La (ou les) *blockchain*(s), une réponse technologique à la crise de confiance

Par Arnaud MANAS
Ingénieur, docteur en économie et en histoire, chercheur associé à l'Université de Paris I – Sorbonne (IDHES)
et Yoram BOSC-HADDAD
Spécialiste de la gouvernance des initiatives émergentes et du pilotage économique

Dans sa forme canonique, la *blockchain* est un refus des tiers de confiance. Cette technologie repose sur une posture idéologique qui n'est pas exempte de populisme. Ce refus des institutions établies s'explique en partie par la crise de confiance que traversent les sociétés modernes. Le solutionnisme technologique qui voudrait établir la confiance par algorithmes, sans ancrage social ou juridique, est illusoire. Compte tenu des coûts et des risques, l'usage de la *blockchain* canonique (sans tiers de confiance) présente peu d'intérêt en dehors d'un nombre limité de domaines. En revanche, la mise en œuvre des technologies *blockchain* par des institutions dépositaires de confiance, à l'intérieur d'un cadre juridique et social, paraît promise à un bel avenir. Mais seule une veille active permettra à ses acteurs d'en bénéficier pleinement.

Introduction

Créer un cadastre dans l'ancienne République « très très démocratique » du Gondwana après le départ de son président-fondateur ne serait probablement pas tâche aisée. Dans ce pays (imaginaire) bien connu pour sa corruption, la transposition d'une administration « à l'occidentale » serait probablement vouée à l'échec. En effet, les cadastres classiques sont coûteux, peu efficaces, peu résistants à la corruption et leur fonctionnement est relativement opaque. De plus, ils n'ont pas effectué leur mue technologique post-Internet.

Pour d'aucuns, la « révolution de la *blockchain* » permettrait sans nul doute de résoudre le problème. La solution serait de créer un wiki-cadastre transparent et certifié par la communauté informatique mondiale reposant sur la *blockchain* canonique respectant les cinq critères de Caseau-Soudoplatoff [1]. Ainsi, le Gondwana disposerait d'un cadastre moderne sans infrastructure étatique ni tiers de confiance, et ce, pour un faible coût.

Cependant, un tel projet issu du solutionnisme technologique et sans lien avec la réalité sociale risquerait de finir comme un « éléphant blanc 2.0 ». L'acceptation et la diffusion de la *blockchain* repose sur la confiance. Or, cette dernière ne peut être réduite à un algorithme. Une hybridation est donc nécessaire entre les mécanismes traditionnels et les technologies *blockchain*. Celle-ci permettra de surmonter la crise de confiance que traversent les sociétés modernes et d'offrir de nouvelles opportunités technologiques.

Crise de confiance des sociétés modernes et solutionnisme technologique

La *blockchain*, assemblage habile de protocoles et de primitives cryptographiques adossées à Internet, apparaît comme une solution idéale moderne au problème de la confiance. Les solutions sociales (publicité foncière, dépositaires, banques centrales…) qui ont été élaborées par le passé semblent doublement critiquables au nom de l'efficacité et de la perte de confiance dans les institutions.

Il faut reconnaître que les institutions en place sont souvent conservatrices et lentes à profiter des innovations technologiques. De même, la perte de confiance est un phénomène bien réel. Comme le montrent Yann Algan et Pierre Cahuc [2], une méfiance croissante gagne les pays

(1) CASEAU Y. & SOUDOPLATOFF S., « La Blockchain*, ou la confiance distribuée », Fondapol.org, 2016.*
(2) ALGAN Y. & CAHUC P., La Société de défiance : comment le modèle social français s'autodétruit*, ENS, 2007.*

occidentaux, et plus particulièrement la France. La crise financière de 2008 et l'affaire Snowden de 2013 ont singulièrement accentué ce divorce entre les citoyens-consommateurs et les institutions : « *Trust no one* ».

Après le bitcoin, la *blockchain* est apparue comme un recours face à des institutions discréditées. Son caractère « antisystème » et « anti-*establishment* » répond à la renaissance d'un certain populisme. Cette réponse technologique à la crise de confiance qui mine les sociétés modernes repose sur une logique anarcho-libertaire et sur l'imaginaire historique des mineurs d'or individualistes de la Ruée vers l'Or du XIXe siècle. À la croisée du refus de l'État des libertariens et du communautarisme « technophilique », la *blockchain* est l'incarnation contemporaine d'une vision où la conjonction d'intérêts – voire de vices – privés produirait de la vertu publique. Elle s'oppose non seulement à l'État et à la conception régalienne de l'intérêt public, mais aussi aux mécanismes traditionnels de la confiance et de la régulation par le droit.

Il est intéressant de noter que, de manière analogue, la période des années 1930 avait vu se développer de nombreuses initiatives dans le domaine de la monnaie qui ne sont pas sans présenter certains parallèles avec le bitcoin et avec la *blockchain*. En particulier, la monnaie fondante (WIR [3] et expérience de Wörgl [4]) et la technique de l'estampillage, qui ont vu le jour à cette époque, avaient inspiré une littérature considérable. Ces mécanismes sont largement retombés dans l'oubli avec la guerre.

Paradoxalement, la défiance envers les individus et les institutions va de pair avec une confiance dans les systèmes informatiques et dans la technologie algorithmique de la *blockchain*. Cette confiance s'apparente à une foi quasi religieuse dans la mesure où les protocoles et l'économie du système sont difficiles à appréhender. Dans de nombreux esprits, il existe un parallélisme entre la *blockchain* et Facebook. Les deux sont nés de l'Internet social sur lequel, dans une certaine mesure, les « amis » d'un réseau « likent» une transaction, créant ainsi une « multitude anonyme de confiance ».

Dans sa forme canonique, la *blockchain* propose de remplacer des individus ou des institutions dépositaires de la confiance (droits et devoirs) au nom de l'intérêt général par une communauté immatérielle d'individus mus seulement par leur intérêt individuel. Cette approche anhistorique présente des risques.

Un détour par la monnaie

Parmi les institutions sociales, la monnaie fiduciaire est probablement celle qui repose le plus sur la confiance. La monnaie est une lente construction sociale éprouvée par des crises. Elle repose sur des technologies, mais son fondement essentiel est le droit et la construction juridique. La technologie de la monnaie fiduciaire est faillible : le faux-monnayage est une réalité et aucune technique, qu'elle soit typographique, papetière ou autre, n'éliminera les contrefacteurs. Néanmoins, il reste à un niveau socialement acceptable grâce au Code pénal, qui réprime le faux-monnayage, et grâce aux services de police, qui poursuivent les faussaires. À l'opposé, le bitcoin est construit en dehors de l'État et professe une confiance illimitée dans la technologie. Comme le souligne Hayek [5], la conception *a priori* de constructions sociales est périlleuse. La foi aveugle en la technologie pose un problème de responsabilité : si un *hacker* casse le système, personne n'est véritablement responsable ni en charge de la lutte [6]. La formule « *Code is law* » est trompeuse, à cet égard. L'essor du bitcoin repose en partie sur le « dégagisme » bancaire et institutionnel, sur un refus du « système ».

Ce mouvement de défiance qui semble clair depuis plusieurs dizaines d'années correspond peut-être à la phase descendante d'un cycle d'Hirschman [7], selon lequel les sociétés alternent engagement public et repli vers la sphère privée accompagné de défiance sociale. Dans ce cas, le cycle finira par s'inverser et des institutions réinventées retrouveront des formes de confiance [8].

Enfin, il est primordial d'éviter l'écueil du solutionnisme qui part du constat qu'il est naturel de vouloir utiliser le plus largement possible les nouveaux outils indépendamment de leur utilité marginale : « pour un marteau, tous les objets ressemblent à des clous ». Il se pourrait que l'intérêt suscité par la technologie de la *blockchain* soit une manifestation du solutionnisme qui réduit tout problème à la recherche exclusive d'un algorithme, alors que d'autres mécanismes mixtes alliant des dimensions à la fois sociales, juridiques et technologiques pourraient mieux répondre à la question posée.

Des opportunités technologiques pour répondre à la tension croissante entre monopoles institutionnels et aspirations modernes

Faire confiance au darwinisme

Dans le cadre de notre propos, la crise de confiance dans les institutions se nourrit de trois sources :

- Internet porte en germe une vision libertarienne reflétant son émergence soixante-huitarde et son ancrage californien ;
- les institutions en situation de monopole de droit ou de fait, malgré des améliorations et des modernisations notables (comme les actes authentiques électroniques) sont souvent des tiers de confiance inefficaces au regard des aspirations de la société de l'immédiateté, de la transparence et du *peer-to-peer*.

(3) http://www.alpesolidaires.org/le-cercle-de-cooperation-economique-wir-une-monnaie-suisse-depuis-1934
(4) Voir l'article Wikipedia sur Wörgl et http://www.alterinfo.net/L-experience-de-monnaie-fondante-de-Worgl-a-pris-fin-il-y-a-75-ans-Une-solution-pour-des-temps-de-crise_a29371.html
(5) VON HAYEK F., Scientisme et sciences sociales*, Plon, 1953.*
(6) Ethereum Wikipedia et https://bitcoinmagazine.com/articles/rejecting-today-s-hard-fork-the-ethereum-classic-project-continues-on-the-original-chain-here-s-why-1469038808/
(7) HIRSCHMAN A., Bonheur privé, action publique*, Fayard.*
(8) Il est intéressant de noter qu'Airbnb ou eBay avec leur système de notation n'ont fait que reprendre et moderniser l'ancienne technologie de confiance qu'était la lettre de recommandation. De même, on peut trouver un parallèle entre la blockchain *et la suite d'endos qui crée une chaîne ininterrompue de transferts de propriété et de responsabilité.*

Paradoxalement, la multiplication des transactions désintermédiées, au sens classique, mais passant par des plateformes de « confiance » (dont BlaBlacar et Airbnb sont des archétypes) éduquent le consommateur digital à prendre des risques si la valeur perçue lui semble suffisante et si les commentaires sont globalement favorables.

Cette crise et l'espoir de profits élevés à terme conduisent à un foisonnement d'initiatives et d'investissements pour répondre à travers la *blockchain* à des problématiques de transactions C2C, et, par diffusion, B2B ou pourquoi pas X2Y2Z.

Il y a probablement une bulle comparable à l'explosion de l'Internet dans les années 1990 : au minimum ce sont 80 % des *start-ups* de la *blockchain* qui vont mourir [9]. Mais « l'exaptation » – c'est-à-dire le fait qu'un caractère sélectionné, au sens darwinien, par un bénéfice initial finisse par prospérer sur d'autres bases – nous semble un scénario plus probable que l'extinction dans l'œuf.

Les technologies *blockchain* plutôt que la *blockchain*

Nous considérons que les freins que sont la vulnérabilité, la puissance de calcul, les besoins en énergie, l'absence de gouvernance et les conséquences négatives en termes d'emploi [10] vont limiter les « vraies » *blockchains* à peu de cas se situant souvent en marge de la légalité. Nous pensons, en revanche, que les composantes technologiques de la *blockchain* vont permettre, à terme et à une échelle large, de reconstruire des infrastructures de transaction et de partage à moindre coût, et ce, avec des performances très supérieures, en termes :

- d'automatisation (par exemple, agent de transfert pour l'échange de parts de fonds [11] ou les crédits documentaires) ;
- de temps de latence pour l'enregistrement (de quelques mois aujourd'hui, pour la publicité foncière, à quelques millisecondes, demain, avec un contrat automatique) ;
- et, sans doute encore davantage, d'accès transparent et immédiat à une information authentifiée.

Ignorer le foisonnement créatif (ou, pire, le combattre) serait donc prendre le risque de passer à côté du potentiel élevé d'innovation des briques technologiques de la *blockchain*.

C'est dans ce sens que nous interprétons, par exemple, le projet Hyperledger (Linux Foundation) ou l'approche d'Ethereum.

Les scénarios plausibles

Entre le tiers de confiance « canal historique » lent, opaque et inefficace, et le « machin » distribué anonyme dans le *darkWeb*, il y a de la place pour des tiers de confiance réinventés.

Des consortiums vont probablement émerger pour proposer des solutions hybrides, à l'instar de ce qui s'est fait par le passé pour les systèmes de paiement ou de compensation, mais, cette fois, sans opérateurs centralisés, avec une approche du tiers de confiance très différente et des solutions ouvertes et transparentes (à l'instar de ce qu'est un Blablacar ou un Airbnb par rapport à une chaîne d'hôtels ou à un transporteur public).

En revanche, le rythme d'émergence des modèles économiques viables nous semble encore très incertain.

Des impératifs prospectifs pour les institutionnels, pour les opérateurs installés et pour les *start-ups* qui veulent durer

Dans cet environnement, les stratégies extrêmes sont très risquées, et ce, pour tous les acteurs :

- Attendre, c'est prendre le risque de passer à côté d'une disruption réelle ou de continuer à investir massivement dans une infrastructure dont la valeur peut chuter brutalement ;
- Tout miser sur la *blockchain*, c'est combiner risque technologique et risque financier, sauf, bien sûr, pour les *start-ups* et leurs investisseurs, qui viseraient de « pivoter [12] » en se revendant rapidement à un consortium institutionnel.

Il est préférable, dans une logique prospective, de se donner les moyens, d'une part, d'une veille active pour comprendre en profondeur le sujet et, d'autre part, de l'apprentissage par l'expérimentation focalisée et répétée pour se confronter à un monde réel, lui-même en mouvement.

En particulier :

- pour les institutions, il s'agira d'embrasser les besoins de transparence et de vitesse en ayant des stratégies de couverture permettant de contrôler (si possible) les émergences sur les points de faiblesse ;
- pour les *start-ups* qui veulent durer, il nous semble important de cristalliser leur essence comme fournisseurs de briques de savoir-faire technologique ou comme créateurs/développeurs de nouveaux usages ;
- pour tous, il nous semble essentiel de favoriser la création de consortiums d'expérimentation confrontant ces logiques, et d'incubateurs verticaux qui soient des creusets d'émulation et de raffinement des savoirs sur les usages des technologies *blockchain*.

Conclusion

Au vœux de Jean-Paul Delahaye : « Imaginez […] un très grand cahier que librement et gratuitement tout le monde puisse lire, sur lequel chacun puisse écrire, mais qui soit impossible à modifier et indestructible [13] ! », on peut ajouter : « Imaginez des gardiens du registre dépositaires d'une mission d'intérêt général, responsables devant la Loi et la société [14], chargés de l'interprétation des

(9) MOUGAYAR W. : http://www.ibtimes.co.uk/ethereums-william-mougayar-successful-ico-not-indicative-success-ico-1607859
(10) TAPSCOTT in *McKINSEY, May 2016,* How blockchains could change the world.
(11) Les Échos*, « Gestion d'Actif », 4 avril 2017, SCHAFROTH E., « La* Blockchain *s'invite dans la gestion d'actif ».*
(12) Au sens lean start-up.
(13) DELAHAYE Jean-Paul, « Les Blockchains*, clé d'un nouveau monde »,* in Mathématiques et mystères*, Belin, 2016, p. 40*
(14) Le faux en écritures publiques ou authentiques est puni de 10 ans de prison, contre 3 ans pour un faux « ordinaire ».

règles ! ». Croire que les algorithmes règleront tout est illusoire, car l'expertise juridique et la responsabilité sociétale sont nécessaires chez des dépositaires de confiance.

Est-il vraiment nécessaire de choisir entre le dépositaire de confiance « à l'ancienne » et la *blockchain* moderne informatisée reposant sur une communauté immatérielle anonyme ?

En alliant la technologie du registre signé, transparent et accessible sans coût à la confiance envers des individus ou des institutions insérés dans la société, le meilleur des deux mondes est possible.

Laissons donc manches de lustrine, registres jalousement conservés et refus idéologique des tiers de confiance. Préparons-nous à créer un ensemble de technologies et de concepts alliant confiance sociale et algorithmique pour réaliser, avec une signature digitale, des partages horizontaux et transparents, en toute responsabilité et à la vitesse d'Internet.