivité et transfert de confiance

La blockchain a été conçue pour ne plus avoir recours à des tiers de confiance, or ceux-ci sont souvent des institutions anciennes qui souhaitent logiquement perdurer, qui possèdent un réel capital confiance auprès de leurs clients, et peuvent trouver un nouveau rôle dans l'écosystème de la confiance qui

se met en place, ne serait-ce que pendant une phase transitoire. Une évolution possible de l'action de ces tiers de confiance, qui le sont également en tant qu'institutions vis-à-vis d'autres institutions, serait ainsi de mettre en œuvre le principe de transitivité de la confiance, en y adjoignant le respect de la vie privée des clients par le non dévoilement des informations non nécessaires.

C'est une expérience que chacun aura en effet pu faire à la réception d'un hôtel où l'on vous prend parfois votre carte d'identité pour la photocopier, sans que vous ne soyez informé des suites. Un tel document d'identité est précieux et ne devrait pas pouvoir être conservé facilement, d'autant plus qu'il s'agit juste ici de prouver votre identité associée à votre solvabilité et que d'autres moyens pourraient apporter cette confiance à l'hôtelier. De même, présenter un bulletin de salaire à son propriétaire, c'est divulguer trop d'informations alors qu'il s'agit juste de lui prouver qu'on pourra le payer. Connaissant par exemple la bonne réputation de la personne sur un service comme Amazon, croisée avec la connaissance que vous êtes un bon conducteur grâce aux documents d'assurance, et celle que vous possédez bien votre permis, un système de gestion de transitivité de la confiance pourrait apporter à un loueur de voitures les éléments de satisfaction nécessaires,

sans être détaillés – pas de nom, pas de provenance par exemple – pour qu'il accepte de vous louer un véhicule. On établit là une sorte de confiance pré-créée, construite dans un domaine X qui peut s'appliquer, se transférer dans un domaine Y. Techniquement, ceci passe par une analyse des documents écrits, et l'obligation de pouvoir expliquer ce qui a été analysé et compris.

### Apprendre à gérer ces permissions

Le travail de la donnée personnelle nécessite un consentement éclairé. Au Groupe La Poste, qui se positionne dans la transitivité de la confiance, la question de l'ingénierie du management des permissions et du consentement des particuliers est un chantier important : il s'agit de guider le particulier pour qu'il sache comment accepter les requêtes des tiers sur ses informations, comment vérifier qui demande, comment transmettre ces informations. Un système d'intelligence artificielle pourrait gérer ceci en partie, pour simplifier la prise de décision, pour procéder par analogie et pour apprendre des autres.

Comment s'assurer que le particulier a bien compris ce qu'il autorise... sujet difficile qui nécessite sans doute un travail de normalisation. L'enjeu est essentiel : c'est celui de *rendre la confiance lisible et compréhensible*.

## La vie privée en mutation

« La vie privée est traditionnellement perçue comme la possibilité pour un individu de conserver une forme d'anonymat dans ses activités et de disposer d'une capacité à s'isoler pour protéger ses intérêts. Elle est donc intimement liée à la notion de liberté », met en exergue une étude publiée en janvier 2017 par **Wavestone**. Le cabinet de conseil a interrogé 1587 personnes à l'été 2016 dans 6 pays (Allemagne, Chine, États-Unis, France, Italie et Royaume-Uni) et observé que la notion de vie privée était en mutation, et noté une prise de conscience globale des individus, qui se voient de plus en plus responsabilisés. Autre enseignement intéressant, elle est perçue de manière homogène selon les cultures, alors que les réglementations diffèrent dans chaque pays. Par ailleurs,

« l'analyse des résultats du panel a montré que [la notion de liberté] tend à disparaître au profit de la maîtrise des informations. » La vie privée c'est avant tout « avoir le contrôle sur qui peut obtenir des informations sur moi », et en dernier « ne pas être systématiquement identifié dans les espaces publics ».

Soulignant qu'une approche uniquement technique ne suffira pas à protéger la vie privée numérique, l'étude liste 4 principes à retenir : communiquer de manière transparente et explicite en informant sur les données collectées, minimiser et désensibiliser les données personnelles collectées et stockées, garantir aux individus le contrôle sur leurs données personnelles, et mettre en place un modèle gagnant-gagnant affichant clairement les bénéfices engendrés par la collecte et l'utilisation des données, pour l'organisation et pour les individus.

## Considérations économiques

### Jeux de la confiance

Le problème des généraux byzantins (voir page 10) au cœur de la gestion du consensus dans la blockchain est un problème classique de la théorie des jeux. Il n'est pas le seul à être utile pour comprendre les mécanismes de la confiance et en imaginer les évolutions possibles.

Le dilemme du prisonnier met en situation deux complices d'un méfait interrogés séparément et ne pouvant pas communiquer entre eux. S'ils ne se dénoncent pas, ils n'écopent que d'une peine minime, faute de charge. Si les deux se dénoncent entre eux, ils ont tout deux une peine importante. Si l'un coopère et l'autre pas, le premier est libéré et le second purge une peine très lourde. La meilleure situation consiste à ne pas coopérer avec la police. Elle est cependant très risquée, car l'autre est peut-être en train de vous dénoncer. Le seul équilibre est celui où les deux complices se dénoncent mutuellement.

« Le fait que cette situation ne se produit qu'une seule fois est cruciale pour comprendre cet équilibre de défiance », précise **Patrick Waelbroeck**, professeur en sciences économiques à Télécom ParisTech. « Si l'on répète cette situation un nombre infini de fois, il s'avère que des équilibres coopératifs émergent où les agents économiques se font confiance. » En effet, dans cette version du dilemme du prisonnier itératif, si un agent décide de dévier unilatéralement, il peut être puni par les autres de telle manière que son gain à court terme ne soit pas rentable par rapport à une collaboration durable. Et l'on observe effectivement des comportements altruistes émerger au fil du temps.

« Un autre jeu », poursuit le chercheur, « est le jeu dit du dictateur, dans lequel un personnage choisit comment diviser un montant financier entre lui et un bénéficiaire anonyme. » Alors qu'on pourrait penser a priori que le premier per-

sonnage serait prêt à tout garder pour lui, il n'en est rien et un grand nombre d'entre eux se montrent équitables, et certains, généreux. La connaissance de l'identité et du profil socio-économique des joueurs est importante : plus la proximité sociale est proche, plus le montant donné est équitable. « Dans une variante du jeu, appelée jeu de la confiance, le montant donné par le dictateur au bénéficiaire est augmenté arbitrairement, et le bénéficiaire peut redonner tout ou partie du montant reçu. On observe qu'il retourne un montant non nul correspondant à un comportement de réciprocité. Il faut à la fois faire confiance et être digne de confiance. »

### Risques économiques

C'est là sans doute un raisonnement que de nombreuses start-up, développant leurs activités dans le domaine de la confiance, notamment de la blockchain, ou celui des transactions pair-à-pair non nécessairement monétisées, aimeraient avoir avec l'État, avec le législateur ou avec les autorités de régulation. Dans le domaine de la santé numérique, par exemple, où la législation est extrêmement lourde et handicapante, on compte 30% des start-up françaises. Ces entreprises ont besoin d'une confiance réciproque avec les autorités pour pouvoir créer des preuves de concept et des prototypes dans un cadre leur assurant un minimum de sécurité juridique. C'est d'autant plus vrai que ces start-up s'attaquent à des activités auparavant régulées, et l'incompréhension est souvent de mise. De nombreuses voix s'expriment pour multiplier les échanges entre les autorités et ces entreprises défricheuses, et leur permettre de co-construire au fur et à mesure les nouvelles règles de confiance dans l'économie numérique. Il semble nécessaire également de sensibiliser dès maintenant les juristes de demain, en les formant aux technologies de type blockchain, et notamment à l'impact des *smart contracts* qui prendra vite un tour juridique.

## La commodité confiance

Car entre temps la blockchain est en passe de devenir une commodité comme une autre. Des propositions de type *blockchain as a service* (dans le cloud, par exemple Microsoft Azure avec Ethereum) sont apparues, rendant facilement accessibles ces technologies, le développement d'applications liées, et la recherche de nouveaux modèles économiques. Pour de petits acteurs, se présente la possibilité d'inventer des modèles de type *trust as a service*, avec a priori les garanties de transparence, de pérennité et de sécurité offertes par les grands fournisseurs...

## Désintermédiaire les plate-formes

Ceci à condition d'avoir confiance dans ces grands acteurs, ce qui n'est plus toujours le cas. L'intrusion de plus en plus importante de certaines grandes plate-formes dans les données personnelles de leurs utilisateurs, des règles de conditions générales d'utilisation souvent changeantes, ardues à lire et à en comprendre les modifications, des exclusions de ces réseaux parfois perçues comme arbitraires, font que la confiance est souvent érodée, et peine à se reconstruire.

La question porte également sur les algorithmes de ces plate-formes, notamment celles qui visent à mettre en relation des offreurs de services (conducteurs automobiles) et des demandeurs (passagers) et qui ajustent à la fois la rémunération de ces chauffeurs et leur taux de commission en fonction de nombreux critères (proximité, notes attribuées antérieurement aux chauffeurs...). Le Conseil national du numérique s'est déclaré favorable à la création d'une plate-forme de régulation des plate-formes, de manière à historiciser la sécurisation des données, leur lieu de stockage, la stabilité de l'algorithme et la stabilité de la relation commerciale. Dans l'exemple des services de type VTC, cela permettrait aux futurs chauffeurs

de choisir leur plate-forme avec la meilleure estimation possible de leur avenir. C'est le principe ici de la transparence qui crée la confiance.

L'étape suivante consiste à considérer que ces plate-formes sont comme autant de tiers de confiance dans leur domaine, et qu'elles aussi peuvent être... blockchainisées. Des start-up se créent pour attaquer leurs aînées rendues célèbres pour leur capacité à «uberiser» leurs propres ancêtres. L'objectif poursuivi en recréant ces services à base de blockchain est de redonner du pouvoir à la masse des travailleurs indépendants dans ces nouveaux secteurs, leur permettant d'anticiper leurs revenus sans être sujets à des décisions unilatérales, et de construire en commun leurs règles de fonctionnement. Covoiturage, partage ou vente d'objets, locations de chambres, production d'énergie renouvelable, c'est toute une économie avec laquelle nous venons seulement de prendre nos habitudes qui pourrait à nouveau changer de nature.

## La confiance, un nouveau bien commun ?

La blockchain est finalement beaucoup plus qu'une technologie, et qu'une technologie de rupture accompagnant un monde en multiples transitions. Elle possède une capacité de transformation de la société dont la puissance n'a pas encore été suffisamment ressentie. En ce sens, elle nous avertit sur l'importance de la confiance au XXI<sup>e</sup> siècle, qui ne se limite pas à une nouvelle monnaie et serait un bien commun à se créer et à préserver. Pour le théoricien du pair à pair Michel Bauwens, des pistes autres que la *trustlessness* de la blockchain sont à explorer : la *trustfulness* de la confiance transitive, par exemple. C'est cette confiance que l'on retrouve dans les mécanismes et les communautés du *couchsurfing*, ou dans les mécanismes émancipateurs où chacun peut librement allouer son temps et son énergie à la création de communs.

## Lectures complémentaires

Sur les réseaux, on fait davantage confiance à la personne qui partage qu'à la source de l'information, Le Monde, 24 mars 2017, <https://goo.gl/rrIL7W>

Blockchain : état des lieux et prospective, Ethereum France, 13 janvier 2017 <https://goo.gl/c73u61>

Qu'est-ce que la preuve d'enjeu ? Ethereum France, 3 janvier 2017, <https://goo.gl/kzHTLm>

Identité, biopouvoir et confiance, Bruno Salgues, Iste éditions 2017, <https://goo.gl/s4RUot>

Blockchain protocols in clinical trials: Transparency and traceability of consent, Stratum 2017, <https://goo.gl/d3D6sa>

Blockchain : entre risque et innovation, trouver le bon équilibre, Wavestone, décembre 2016, <https://goo.gl/CY3LPS>

eIDAS - en route vers une Europe de la confiance numérique, Wavestone, novembre 2016, <https://goo.gl/6pkLRD>

La vie privée à l'ère du numérique : au-delà de la conformité, un enjeu de confiance, Wavestone, janvier 2017, <https://goo.gl/W3AsNq>



# La confiance dans les groupes humains

ments de confiance. Cette réalité est apparue très nettement en juin 2016 lors d'un épisode qui a marqué la communauté Ethereum et certainement les communautés des autres blockchains.

## Quand un bug grippe la machine

Ethereum se distingue de la blockchain bitcoin à plusieurs points de vue, et notamment par sa capacité à pouvoir « s'étendre » en dehors des cas d'usage de transferts d'actifs, par le biais des *smart contracts*. Fin avril 2016, un collectif plat –sans leaders– propose via un de ces *smart contracts* « d'émuler le fonctionnement d'un fonds de placement, qui pourrait financer et percevoir des fonds d'autres entités ayant des activités sur une blockchain. » Il s'agit d'un morceau de code, aux sources publiques et auditables de tous, autonome et s'exécutant automatiquement selon des conditions qui y sont définies, sans nécessité d'intervention humaine. Celui-ci permet à des investisseurs de voter sur des projets à financer, et a pour nom TheDAO, pour *Decentralized Autonomous Organization*. Avant de débiter son activité, TheDAO rassemble ses forces financières auprès des utilisateurs d'Ethereum sous forme de DAO-Tokens, en contrepartie de droits de vote sur les projets qui seront présentés. Si l'exercice de ces droits de vote s'effectue bien selon les mécanismes *trustless* classiques, les propositions de projets à financer nécessitent tout de même une phase de vérification humaine. Celle-ci est effectuée par des *curators* choisis parmi des personnes très impliquées dans Ethereum et respectées –dignes de confiance– et dont le rôle consiste à s'assurer notamment que les projets émanent de personnes ou d'organisations réelles, et que personne ne possède plus de 50% des droits de vote. Fin mai 2016, à l'issue de la levée de fonds, l'enthousiasme était de mise pour ce premier exemple concret d'organisation autonome décentralisée.

## La technologie peut-elle tout ?

Pendant quelques années après l'invention de la blockchain, l'idée que la confiance pourrait à présent reposer uniquement sur la solidité et la subtilité d'algorithmes conçus à cet effet, cette vision de mécanismes efficaces dits *trustless*, s'est peu à peu transformée en idéal parmi la communauté de développeurs et d'utilisateurs, et parfois en dogme. Certes, de nouvelles blockchains étaient proposées suivant de nouveaux protocoles, ce qui pouvaient donner à penser qu'à un moment quelques développeurs d'un projet précédent ne croyaient plus complètement aux choix qui avaient été faits, et désiraient tenter une autre piste. Pour autant les discours montraient que le principe fondamental énonçant que le consensus, la mécanique au cœur d'une blockchain, devait rester de l'unique ressort algorithmique, dans un monde d'humains n'ayant pas besoin de (ou ne pouvant plus ?) se faire confiance, restait immuable.

La réalité est pourtant tout autre. Les humains sont toujours présents et ont besoin régulièrement de ressentir, d'exprimer, de partager, de vérifier des élé-

Il allait malheureusement être de courte durée. TheDAO comportait en effet une faille qui fut exploitée. Alors que 150 millions de dollars en ethers avaient été collectés, une attaque via cette faille le 17 juin permet le détournement de 3,6 millions d'ethers, soit 50 millions de dollars à ce moment. Pour Primavera de Filippi, chercheuse au CERSA et au Berkman Center for Internet & Society de l'Université d'Harvard, et spécialiste reconnue des gouvernances décentralisées, cette date marque le moment de la prise de conscience que « *l'idéal d'une technologie parfaitement trustless n'est rien d'autre qu'un idéal.* » Car les échanges se font rapidement vifs entre les partisans d'une mise à jour du client Ethereum – l'application tournant sur chacun des nœuds Ethereum –, ce qui gèlerait les futurs mouvements de fonds et transactions en provenance de la somme détournée, et ceux proposant de modifier l'état de la blockchain Ethereum pour restaurer l'état originel de TheDAO avant le vol du 17 juin. La première solution a l'avantage de ne pas nécessiter le consensus de l'ensemble de la communauté Ethereum car elle peut être déployée par les développeurs. Mais dans ce cas, la confiance dans la pérennité du code n'en serait-elle pas ébranlée ?

La question posée est celle de l'esprit et de la lettre. Est-ce l'intention originelle du code qui doit être reprise, ou le code, même défaillant, qui doit être conservé ? Pour Primavera de Filippi, cet épisode montre qu'une technologie *trustless* est utopique, et que « *des agents de confiance [développeurs, mineurs et autres utilisateurs] ont un rôle important à jouer quand la confiance dans la technologie est rompue à cause de circonstances imprévues, comme une faille dans le code ou la conception de la blockchain. [...] Cela implique de permettre à ces agents d'intervenir [d'une des deux manières ci-dessus] dans le but de restaurer les garanties originelles du système, et idéalement, de restaurer la confiance dans la technologie.* »

## L'apprentissage de la responsabilité

Finalement cet épisode, qui s'est terminé le 20 juillet – une mesure du temps nécessaire pour être capable de dégager un nouveau consensus – par la scission d'Ethereum en deux chaînes, une reprenant l'état avant le vol, et l'autre n'en faisant rien, a sans doute été une chance pour les communautés de la blockchain, qui ont dû se reposer la question des intentions originelles, non pas du code, mais de la blockchain elle-même. « *Permettre aux gens de collaborer et de se coordonner entre eux d'une façon pair-à-pair, sans autorité centrale* », rappelle Primavera de Filippi, qui poursuit : « *Ce qui était initialement une façon de parvenir à une fin est maintenant devenu une fin en soi.* » Certes la gouvernance centralisée que la blockchain a écartée n'a plus sa place, mais en se déplaçant, en se distribuant au sein de chaque individu participant, elle leur apporte une responsabilité qu'ils ne peuvent pas déporter, « *déléguer sur un morceau de code, si ce sont eux qui font fonctionner ce code.* »

## Le choix des gouvernances

Blockchain bitcoin et Ethereum sont toutes les deux *publiques*, organisées autour de grandes communautés d'utilisateurs, de constructeurs de blocs et de développeurs. Tout le monde peut participer et jouer un des rôles sans demander de permission en entrant.

D'autres protocoles et modes de gouvernance existent. Des acteurs comme les banques ont ainsi déployé des blockchains dites *privées*, auxquelles l'accès est restreint aux seuls testeurs et dont les protocoles peuvent changer en fonction de l'expérimentation. Elles ne servent qu'à tester les usages de type registre, à raccorder des systèmes d'informations entre eux, et plus généralement à appréhender ce qu'est la blockchain, au sein d'un groupe de confiance. Il faut bien prendre en compte que ces acteurs doivent être

en conformité avec un certain nombre de réglementations et qu'ils ne peuvent pas déployer des blockchains sans précaution ni période d'étude, quels qu'en soient les pouvoirs attractifs. Le fait que les utilisateurs d'une blockchain publique ne soient identifiables qu'en tant que pseudonyme est l'un des points de friction. Car ces acteurs opérant dans des contextes régulés ont l'obligation de connaître l'identité de leurs clients. Une gouvernance hybride où certains nœuds seraient publics et d'autres privés, et auraient des droits différents des autres, par exemple en écriture ou en modification du registre, peut être souhaitable. Une telle blockchain est appelée *consortium*, et regroupe parfois quelques dizaines d'acteurs.

## L'immutabilité est-elle définitive ?

L'épisode TheDAO a également eu des impacts sur le caractère immuable et irrévocable des transactions. Doit-il l'être coûte que coûte ? Est-ce une dimension essentielle de la confiance que l'on peut mettre dans cette technologie, ou un certain degré d'adaptation est-il possible, souhaitable, dans un monde où l'erreur humaine est toujours présente ?

Dans le cadre d'une collaboration avec des partenaires académiques, **Accenture** a ainsi proposé une solution technologique pour éditer, écrire ou ôter des blocs dans une chaîne sans la casser, l'objectif principal étant d'éviter les *hard fork*, ces moments où une chaîne n'aurait pas d'autre choix que d'être scindée en deux pour survivre à son esprit et à sa lettre. L'invention, brevetée, consiste en une variation d'une des fonctions de chiffrement actuelles, et ne nécessiterait qu'une mise à jour des clients opérant sur les nœuds pour devenir la norme. Quand une ré-écriture au sein de la chaîne est nécessaire, le processus n'implique pas de retoucher à l'ensemble des blocs plus récents, et peut laisser une « cicatrice », non effaçable, pour indiquer qu'une action corrective a été entreprise à cet endroit.

## La confrontation au réel

### Les objets connectés

Ces gouvernances alternatives et ces possibilités pragmatiques d'édition de blocs sont nécessaires pour apporter certaines des dimensions de la confiance dans le secteur industriel et en particulier pour l'internet des objets. Fin mai 2016, l'Institut de recherche de Toyota annonçait un consortium avec le MediaLab au MIT et quatre entreprises

pour étudier les apports de la blockchain dans la mobilité du futur, et rejoignait la liste d'autres initiatives tentant de lier objets connectés et blockchain. Un des enjeux, et un de leurs projets, est en effet de pouvoir partager des données issues des véhicules autonomes de manière sécurisée et en étant capable d'attribuer la propriété de ces données à chacun des contributeurs. Ce projet s'appuie sur des développements antérieurs au MediaLab concernant la juste répartition des droits d'auteurs entre artistes, dans un contexte où des sociétés d'auteurs, anciennement tiers de confiance, sont critiquées pour leur opacité.

Les blockchains publiques actuelles ne sont pas réellement adaptées aux liens avec les objets connectés. Leurs capacités de stockage de données

sont limitées, et les *smart contracts* ne fonctionnent que sur des données pré-rentrées et figées dans la chaîne, sans pouvoir faire appel à des *API* externes qui fourniraient des données fluctuant dans le temps. Des services, appelés *Oracles*, ont été imaginés pour apporter dans une blockchain des données externes avant qu'un *smart contract* ne se déclenche en les utilisant, ce qui implique que ces oracles soient eux-même dignes de confiance. Certains oracles fonctionnent en fournissant une preuve d'honnêteté garantissant que la donnée entrée dans la blockchain est identique à celle qui a été récupérée par l'oracle sur le serveur qui la délivre –parfait si l'on est sûr de cette dernière–, d'autres en introduisant à nouveau les mécanismes de consensus et en faisant collecter puis envoyer la donnée par une

### La confiance décentralisée, un enjeu de gouvernance

La technologie blockchain porte la promesse de désintermédiation de l'économie : décentralisée, transparente et sécurisée, elle est capable de faire émerger un consensus sans tiers de confiance et permet des transactions entre pairs adhérant et coopérant au système.

Tiers de confiance depuis plus de 200 ans, la **Caisse des Dépôts** s'est rapidement positionnée sur la thématique blockchain, afin d'anticiper cette rupture technologique et d'explorer les opportunités qu'elle offre pour penser les infrastructures numériques de demain.

Afin d'accompagner la place financière et de soutenir les écosystèmes blockchain émergeant en France et en Europe, la Caisse des Dépôts s'est engagée dans une démarche d'innovation et d'expérimentation en coopération au sein du consortium LaBChain, laboratoire collaboratif d'exploration de la blockchain et de ses usages qu'elle a lancé en 2015 et qui fédère aujourd'hui 29 partenaires, institutions financières, assurances, startups et entreprises industrielles.

Les expérimentations réalisées dans ce cadre ont permis de délimiter le champ des possibles et d'identifier les opportunités tout en éclairant certaines limites, qu'elles soient opérationnelles, comme l'interopérabilité avec les systèmes existants, ou juridiques et réglementaires, dans la mesure où seules quelques ouvertures législatives permettent aujourd'hui d'envisager des applications concrètes de la technologie.

Pour Nadia Filali, Directrice des Programmes Blockchain du Groupe Caisse des Dépôts, un des points centraux, et au demeurant le plus complexe à résoudre, réside dans la gestion de la gouvernance des blockchains garantissant le maintien de l'élément essentiel qu'est la confiance distribuée. Nombreux s'intéressent aux blockchains dites de permission ou de consortium qui permettent notamment de résoudre la gestion de l'anonymat des parties prenantes et le problème de passage à l'échelle des protocoles publics.

Cependant si ces dernières permettent de faciliter la définition d'une gouvernance maîtrisable entre acteurs connus, elles font perdre rapidement la notion de confiance distribuée. De même, il est complexe d'envisager les modalités de gouvernance d'une blockchain publique telle que celle du Bitcoin, par exemple, les acteurs participant n'étant pas connus et ne répondant qu'à des principes de gouvernance décentralisée qui nécessitent de revoir nos modèles de pensée jacobins et d'imaginer d'autres modèles de gestion et de répartition de la valeur. Enfin, même si les utilisateurs partagent tous le même registre distribué, certaines fonctionnalités comme les *smart contracts* nécessitent la présence d'«oracles» et de «garants» reconnus, ayant pour mission de faire entrer des informations externes certifiées dans la blockchain. Au-delà de l'exploitation de cryptomonnaies, la mise en place d'infrastructures blockchain imposera donc aux tiers de confiance de réinventer leur rôle, en coopération avec l'écosystème, afin de garantir le bon fonctionnement et la sécurité d'infrastructures décentralisées innovantes.

multitude de participants qui ont tous un intérêt à être honnêtes, d'autres enfin n'ont pas d'autre choix que de collecter une mesure physique en provenance d'un capteur en qui il faut également avoir confiance.

Dans tous ces cas d'usages autour de la propriété intellectuelle ou matérielle, la blockchain est sollicitée pour porter plus que de simples informations de transaction. Cependant il existe un peu de place pour des meta-données, ce que l'on peut utiliser en faisant une transaction vers soi-même, et c'est surtout la fonction d'horodatage qui importe. La start-up Woleet, située à Rennes dans l'incubateur de l'IMT Atlantique, a ainsi lié dans la blockchain bitcoin l'ensemble des diplômes délivrés par cette école en 2017, fournissant aux diplômés un certificat infalsifiable de leur document. «*De la même façon, des données de cadastre numérisées ou des indices de qualité de récolte pour indexer les prix du secteur agro-alimentaire pourraient être inscrites dans le registre Bitcoin*», précise son fondateur Gilles Cadignan. La solution proposée par la start-up permet de faire les manipulations sur la blockchain sans avoir à en connaître les arcanes, par un simple glisser-déposer, ou par un plug-in embarqué dans les logiciels qui en auraient besoin. Le dépôt de preuves est en passe de devenir lui aussi une simple commodité.

### À l'échelle d'un pays

Amélioration du parcours santé, gestion du cadastre, gestion des documents administratifs, mais également traçabilité des biens, gestion simplifiée de la TVA, non falsification des documents d'identité... la technologie blockchain a sur le papier de quoi séduire des États soucieux de moderniser et rendre plus efficace leur administration et les relations avec leurs citoyens. En la matière, l'Estonie fait figure de pionnière. Le pays a en effet développé des partenariats avec divers acteurs blockchain autour des problématiques de sécurisa-

tion de dossiers médicaux, de registres des mariages, d'actes notariés... Plus récemment en avril 2017, la ville de Dubaï a annoncé vouloir utiliser la blockchain pour économiser plus d'un milliard d'euros chaque année sur le traitement des documents tels que les demandes de visa, les paiements de factures et les renouvellements de permis. Ce qui est visé est une appropriation plus fluide de la ville pour ses habitants comme pour ses visiteurs. Cette expérimentation à grande échelle de la blockchain propose une version numérique de la *confiance patte blanche*. Les entrées seront par exemple plus rapides avec des passeports et des visas pré-approuvés, la mobilité plus aisée avec des contrats de location de voiture pré-signés.

La confiance entre les citoyens et leur État ne s'arrête pas à une administration et un quotidien plus fluides. Conscients des mutations de la notion de vie privée (voir page 19), ils souhaitent néanmoins rester maîtres de leur destin, exercer leurs libertés et leurs droits. Parmi ceux-ci se trouve le droit d'exprimer leur opinion dans le cadre d'une décision collective, et les mécanismes de consensus de la blockchain, qui remplacent le vote formel, pourraient bien apporter de nouveaux outils à la démocratie.

En attendant, des expériences de vote profitant de l'immutabilité et l'horodatage de la blockchain ont déjà eu lieu, notamment à grande échelle en France via laprimaire.org dans le cadre de l'élection présidentielle 2017 (170 000 transactions enregistrées sur la blockchain Ethereum). Les principes du vote physique, l'anonymat des votants, la transparence, la fiabilité et l'inaltérabilité des votes, rencontrent en effet les principes techniques d'Ethereum.

### Acceptabilité

La confiance est un bien précieux qui se construit lentement et se détruit rapidement. Pour ne pas risquer de passer par des phases luddites de rejet

des technologies et de la science, il convient de se doter collectivement d'outils d'observation de l'évolution de cette confiance (cf. la *Decision Automation Map*, pour estimer l'évolution de notre confiance-*trust* à accorder dans les robots, évoquée dans le cahier de veille 2016 sur les intelligences artificielles, page 29). Il y a d'ailleurs là un paradoxe de la confiance. Celle-ci passe par plus de transparence et plus d'informations – c'est pourquoi on préconise plus d'éducation au numérique par exemple –, mais en savoir plus a tendance à créer de nouvelles théories complotistes, et donc plus de défiance.

Ceci amène à un autre champ d'étude qui n'a pas encore été assez exploré. Comment la confiance s'élabore-t-elle dans nos neurones? Existe-t-il une biologie de la confiance? Des études suggèrent ainsi que l'ocytocine serait une molécule impliquée dans l'émergence de la confiance, ce qui a été observé lors d'expériences du jeu du dictateur (voir page 20) sous ocytocine par l'économiste Paul Zak au début des années 2000. D'autres expériences ont montré qu'elle y était seulement associée et pas la cause directe, et c'est un champ de recherche toujours ouvert. Ce qui semble acquis en revanche est qu'un certain état interne (comment notre cœur bat, à quel point sommes-nous en alerte...) compléterait les informations provenant de nos sens pour nous faire prendre des décisions en toute confiance.

Pour nous mettre dans ce bon état d'esprit, les designers ont certainement un rôle important à jouer. Telle forme de véhicule nous semble plus sécurisante, tel emballage alimentaire nous semble plus en accord avec la traçabilité qu'on souhaite y associer. De même, le choix des voix, des mots et de la prosodie des agents conversationnels, celui des formes, des textures et des couleurs de la peau des robots, et le design des algorithmes en général, sont essentiels pour nous rendre les technologies plus amicales et dignes de confiance.

## La confiance libérée

Déplacement probable de la confiance-assurée vers la confiance-décidée, évolution nécessaire des tiers de confiance selon de nouveaux principes de gouvernance, ou offrant des services de transitivity de la confiance, construction et propagation de la réputation au sein des réseaux de confiance, irruption de la confiance comme une capacité de transformation de la société, articulations mouvantes entre la force du consensus algorithmé et la nécessité du consensus social, les nouveaux équilibres de la confiance sont bien présents et les ajustements encore nombreux.

Ces mouvements affectent les structures hiérarchiques traditionnelles, soumises à la décentralisation des décisions, à l'émergence de la multitude et à la désintermédiation généralisée. De nouvelles formes de consensus apparaissent, et elles vont, comme l'ont fait avant le web et les mobiles, envahir toutes les strates de la société, et notamment les organisations humaines. Le concept d'entreprise libérée – ces organisations caractérisées « *par un respect des collaborateurs considérés comme des adultes pleinement responsables* » – est déjà ancien, il pourrait se trouver renforcé par l'apport des technologies de la confiance. La start-up Backfeed s'attache ainsi à réinventer le management – après tout, le manager classique n'est-il pas lui aussi une sorte de tiers de confiance, une autorité cen-

tralisée à laquelle on se réfère et auprès de laquelle on a délégué son pouvoir de décision? – en s'inspirant de la blockchain, avec comme objectif de libérer et d'émanciper les collaborateurs.

Dans une telle organisation, ce n'est plus la hiérarchie qui juge de la qualité du travail accompli, mais l'ensemble des contributeurs à travers un mécanisme de consensus appelé preuve de valeur. Les critères d'évaluation sont d'ailleurs totalement subjectifs, le système de valeurs émergeant des actions, actions qui définissent, par la réputation qu'elles engendrent, le poids d'un individu au sein d'un groupe. Chacun est libre de proposer des tâches, qui seront elles aussi évaluées, mais également recensées, documentées et horodatées.

À bien y réfléchir, cette organisation qui responsabilise chaque individu pourra paraître pesante car elle semble forcer à rechercher les bonnes notations. Il faudra au contraire la voir comme une possibilité de lâcher prise et de motiver ses actions individuelles et collectives par la confiance en leur réussite. Elle est peut-être également la solution à un monde du travail qui se déplace vers un monde des activités, multiples et parallèles tout au long de la vie. Dans cette société en transition, faisons confiance dans la créativité et l'imagination du petit d'homme pour écrire les nouvelles lignes de son contrat social. ■

### Références & lectures complémentaires

La fin de l'idéal trustless, Primavera de Filippi, juillet 2016, <https://goo.gl/Q9eW6X>

Unexpected arousal modulates the influence of sensory noise on confidence, Micah Allen Darya Frank D Samuel Schwarzkopf Francesca Fardo Joel S Winston Tobias U Hauser Geraint Rees, octobre 2016, <https://goo.gl/Lc9LFm>

Accenture Debuts Prototype of Editable Blockchain for Enterprise and Permissioned Systems, Accenture, septembre 2016, <https://goo.gl/4DC32s>

Algorithmes, Sciences du Design, novembre 2016, <https://goo.gl/PpClWY>

Comment la blockchain va tuer le management traditionnel, mars 2017, <https://goo.gl/1GjlrT>

## Lexique

**API** : *Application Programming Interface*, interface permettant de se brancher sur une application pour accéder aux données qu'elle produit.

**Auditabilité** : disponibilité d'une preuve de délivrance d'une information, de manière authentifiée et non-répudiée.

**Audit trail** : historique complet d'une transaction.

**Confiance assurée** : confiance se jouant au sein du corps social et de ses institutions mises en place. *Confidence* en anglais.

**Confiance décidée** : confiance se jouant à une échelle individuelle et un cadre de référence plus personnel. *Trust* en anglais.

**Consensus décentralisé** : mécanismes utilisés pour s'assurer que l'ensemble des nœuds d'un réseau disposent des mêmes informations et s'accordent sur un même état interne global.

**Consortium** : désigne une blockchain hybride, non publique, avec des participants ayant des droits différents.

**Crypto-monnaie (Cybermonnaie)** : monnaie électronique sur un réseau informatique pair à pair, ou décentralisée, fondée sur les principes de la cryptographie pour valider les transactions et émettre la monnaie elle-même.

**Decentralized Autonomous Organization** : programme qui scelle dans une blockchain la gouvernance d'une organisation. Contient plusieurs *smart contracts* qui interagissent entre eux.

**Distributed ledger (Distributed ledger technology, DLT)** : désigne les blockchains privées et les consortiums.

**Immuabilité (immutabilité)** : capacité à ne pas être modifiable une fois créé.

**Jeton / token** : nom générique pour désigner l'unité transactionnelle et informationnelle sur une blockchain, sans nécessairement faire référence à la notion de monnaie.

**Ledger** : livre de compte, registre.

**Oracle** : service puisant des données d'une ou plusieurs sources (base de données privées ou publiques, réseaux sociaux...) et les injectant dans les *smart contracts* pour leur exécution.

**Pseudonymat** : capacité à prouver une identité cohérente sans indiquer son nom réel.

**Side chain** : blockchain secondaire rattachée à une blockchain principale, permettant d'augmenter le volume d'informations (normalement limité) pouvant être traité au sein de cette dernière.

**Smart contracts** : programmes autonomes qui exécutent automatiquement les conditions et termes d'un contrat, sans nécessiter d'intervention humaine une fois démarrés.

**Tiers de confiance** : entité habilitée à mettre en œuvre, pour le compte de tiers, des opérations nécessitant la confidentialité et la sécurité des transactions.

**Transaction** : désigne, dans le cadre de ce cahier, une opération de transfert d'informations ou d'actifs entre deux participants.

Pour plus de mots du lexique de la blockchain, voir <https://blockchain-france.net/blockchain-pour-les-nuls/>

## Collaborations possibles avec l'IMT & la Fondation Mines-Télécom

L'Institut Mines-Télécom est un établissement public dédié à l'enseignement supérieur et la recherche pour l'innovation dans les domaines de l'ingénierie et du numérique. À l'écoute du monde économique, l'IMT conjugue légitimité académique et proximité concrète avec les entreprises. Il se positionne sur les transformations numériques, industrielles, énergétiques et écologiques et forme les ingénieurs, managers et docteurs qui seront les acteurs de ces changements majeurs au XXI<sup>e</sup> siècle. Ses activités se déploient au sein des grandes écoles Mines et Télécom sous tutelle du ministre en charge de l'Industrie et des communications électroniques, d'une école filiale et de trois partenaires associés ou sous convention. Les écoles de l'IMT sont classées parmi les toutes premières grandes écoles en France.

La Fondation Mines-Télécom soutient l'IMT dans ses missions en formation, innovation, recherche et prospective. Issue de la transformation de la Fondation Télécom créée en 2008 et reconnue d'utilité publique depuis 2012, la Fondation Mines-Télécom contribue au développement et au rayonnement de l'IMT et de ses écoles.

De multiples formes de collaborations sont possibles avec l'IMT et la Fondation Mines-Télécom. Ces partenariats donnent l'opportunité aux entreprises de participer dans un cadre mutualisé d'échanges et de partage, à d'ambitieux programmes de recherche sur des thématiques stratégiques pour le monde industriel, de partager l'expertise des enseignants-chercheurs, d'accéder au potentiel d'innovation des laboratoires et des incubateurs et d'identifier des talents dans les écoles.

Ce cahier de veille a bénéficié des contributions d'enseignants-chercheurs des écoles de l'IMT :

**Claire Levallois-Barth**, Télécom ParisTech, **Patrick Waelbroeck**, Télécom ParisTech, **Maryline Laurent**, Télécom SudParis, **Armen Khatchatourov**, Télécom École de Management, et **Bruno Salgues**, Mines Saint-Étienne, ainsi que des interventions des chercheurs, partenaires et experts externes invités aux petits-déjeuners du cycle Confiance Numérique de la Fondation Mines-Télécom.

# Les cahiers de veille de la Fondation Mines-Télécom

Les cahiers de veille de la Fondation Mines-Télécom sont le résultat d'études menées conjointement par des enseignants-chercheurs de l'IMT (Institut Mines-Télécom) et des experts industriels. Chaque cahier, qui traite d'un sujet spécifique, est confié à des chercheurs de l'Institut qui réunissent autour d'eux des experts reconnus. Tout à la fois complet et concis, le cahier de veille propose un état de l'art technologique, et une analyse tant du marché que des aspects économiques, sociologiques, juridiques et éthiques, en mettant l'accent sur les points les plus cruciaux. Il se conclut sur des perspectives qui sont autant de pistes possibles de travail en commun entre les partenaires de la Fondation Mines-Télécom et les équipes de l'IMT.

## Fondation Mines-Télécom

37-39 rue Dareau – 75014 Paris – France

Tel.: + 33 (0) 1 45 81 77 46

Directrice des opérations & des programmes  
audrey.loridan-baudrier@fondation-mines-telecom.org

[www.fondation-mines-telecom.org](http://www.fondation-mines-telecom.org)

Avec le soutien des partenaires des programmes de la Fondation :



BNP PARIBAS

NOKIA



accenture

AIRBUS  
DEFENCE & SPACE

CIRPACK

sopra  steria



WAVESTONE

Et le soutien des partenaires du cycle confiance numérique :

