Juin 2016

LA BLOCKCHAIN, OU LA CONFIANCE DISTRIBUÉE

FONDATION POUR L'INNOVATION POLITIQUE
fondapol.org

Yves CASEAU
Serge SOUDOPLATOFF

FONDATION POUR
L'INNOVATION
POLITIQUE
fondapol.org

www.fondapol.org

LA BLOCKCHAIN, OU LA CONFIANCE DISTRIBUÉE

Yves CASEAU
Serge SOUDOPLATOFF

FONDATION POUR
L'INNOVATION
POLITIQUE
fondapol.org

La Fondation pour l'innovation politique
est un think tank libéral, progressiste et européen.

Président : Nicolas Bazire
Vice Président : Grégoire Chertok
Directeur général : Dominique Reynié
Présidente du Conseil scientifique et d'évaluation : Laurence Parisot

La Fondation pour l'innovation politique publie la présente note
dans le cadre de ses travaux sur *le numérique*.

FONDATION POUR L'INNOVATION POLITIQUE

Un think tank libéral, progressiste et européen

La Fondation pour l'innovation politique offre un espace indépendant d'expertise, de réflexion et d'échange tourné vers la production et la diffusion d'idées et de propositions. Elle contribue au pluralisme de la pensée et au renouvellement du débat public dans une perspective libérale, progressiste et européenne. Dans ses travaux, la Fondation privilégie quatre enjeux : la croissance économique, l'écologie, les valeurs et le numérique.

Le site www.fondapol.org met à disposition du public la totalité de ses travaux. Sa plateforme « Data.fondapol » rend accessibles et utilisables par tous les données collectées lors de ses différentes enquêtes et en plusieurs langues, lorsqu'il s'agit d'enquêtes internationales.

Par ailleurs, notre média « Trop Libre » offre un regard quotidien critique sur l'actualité et la vie des idées. « Trop Libre » propose également une importante veille dédiée aux effets de la révolution numérique sur les pratiques politiques, économiques et sociales dans sa rubrique « Renaissance numérique ».

La Fondation pour l'innovation politique est reconnue d'utilité publique. Elle est indépendante et n'est subventionnée par aucun parti politique. Ses ressources sont publiques et privées. Le soutien des entreprises et des particuliers est essentiel au développement de ses activités.

DÉFINITION DE LA BLOCKCHAIN

La blockchain est une technologie novatrice qui permet à des utilisateurs d'effectuer des transactions, financières ou non, garanties et auditables par tout le monde, sans avoir besoin d'un tiers de confiance.
Après chaque transaction, une nouvelle ligne vient se greffer au bloc, formant une chaîne indéfectible : la blockchain. Elle incarne le livre de compte 2.0, l'historique de chaque transaction étant répertorié dans un registre décentralisé et redistribué. La complexité des algorithmes utilisés rend ces transactions infalsifiables.

RÉSUMÉ

Les grandes innovations sont le fruit du croisement de nouvelles possibilités technologiques et d'un contexte sociologique propice qui transforme ces technologies en usages. Ainsi, la blockchain est née, d'une part, de la rencontre de la cryptographie asymétrique et des systèmes distribués, et, d'autre part, d'un terreau sociologique opportun. Ce dernier résulte de la crise de confiance des citoyens envers les institutions, les amenant à chercher de nouvelles formes de gouvernance.

L'avènement d'Internet a démontré l'effectivité d'un système mondial de communication sans le besoin d'opérateurs de télécommunications. Désormais, il est possible de se connecter en quelques secondes à n'importe quel réseau Wi-Fi dans le monde. La blockchain permet la même révolution, mais appliquée aux transactions. Elle permet à des personnes de réaliser entre elles des opérations, notamment financières, qui sont garanties sans l'interaction d'un tiers de confiance. De ce fait, les échanges sont plus rapides et moins coûteux. Par conséquent, la blockchain remet totalement en question le rôle des institutions, banques, études notariales, et modifie en profondeur l'administration.

Les premières expérimentations, qui vont bien au-delà du bitcoin, comme les organisations décentralisées autonomes, montrent le caractère radicalement disruptif de la blockchain.

LA BLOCKCHAIN, OU LA CONFIANCE DISTRIBUÉE

Yves CASEAU
Membre de l'Académie des technologies

Serge SOUDOPLATOFF
Expert de l'Internet, cofondateur de Sooyoos et Scanderia

Note : *Comme souvent dans le numérique, le sujet des blockchains est très technique. Il n'est pas possible de l'aborder sans faire un détour par quelques explications technologiques. La partie centrale de ce document y est consacrée. Que le lecteur ne s'effraye pas, il peut parcourir sans danger cette piste noire et continuer la lecture jusqu'au bout du document, sans y perdre.*

Il ne se passe pas une journée sans que l'on parle des « blockchains ». Elles ont révolutionné la monnaie avec les bitcoins, et maintenant elles vont « disrupter » les banques, mais aussi les notaires, les avocats, les agents immobiliers, le monde de l'énergie, la santé, la culture, les administrations… Bref, on cherche en vain un pan de l'activité humaine transactionnelle qui ne va pas être impacté par les blockchains. Rien que dans le secteur financier, depuis juillet 2015 les banques suivantes expérimentent la blockchain : BNP Paribas, Société générale, Citi, Deutsche Bank, Westpac, ANZ, Santander, ABE, DBS, Commonwealth Bank, UBS, Barclays, ING, Fidor, etc., et même la Réserve fédérale américaine s'y met. La Caisse des dépôts vient de réunir autour d'elle seize autres institutions (quatre banques, quatre assureurs, cinq industriels et trois partenaires scientifiques) pour créer une place de blockchains[1]. Le gouvernement britannique a écrit un rapport[2], le gouvernement du Honduras teste la blockchain pour son cadastre dans le but d'arrêter la corruption[3], le

1. « La Caisse des dépôts lance officiellement l'initiative de place Blockchain », caissedesdepots.fr, 31 mars 2016 (www.caissedesdepots.fr/la-caisse-des-depots-lance-officiellement-linitiative-de-place-blockchain).

2. Government Office for Science, *Distributed Ledger Technology: beyond block chain*, 2016 (www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf).

3. « A Humble Update on the Honduras Title Project », factom.com, s.d. (www.factom.com/a-humble-update-on-the-honduras-title-project/).

gouvernement estonien l'utilise pour les services notariés de ses e-résidents[4] et le ministre français de l'Économie, de l'Industrie et du Numérique entend « aménager la loi pour tester la blockchain[5] ».

Il ne s'agit pas de projets futuristes encore dans les cartons. Depuis début 2009, année de l'apparition des bitcoins, la blockchain correspondante ne cesse de grandir[6]. La cryptomonnaie bitcoin repose sur un système opérationnel qui a fait ses preuves jusqu'à présent et qui a nécessité pour sa construction bien moins d'effort que les grands systèmes transactionnels, dont certains ont même échoué dans leur mise en service opérationnel après des dépenses énormes.

Si la blockchain n'était, au début, que la technologie qui supportait les bitcoins, il est vite devenu évident qu'elle pouvait être utilisée pour d'autres usages que la cryptomonnaie. De manière synthétique, tout ce qui est transactionnel, financier ou pas, peut se mettre sur une blockchain avec le même principe : garantir la confiance, tout en étant plus efficace, d'une part en offrant une meilleure fluidité et rapidité des transactions, et, d'autre part, en réduisant fortement leurs coûts, tout simplement en éliminant le goulet d'étranglement opérationnel qui se nomme « tiers de confiance ». Ces changements sont suffisamment fondamentaux pour que l'on puisse parler de disruption. Le graphique 1 illustre bien la diversité des usages actuels des blockchains.

Il serait légitime de se demander où se situe la blockchain sur la célèbre « courbe du hype[7] » de Gartner et se dire que nous sommes actuellement en dessous du pic des espérances exagérées et que nous allons bientôt plonger vers l'abîme de désillusion. Sans tomber dans le travers de cabinets de conseils qui prédisent l'avenir plutôt que de le fabriquer, il est sûr que nous ne sommes qu'à l'aube des blockchains, que les deux mécanismes de percolation et d'exaptation qui caractérisent l'expansion du monde du numérique[8] vont fonctionner, et que les usages des blockchains formeront un ensemble très étendu et différent de ce que nous imaginons aujourd'hui.

Mais tout ceci n'enlève rien à l'intérêt qu'il faut y porter. Car la blockchain non seulement représente une véritable rupture en termes d'architecture avec

4. Giulio Prisco, « Estonian Government Partners with Bitnation to Offer Blockchain Notarization Services to e-Residents », 30 novembre 2015 (bitcoinmagazine.com/articles/estonian-government-partners-with-bitnation-to-offer-blockchain-notarization-services-to-e-residents-1448915243).

5. Enguérand Renault et Benjamin Ferran, « Macron aménage la loi pour tester la "blockchain" sur la finance », *Le Figaro*, 24 mars 2016.

6. En cliquant sur le lien blockchain.info/, il est possible de voir les blocs de la chaîne bitcoin défiler en temps réel.

7. Voir l'article « Cycle du hype » sur Wikipédia (fr.wikipedia.org/wiki/Cycle_du_hype).

8. L'exaptation est la capacité de la nature à créer des formes pour résoudre un problème précis, mais qui servent finalement à tout autre chose. Voir Serge Soudoplatoff, « Internet, entre percolation et exaptation », in Martine Behar-Touchais, Nicolas Charbit, et Rafael Amaro (dir.), *À quoi sert la concurrence ?*, Institut de droit de la concurrence, 2014, p. 501-506.

Graphique 1 : Des usages possibles de la blockchain

Source : www.letstalkpayments.com/blockchain-use-cases-comprehensive-analysis-startups-invoved

tout ce que nous offre le monde de la transaction financière (qui, rappelons-le, n'a pas beaucoup changé de paradigme depuis l'invention de la monnaie et de la comptabilité en partie double) et aussi d'autres domaines transactionnels, mais surtout elle s'inscrit dans un contexte qui lui permet de s'épanouir, à savoir la crise de confiance actuelle dans les institutions. Cette combinaison de possibilités technologiques nouvelles et puissantes avec un terreau favorable à la disruption est ce qui fait le succès des grandes innovations.

LE TERREAU : LA CRISE DE CONFIANCE

Nous sommes à l'aube d'une véritable Renaissance. D'un côté, la science et la technologie font d'énormes progrès. Nous découvrons des exoplanètes, nous explorons l'infiniment petit et construisons des ordinateurs quantiques, tout comme à la Renaissance on inventait le parachute, la cale sèche ou bien la perspective en peinture. Nous connaissons maintenant notre place dans l'univers, que nous réussissons à cartographier avec plus de précision, tout comme à la Renaissance nous explorions le monde qui n'avait plus de limites. L'Internet aujourd'hui fait écho à l'imprimerie de la Renaissance. Nous avons les outils pour comprendre le cerveau plus finement, permettant ainsi aux neurosciences de faire des grands progrès, et nous séquençons le génome avec un coût divisé par 30 millions permettant ainsi un meilleur diagnostic de maladies, tout comme, à la Renaissance, André Vésale révolutionnait la médecine en mettant en cause les textes romains anciens et en découpant les corps avec une méthodologie moderne, remplaçant trois personnes par une seule. Mais, tout comme à la Renaissance aussi, l'ordre ancien s'arc-boute sur ses privilèges, refuse de muter et tue l'innovation en la diabolisant afin de garder le pouvoir à tout prix. Nous sommes également à présent dans une phase de régression qui, alimentée par la peur, engendre une phase de répression.

Tout ceci pose le problème fondamental de la confiance. Il ne peut y avoir de transformation s'il n'y a pas de confiance. Le levier de la peur, utilisé justement par ceux qui ont le pouvoir et refusent les mutations, est incompatible avec la confiance. À qui fait-on confiance en 2016 ? Pas vraiment à Google, pas trop à Facebook, à qui on confie de moins en moins de secrets, ni à Apple. On ne fait plus trop confiance aux marques, et on ne fait plus confiance aux États non plus. Même en France, pourtant l'un des pays où la confiance dans l'État est

relativement élevée, celle-ci se dégrade [9]. La confiance aujourd'hui se maintient dans deux milieux : la famille et la communauté. Si demain une guerre éclatait en France, il n'est pas sûr que les jeunes soldats défendraient la patrie, mais ils défendraient sans doute leur famille et leurs copains.

La confiance est un équilibre instable. Lorsque deux personnes se font confiance, il suffit que l'une d'entre elles doute pour que l'autre doute également, et que les deux se retrouvent dans la méfiance réciproque, sentiment, lui, d'un équilibre beaucoup plus stable. Pour maintenir la confiance, il faut donc de l'énergie, et pour faciliter cette énergie, il faut de l'information. Une des grandes ruptures de modèle se situe actuellement au niveau de la provenance de cette énergie. La France s'appuie sur un modèle où l'énergie est externalisée : c'est le juge, le professeur, le manager, les parents, etc., qui sont en charge d'impulser cette énergie. Dans le modèle anglo-saxon, l'énergie vient des deux parties, ou bien de la communauté quand il y a plusieurs personnes. Lorsque eBay est né, il n'était pas le seul site de vente aux enchères, mais il a inventé ce concept de co-notation entre acheteurs et vendeurs, concept que l'on retrouve maintenant dans tous les sites communautaires comme Airbnb, BlaBlaCar, etc. Ce que eBay a compris, c'est que la confiance devait émerger de la communauté, et non pas de tierces personnes extérieures à la communauté, en l'occurrence des experts dans le cas de la vente aux enchères.

On peut discuter sans fin de la validité du modèle de confiance communautaire *versus* le modèle de confiance externalisée. En revanche, dans un monde où la quantité d'interactions explose, il est sûr que le modèle de la confiance externalisée ne peut pas faire face à tout et s'essouffle. La tentation est alors grande pour le régulateur, le tiers de confiance, de réclamer encore plus de moyens afin de faire face à cet accroissement du nombre de transactions ; malheureusement, cette méthode se heurte à la loi des rendements décroissants : à partir d'un certain seuil, plus on augmente les moyens, plus le système devient dysfonctionnel. Le modèle de la confiance dans la communauté, lui, est bien plus « scalable » et permet de faire face à la montée en charge du nombre d'interactions. C'est ce qui fait principalement sa puissance.

Ce que propose la blockchain est un modèle encore plus puissant que le modèle de la confiance communautaire, c'est un modèle où la confiance transactionnelle est fiable, auditable par tous et distribuée grâce à un mécanisme d'obtention d'un consensus décentralisé.

D'une manière générale, la construction de l'Internet est le fruit d'une logique en rupture. Là où les opérateurs de téléphonie construisaient et maintenaient un réseau centralisé, Internet a montré la faisabilité et, surtout,

9. Voir Baromètre de la confiance politique, vague 6bis, réalisé par le Cévipof et SciencesPo, février 2015 (www.cevipof.com/fr/le-barometre-de-la-confiance-politique-du-cevipof/resultats-1/vague6/vague6bis).

la « scalabilité » d'un réseau totalement décentralisé, sans organisme gestionnaire, donc sans propriétaire. Dans sa construction même, on retrouve les mêmes fondamentaux : il n'y a jamais eu de « chef de projet » Internet pour la simple raison qu'il n'y a jamais eu de projet Internet. Internet a été construit par « un ensemble flou auto-organisé de personnes qui s'intéressaient à la construction de l'Internet[10] ». Là où le monde ancien ne se pensait qu'en mode « diffusion », et surtout diffusion de masse, l'Internet a montré que tout le monde pouvait être créateur et diffuseur de contenus – et c'est d'ailleurs une erreur que d'appliquer le modèle de la télévision à Internet. Là où le monde ancien raisonne en logique de « fournisseur vers client », Internet a montré la faisabilité de modèles d'échanges entre pairs à grande échelle.

Tout ceci ne pouvait que s'appliquer un jour au modèle transactionnel : là où le monde ancien pense qu'il faut obligatoirement un tiers de confiance, là où l'Internet 2.0 passe encore par des organismes proposant des plateformes de mise en relations, le modèle de la blockchain montre qu'on peut s'en passer et créer un pur modèle pair à pair (*peer-to-peer* ou P2P). En ce sens, la blockchain est la version transactionnelle des réseaux de pair à pair comme BitTorrent, qui correspondait, rappelons-le, aux fondamentaux de l'Internet à partir de 1968, bien avant l'invention du Web (1991). Ce modèle en pur P2P est différent par cette approche du modèle du fournisseur de contenu (Web 1.0) et de la plateforme de mise en relation (Web 2.0).

LA BLOCKCHAIN

La blockchain regroupe en fait deux choses différentes : une technologie et un système qui utilise cette technologie.

Sur le plan historique, la blockchain est la technologie sous-jacente aux bitcoins. L'invention du bitcoin, fin 2008, avait pour objectif de montrer la faisabilité d'une monnaie basée sur un système de confiance répartie. Il s'agit d'une monnaie cryptée, dont le mécanisme de confiance est basé sur un système où le registre des transactions est réparti entre plusieurs nœuds du réseau. Les algorithmes de cryptage des transactions sont *open source*, ce qui renforce l'idée de confiance dans la monnaie.

10. Cité in Paul Hoffmann (éd.), *The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force* (« The IETF is a loosely self-organized group of people who contribute to the engineering and evolution of Internet technologies »), www.ietf.org/tao.html, 2012.

De facto, le bitcoin est la première démonstration de l'inutilité d'un tiers de confiance, une banque en l'occurrence. Dans notre système traditionnel, une banque est l'organisme garant de la fiabilité et de la sécurité des transactions, donc l'exemple typique d'un tiers de confiance externalisé. Les bitcoins s'échangent sans tiers de confiance, tout en garantissant la sécurité, l'auditabilité et la fiabilité. Le sujet de cette note n'est pas le bitcoin [11], mais la technologie sur laquelle repose le bitcoin : la blockchain. Celle-ci est elle-même basée sur trois piliers : deux sont technologiques, à savoir la cryptographie asymétrique et les systèmes distribués, et le troisième est sociologique, la vision d'un modèle transactionnel dont l'architecture est en mode pair à pair, offrant la possibilité d'un consensus distribué sans nécessité d'un tiers de confiance.

Le premier pilier, la cryptographie, repose sur le concept de clé. Quand elle est symétrique, la clé est possédée par les deux extrémités du message et doit être secrète ; ceci est connu depuis l'Antiquité. L'invention de la cryptographie asymétrique date des années 1970 et consiste à mélanger une clé publique et une clé privée. Cette invention est importante car elle résout le problème de la transmission d'une clé sans avoir besoin d'une institution. Pour illustrer ce mécanisme, prenons l'exemple d'un bien immobilier qui doit changer de propriétaire. Actuellement, un notaire garde le trousseau et garantit le passage d'un propriétaire à l'autre : c'est la clé symétrique. Dans une transaction asymétrique, l'ancien propriétaire met la clé (ou tout autre bien qu'il transfère) dans un coffre qui possède deux serrures et l'expédie au nouveau propriétaire en mettant un cadenas sur une des deux serrures, dont il garde la clé. Le nouveau propriétaire reçoit le coffre, rajoute son propre cadenas à la seconde serrure, dont il garde la clé, et renvoie le coffre au premier propriétaire, lequel retire son propre cadenas et renvoie à nouveau le coffre au nouveau propriétaire, qui peut alors ouvrir le coffre et prendre le bien. À l'arrivée, chacun a gardé sa clé, personne d'autre n'a pu ouvrir le coffre durant les allers-retours car il y avait toujours au moins une serrure de fermée, et il n'y a pas eu besoin d'un notaire.

Le deuxième pilier est la distribution. Il n'y a pas plus belle démonstration de la faisabilité d'un système distribué qu'Internet lui-même. Il n'y a pas besoin d'un opérateur de télécommunication unique pour que toute personne, où qu'elle se trouve dans le monde, puisse se connecter au réseau Internet. Rappelons que la logique du Net est que l'intelligence est aux extrémités et que le réseau lui-même est neutre. Néanmoins, le réseau Internet n'est pas transactionnel par définition, il s'intéresse à la communication, les transactions sont seulement l'un de ses usages.

11. Sur le sujet des bitcoins, voir notamment en.bitcoin.it (en anglais).

Le troisième et dernier pilier de la blockchain, le consensus distribué, est un algorithme qui est en fait la solution d'un problème amusant : celui des généraux byzantins. Considérons une armée éclatée en plusieurs corps d'armée encerclant une ville ennemie. Les différents généraux doivent tous attaquer ensemble pour gagner la ville, car s'ils attaquent séparément, la ville sera plus forte. Ils doivent donc se communiquer de l'information, la plus cruciale étant la date et l'heure de l'attaque, et, ne pouvant pas se rencontrer, doivent pour cela utiliser des messagers. Mais, parmi les généraux, il y a des traîtres qui peuvent fausser certains messages. Par exemple, l'un d'entre eux peut dire à la moitié des généraux qu'il faut attaquer à telle date et à telle heure, et à l'autre moitié qu'il faut se retirer, désunion menant ainsi à la défaite des assiégeants. Jusqu'à l'invention de la blockchain, la doxa disait que le consensus entre les généraux ne pouvait être obtenu qu'avec l'aide d'une autorité centrale qui coordonnait l'ensemble : autorité supérieure ou tiers de confiance. La grande nouveauté algorithmique de la blockchain est de proposer une solution pour obtenir un consensus sans avoir besoin de cette autorité.

La solution, trouvée par l'inventeur du bitcoin, est la suivante : chaque général ne peut envoyer qu'un seul ordre à la fois, qui est horodaté. Mais, surtout, les ordres sont concaténés les uns aux autres, puis cryptés, formant une chaîne stockée dans un « grand livre de transactions », lequel est redistribué à tous les généraux. Ainsi, si un général traître reçoit l'information « on attaque demain à 8 heures », et qu'il décide de ne la répercuter qu'à la moitié des autres généraux et d'envoyer l'ordre de retrait à l'autre moitié, il crée *de facto* deux chaînes incohérentes, et les généraux honnêtes à l'origine de l'information de départ s'aperçoivent de la supercherie.

Une blockchain, c'est donc un grand livre de compte (*ledger* en anglais) crypté, distribué et répliqué dans tous les nœuds du réseau, qui contient les chaînes d'ordre permettant ainsi de gérer la confiance sans institution externe grâce à l'obtention d'un consensus.

Lorsqu'une nouvelle transaction a lieu, ses informations ainsi que son horodatage sont mises dans des blocs de données qui sont intégrés à la chaîne, d'où le nom de « blockchain ». Pour cela, cette chaîne est cryptée et doit être certifiée. Ce travail de certification est effectué par des nœuds du réseau, des ordinateurs qui résolvent les problèmes cryptographiques nécessaires à certifier la transaction. Le travail global de certification se nomme « preuve de travail » (*proof of work*). On appelle les personnes (ou institutions) qui effectuent ce travail des « mineurs[12] ».

12. Dans le même sens que « data mining », l'idée étant de creuser profond pour résoudre un problème. Pour approfondir le concept, voir en.bitcoin.it/wiki/Mining (en anglais).

La preuve de travail est un objet cryptographique que le mineur expose, qui prouve qu'il a passé un certain temps sur le problème, ce qui évite un clonage facile pour transformer un mineur adverse en une armée de clones[13]. Comme la blockchain repose sur le consensus, il est important de garantir des « véritables participants », et ainsi éviter qu'un fraudeur puisse changer la blockchain de manière rétroactive. Le mécanisme est même plus sophistiqué : à intervalles de temps réguliers, la difficulté augmente[14].

Afin d'inciter la fabrication de cette certification, les mineurs sont mis en concurrence, et le premier mineur qui réussit à résoudre le problème de la validation d'un nouveau bloc est récompensé (en bitcoin au début de la monnaie). Au début des bitcoin, ce sont des particuliers qui réalisaient ce travail, en utilisant de manière assez innovante les cartes graphiques des ordinateurs, dont la puissance de calcul est largement supérieure aux processeurs eux-mêmes. Puis sont apparus des ordinateurs spécifiques pour faire le travail de minage de la blockchain. Mais la taille des chaînes augmentant, la puissance de calcul nécessaire est devenue énorme, et ce sont maintenant des institutions qui effectuent ce travail. En mars 2016, il y avait 7 420 nœuds de traitement de la blockchain bitcoin dans le monde[15]. Des entreprises se sont mises sur le marché pour offrir des services de mining à partir de leurs datacenters (*cloud mining*). Néanmoins, le modèle économique pour un particulier est de moins en moins intéressant.

13. Cette idée est due à Adam Back, l'inventeur du protocole Hashcash qui est au cœur de la blockchain. Il est aussi utilisé pour se prémunir des spams. Voir en.wikipedia.org/wiki/Hashcash (en anglais).

14. Pour visualiser la courbe de difficulté, voir blockchain.info/charts/difficulty.

15. Visualisables sur le lien bitnodes.21.co.

La photo suivante montre un centre de minage situé à Boden, en Suède [16].

Crédits photo : KncMinerltc (2016). http://en.kncminerltc.org

En revanche, si la certification des blocs demande de la puissance, la vérification est simple et peut être faite par tout le monde ; il devient donc facile d'obtenir un consensus distribué.

LA TECHNOLOGIE EN DÉTAIL

Ce que la blockchain délivre

La blockchain permet de construire un grand livre de comptes distribué en autant de lieux que souhaité, visible de tous, avec un protocole de mise à jour selon un principe transactionnel également distribué et garanti par une communauté, sans besoin d'une autorité tiers de confiance.
Retenons cinq promesses de la blockchain :
1. Confiance distribuée.
2. Système transactionnel.
3. Garanti par une large communauté.
4. Sans tiers de confiance.
5. Opérant des protocoles complexes.

16. Voir Peter Sayer, « Bitcoin miner KnC is planning another four-week datacenter build-out », networkworld.com, 11 décembre 2015 (www.networkworld.com/article/3014467/Bitcoin-miner-knc-is-planning-another-four-week-datacenter-build-out.html).

La blockchain est une véritable innovation : il y a vingt ans, il n'était absolument pas évident qu'un jour il soit possible de pouvoir faire même les seules quatre premières promesses simultanément. En revanche, c'est bien la combinaison des cinq promesses qui définit le domaine d'application des blockchains. Si l'on en a besoin que de deux ou trois, il existe d'autres méthodes, moins chères ou plus efficaces (voir *infra*).

La cinquième promesse est essentielle, car elle explique la nature disruptive des blockchains, la capacité à opérer des protocoles complexes (transfert d'argent, banque, certification, etc.) de façon automatique, donc avec des coûts de transactions beaucoup plus faibles que des systèmes avec des acteurs humains, surtout dans le rôle de tiers de confiance. Autrement dit, la blockchain ne transporte pas que des informations, elle transporte aussi des algorithmes, avec la même garantie de confiance que les informations elles-mêmes. Le lecteur peut déjà imaginer ce que cela signifie en termes d'automatisation de tout un ensemble de processus réalisés actuellement par des êtres humains, comme les actes notariés, par exemple. Ce point sera développé dans la suite de ce texte.

Les ingrédients clés

Pour réaliser la recette magique de la blockchain, il faut cinq ingrédients :

1. Des chaînes signées, donc qui deviennent quasiment infalsifiables.
2. Des clés publiques et privées pour identifier et faire signer les participants.
3. Un protocole de distribution de documents en pair à pair (comme BitTorrent).
4. Une communauté de grande taille non manipulable.
5. Un protocole de certification du consensus, la preuve de travail.

Pour comprendre cette partie, il est nécessaire d'expliquer ce qu'est le « hash ». Un hash est un algorithme qui transforme une chaîne de caractères (qui peut être un fichier) en une clé, généralement de longueur fixe, qui est, on l'espère, unique, en tout cas avec un faible taux de collision (une collision est quand deux chaînes ont la même clé). Le hash a pour caractéristique qu'il n'est pas réversible : on ne peut pas retrouver le texte original à partir de la clé, sauf à maintenir un dictionnaire[17]. On utilise le hash pour crypter des mots de passe : on teste uniquement sur la clé, permettant ainsi de ne pas stocker les mots de passe en clair dans une base, mais uniquement leur clé[18].

17. Notons que c'est ce qui a fait la faiblesse du protocole md5 pour crypter les mots de passe : on trouve des dictionnaires en ligne qui permettent de retrouver le mot original, et donc de casser la clé.

18. Mais il existe encore trop de sites qui stockent les mots de passe en clair, créant ainsi des vulnérabilités dangereuses (par exemple lesechos.fr…).

Dans la blockchain, c'est la succession d'un bloc et de la clé de toute la chaîne qui le précède qui est ainsi crypté, et fournit une clé[19] qui permet de vérifier l'intégrité de toute la chaîne. On ne peut donc pas substituer un bloc à un autre, car la clé ne serait plus la même.

Prenons l'exemple d'un faussaire qui voudrait changer une ancienne transaction, l'effacer ou bien la modifier. Pour cela, il lui faut recréer toute une chaîne de blocs différente, à partir de la date de la transaction qu'il a falsifiée jusqu'au moment où il la falsifie. Il doit persuader plus de la moitié des nœuds du réseau que sa version de la chaîne est la bonne. Grâce à la difficulté de la preuve de travail, ce travail demande trop d'effort en un temps limité et nécessite que le faussaire possède plus de la moitié des nœuds. Ceci rend donc la chaîne robuste. Comme pour une clé publique, le travail de cryptographie est asymétrique : il est très difficile de trouver à partir de la clé, mais facile de vérifier, ce qui confère le caractère auditable de la blockchain. Enfin, un point important est que la blockchain n'est pas anonyme mais pseudonyme : les parties prenantes des transactions sont identifiées, même si leur identité n'est pas connue.

Le point 4 est également essentiel : pour se débarrasser du tiers de confiance, il faut une communauté non orientable. Le point 5 garantit qu'il y a une vraie communauté, mais le point 4 dit qu'il faut à la fois la taille et l'indépendance pour qu'un acteur mal intentionné ne puisse pas prendre la main sur la communauté des mineurs. C'est fondamental, car cela montre que la blockchain prend tout son sens à grande échelle. De même que si le nombre de généraux byzantins n'est que de trois, il n'y a aucune garantie de consensus, une blockchain de petite taille n'est pas utile : si on se fait confiance entre amis, pas besoin des cinq ingrédients, les trois premiers suffisent et on peut faire plus efficace et moins cher que la blockchain.

Le point 5 est le plus complexe, car la taille de la chaîne grandit, et donc la quantité de calcul nécessaire aussi. Il fonctionne car l'algorithme adapte de façon dynamique la charge cryptographique, et également parce que la taille des blocs est constante. Il existe actuellement un débat autour de l'augmentation de la taille des blocs bitcoin qui, comme tous les fondamentaux de l'Internet, se décidera par consensus, les avis étant partagés dans un wiki[20]. Le temps de minage reste constant pour garantir la preuve de travail et il est calé à 600 secondes par bloc. Dans la pratique, on semble voir une limite à

19. Pour le lecteur expert, indiquons que c'est le SHA-256 qui est utilisé (voir fr.wikipedia.org/wiki/SHA-2).
20. Voir en.bitcoin.it/wiki/bloc_size_limit_controversy (en anglais).

6,6 transactions par seconde[21]. La bonne nouvelle est que cela fonctionne au niveau de la planète, mais la mauvaise nouvelle est que, pour que cela fonctionne, il faut utiliser une capacité importante de la puissance de calcul mondiale.

La blockchain a merveilleusement commencé en utilisant des cycles de calculs disponibles sur des machines vides, réparties dans toute la communauté, ce qui est doublement vertueux pour le CO2 et pour le point 4. Au début de la blockchain, des particuliers utilisaient les cartes graphiques de leurs ordinateurs, plus puissantes que les processeurs eux-mêmes. On trouve d'ailleurs en vente sur Internet des machines spécifiques « minage de la blockchain ». Mais, en ce moment, 50 % de la puissance du minage est concentré sur quelques acteurs chinois, avec du hardware spécialisé.

Ce qu'on peut très bien faire sans les cinq promesses

Les promesses 4 et 5 sont extrêmement coûteuses à remplir. Si la crédibilité dans le tiers de confiance est forte, alors il est possible de faire la même chose pour beaucoup moins cher. Par exemple, un tiers de confiance peut proposer un service d'enregistrement et de validation de documents ou d'informations dans un entrepôt numérique, sous la forme de deux interfaces de programmation (API[22]). La première API permet à n'importe qui de stocker une information, et la seconde de valider une revendication. Les promesses 1 et 2 sont remplies par une approche transactionnelle, et la capacité à distribuer la confiance sous la forme de certificats vérifiables. Mais on accepte le fait que l'entrepôt soit une boîte noire. C'est facile à faire et cela coûte beaucoup moins cher qu'une blockchain.

La promesse 3 suppose que l'entrepôt est ouvert, visible par une large communauté. On peut tout à fait réaliser 1 à 3 avec une blockchain partagée avec tous mais authentifié par un seul (le tiers de confiance). Dans ce cas, la structure de la blockchain distribuée est intéressante : une chaîne est une façon de garantir l'intégrité de façon incrémentale ; de plus, en utilisant un mécanisme pair à pair pour partager la chaîne, on permet à beaucoup d'acteurs de faire eux-mêmes les vérifications de cohérence. En termes d'API, cela veut dire que l'on garde la première API d'insertion d'une transaction (insertion réalisée et signée par le tiers de confiance), mais il n'y a plus besoin d'API de vérification, la chaîne est propagée et chacun peut faire la vérification

21. Pour le calcul, voir en.bitcoin.it/wiki/Scalability_FAQ#What_is_this_Transactions_Per_Second_.28TPS.29_limit.3F (en anglais).

22. Les API sont des interfaces de programmation permettant l'ouverture d'un système d'information à l'extérieur. On peut les considérer comme des « prises » qui délivreraient des services spécifiques.

lui-même, comme c'est le cas avec la blockchain. Cette solution supporte les promesses 1 à 3, et donc un des pouvoirs disruptifs de la blockchain, à savoir « trust as a service », serait parfaitement obtenu par une telle approche, du moment que la confiance est mise dans le tiers de confiance.

Il existe donc des solutions qui permettent de produire des blockchains alternatives, beaucoup moins chères, que l'on peut alors appliquer à des sous-domaines fonctionnels. L'intérêt principal est alors de diminuer les coûts de transaction, en éliminant du travail humain qui peut être réalisé avec une meilleure sécurité et à un coût plus faible par les algorithmes. Par exemple, avec l'utilisation d'une blockchain, le transfert d'argent d'un pays à un autre verrait son coût divisé par dix et prendrait dix minutes pour être certifié, au lieu de quelques jours actuellement. C'est cette promesse qui attire aujourd'hui le monde de la finance.

Répétons-le encore une dernière fois : la promesse de résistance à la fraude de la blockchain n'est pas résistante à une décroissance, une petite communauté ne se protège pas contre une tierce partie maligne avec une très forte puissance de calcul, et donc il faut un sujet d'intérêt mondial pour attirer une communauté mondiale de mineurs. La question à se poser est, pour chaque cas d'utilisation de la blockchain, celle de savoir s'il est possible de convoquer une communauté mondiale sur le domaine (sinon le point 4 ne fonctionne pas et il est possible d'être submergé) et si le coût de la preuve de travail massif reste moins cher et plus fluide que le fonctionnement d'une autorité tiers de confiance.

Du point de vue politique, la réponse peut être très différente (ce n'est pas une question de coûts mais de liberté, et c'est ce qui motive la majorité de la communauté crypto/blockchain).

D'un point de vue économique, les cas d'utilisation sont encore en émergence. Dans le monde économique traditionnel, l'idée de la suppression d'un tiers de confiance est inadmissible. Toutes les initiatives des institutions actuelles ne supportent pas toutes les promesses de la blockchain, sinon, par exemple, la vague prudente et réservée d'intérêt des banques pour la blockchain serait remplacée par un vent de panique, puisque la blockchain avec toutes ses promesses rendrait leur rôle de tiers de confiance inutile. En revanche, lorsque le coût de la transaction devient trop élevé, en temps comme en argent, la crédibilité du tiers de confiance disparaît, et la blockchain sans tiers de confiance offre une alternative plus efficace.

Dans le domaine social ou politique, la situation est quelque peu différente. Lorsque le citoyen va véritablement s'interroger sur l'efficacité de l'administration, celle-ci pourra alors commencer à étudier la blockchain. Il y a de nombreux cas où la blockchain peut apporter un vrai bénéfice politique

ou sociétal et dans lesquels nous serions contents de nous passer d'institutions, voire d'un État. Un modèle émerge alors, qui se nomme Decentralized Autonomous Organization (DAO), décrit plus loin dans ce document.

Trois questions clés

La latence est le premier sujet important. Par construction, la blockchain impose une double contrainte sur la latence : d'un côté, la preuve de travail prend du temps et, de l'autre, la validation des blocs de transaction est fonction de la probabilité requise de sécurité. Donc, il faut du temps (au moins 10 minutes par validation de blocs pour le bitcoin), lequel est soumis à des fluctuations aléatoires classiques de file d'attente. Les problèmes de scalabilité se traduisent en problèmes de temps de réponse. Bon nombre de services financiers ne pourront pas se satisfaire de ces temps de latence, surtout à l'heure du trading haute fréquence.

La « scalibilité » est un sujet plus complexe, qui fait l'objet de beaucoup de débats. Faire grandir la blockchain harmonieusement exige de convoquer une puissance de calcul croissante (en petahash[23] par seconde) tout en conservant la « distribution » de la communauté (beaucoup d'acteurs indépendants). L'ingrédient 4 dit en effet que la communauté des mineurs dispose de beaucoup plus de ressources qu'un attaquant malin et que la communauté est suffisamment vaste et distribuée pour qu'on ne puisse pas en prendre le contrôle. La croissance rapide et le besoin de « scalabilité » font qu'au contraire on assiste en ce moment à une concentration. On peut faire un parallèle intéressant avec l'architecture distribuée des DNS[24], pour lesquels on a vu émerger une concentration de fait.

La confiance distribuée engendre également des surcoûts. Au début, les cycles de calculs étaient des « cycles gratuits » pris sur des machines sous-utilisées. La nature compétitive du processus de consensus (les premiers arrivés partagent la récompense) a créé un contexte darwinien de spécialisation. Le coût énergétique de la preuve de travail n'est pas négligeable, même si les machines ont évolué vers des ASIC spécialisés, ce qui d'ailleurs met de côté la communauté ouverte des développeurs. On commence à voir apparaître des complaintes que les coûts de certification deviennent importants par rapport à d'autres méthodes plus classiques. Ceci ne va faire que se dégrader : la loi de Moore joue positivement pour les autres méthodes (qui seront donc de moins

23. Rappelons que 1 peta = 10^{15}, soit 1 000 tera.

24. Le DNS est l'annuaire global de l'Internet. C'est lui qui dit que telle adresse (www.fondapol.org, par exemple) pointe vers tel serveur. S'il ne devient plus global, alors l'Internet explose et la même adresse pourrait alors pointer vers d'autres serveurs suivant le lieu où l'on se trouve, ce qui signifierait la fin de la globalité du réseau.

en moins chères au fur et à mesure que les machines seront plus puissantes à coûts réduits), alors que la blockchain, par nature, conduit à produire de plus en plus d'efforts lorsque les machines progressent. À côté de la preuve de travail où, rappelons-le, tout le monde doit résoudre le même puzzle, une autre manière de créer le consensus a émergé : le *proof of stake*[25], où l'effort de mining ne se fait que sur des sous-ensembles de la blockchain où le mineur est concerné. Bitcoin est construit sur la preuve de travail, mais d'autres cryptomonnaies ont évolué vers le *proof of stake*, comme Peercoin.

LES IMPACTS DE LA BLOCKCHAIN

Les *smart contracts*

Toute personne qui a eu l'occasion de lire un contrat a pu en mesurer la complexité. Les avocats semblent ravis à l'idée de créer du compliqué, rendant par là même l'exécution du contrat difficile, au risque d'ailleurs d'y trouver parfois des contradictions. Mais même pour des contrats simples, on trouve souvent des successions d'événements qui sont importantes dans leur réalisation. En 1993, le concept de « smart contract » a été inventé pour automatiser les relations contractuelles, en éliminant toute intervention humaine. Un prêt bancaire, par exemple, peut très bien être totalement automatisé, sans intervention humaine, puisque tous les paramètres sont non biaisés. Mais se pose toujours la question de la confiance dans l'exécution, donc de l'auditabilité du contrat.

La particularité de la technologie blockchain est de pouvoir y stocker non seulement du contenu, mais aussi des algorithmes grâce aux morceaux de codes. Comme ces algorithmes deviennent, au travers de la blockchain, auditables par tout le monde, la confiance ne peut que s'en trouver renforcée. Prenons un exemple simple : la TVA. Les manques à gagner sont énormes (en 2013, 32 milliards d'euros rien que pour la France[26]) et la fraude, surtout la fraude dite « carrousel », en représente une grande part. Imaginons maintenant que toutes les transactions de TVA soient dans une blockchain. Toutes les parties prenantes peuvent auditer que les règles sont bien respectées et que les

25. Pour une description de la *proof of stake*, voir www.bitsharesfcx.com/bts2_11.php.

26. Philippe Ricard et Patrick Roger, « TVA : 32 milliards d'euros perdus par la France chaque année », lemonde.fr, 18 septembre 2013 (www.lemonde.fr/politique/article/2013/09/18/tva-32-milliards-d-euros-perdus-par-la-france-chaque-annee_3479706_823448.html).

transactions sont sincères, tant dans le calcul de leur montant que dans leur paiement. La fraude n'est plus possible.

Le coût de vérification est bien moindre que la même opération réalisée avec un opérateur humain et, surtout, beaucoup plus rapide. Ceci est vrai si les événements qui permettent de vérifier l'exécution du contrat peuvent être automatiquement captés par la blockchain, comme dans le cas d'un prêt bancaire et de ses remboursements. Mais que faire, par exemple, quand le déclenchement d'une action (un paiement) dépend d'un événement physique comme la livraison d'un bien ? C'est alors que l'intégration des objets intelligents dans le *smart contract* prend tout son sens. On pourrait imaginer un monde de clés électroniques où la possession d'un bien immobilier serait automatiquement déclenchée à partir de l'exécution du contrat de vente ou de location présent dans la blockchain, donc non biaisé et auditable, rendant ainsi la propriété inviolable. L'ancien propriétaire ne pourrait plus rentrer car sa clé électronique ne fonctionnerait plus, et le nouveau ne pourrait y rentrer que lorsque le logiciel aurait débloqué sa clé[27]. La récente décision d'Airbnb de se lancer dans la blockchain[28] pourrait bien être un début de gestion des relations entre locataires et propriétaires par des *smart contracts*. On perçoit maintenant comment des métiers de tiers de confiance, comme les notaires, les avocats ou les greffiers, peuvent être totalement transformés avec la blockchain.

Les organisations décentralisées autonomes

Le monde des entreprises, tout comme l'administration, fait face à une crise fondamentale. Les raisons sont équivalentes dans les deux domaines : modèles en silo, structures verticales, hiérarchies pesantes, management basé sur la méfiance, gouvernance laissant peu de place à la créativité et l'inventivité, différenciation entre le « pensant » et l'« exécutant »… Dans un monde en interactions, où l'intelligence collective est la règle, ces modèles sont inefficaces car ils font très mal circuler l'information et donc développent insuffisamment la connaissance[29].

En 1937, l'économiste Ronald Coase montrait que le concept d'entreprise a été principalement créé pour diminuer les coûts de transactions, entre autres

27. La première réalisation de cette idée est bien expliquée dans une vidéo intitulée « Rent, sell or share anything – without middlemen » (slock.it), réalisée par une start-up qui rend possible la location où le prêt de tout objet personnel grâce à une blockchain.

28. Voir « Airbnb just acquired a team of bitcoin and blockchain experts » qs.com, 12 avril 2016 (qz.com/657246/airbnb-just-acquired-a-team-of-bitcoin-and-blockchain-experts).

29. Sur l'importance d'une société basée sur la connaissance, Idriss J. Aberkane, Économie de la connaissance, Fondation pour l'innovation politique, 2015 (www.fondapol.org/etude/idriss-j-aberkane-economie-de-la-connaissance).

en regroupant l'information et la logistique[30]. Dans ce modèle, la hiérarchie est importante parce qu'elle réduit l'incertitude, donc les coûts de transaction. Mais pourquoi le monde n'est-il pas alors une seule entreprise ? Parce qu'un second coût vient se greffer sur le premier : le coût d'organisation. En d'autres termes, la loi des rendements décroissants fait que le résultat n'est pas toujours proportionnel aux moyens. Le modèle en pair à pair permet justement de continuer d'assurer la transmission de l'information tout en garantissant la confiance. Ceci s'applique également au modèle transactionnel.

Ronald Coase s'intéressait aussi aux coûts sociaux et montrait que l'État n'a pas assez d'informations pour taxer au bon niveau mais que les agents taxants et les taxés pouvaient se mettre d'accord – on dirait aujourd'hui « en mode pair à pair » –, pourvu que les coûts de transaction soient faibles.

Il ne manquait plus qu'une technologie pour supporter les idées de Coase : c'est justement ce que fait la blockchain. On perçoit alors que le modèle de la blockchain sape en profondeur la raison principale d'existence des institutions. Une organisation est constituée d'actifs matériels et immatériels et de personnes. Dans le paradigme traditionnel, certaines personnes décident (le conseil d'administration, les managers, ou bien l'Assemblée nationale, le gouvernement…), d'autres exécutent. La révolution industrielle a largement réduit le nombre d'exécutants en les remplaçant efficacement par des robots. Mais les cols blancs vont bientôt suivre la même logique : si le « cerveau-d'œuvre » a remplacé la main-d'œuvre[31], celui-ci peut être également automatisé, et donc remplacé par des ordinateurs. Plus l'entreprise sera gouvernée par des règles et des processus, plus leur automatisation deviendra évidente. Si l'on reprend l'exemple de la banque, effectuer un virement ne nécessite en rien la présence d'un être humain « au milieu » qui n'apporte aucune valeur ajoutée par rapport aux règles de la banque, voire qui ralentit le processus – ou même qui ne devient utile que quand il s'agit de contourner les règles. Appliquer les règles d'une entreprise pour effectuer une transaction valide peut très bien se faire uniquement avec des logiciels, nous l'avons montré avec les *smart contracts*. Cela ne signifie bien sûr pas la fin de l'être humain, mais l'apparition d'un modèle d'entreprise où les intelligences seraient alors utilisées non plus pour faire des tâches répétitives sans valeur ajoutée, mais pour créer de la connaissance. Toutes les conditions sont alors réunies pour créer un modèle d'entreprise totalement efficace, où toutes les

30. Ronald Coase, « The Nature of the firm », *Economica*, vol 4, n° 16, novembre 1937, p. 386-405 (onlinelibrary.wiley.com/doi/10.1111/j.1468-0335.1937.tb00002.x/epdf).

31. Jean-Pierre Corniou *et al.*, *Le Choc numérique*, Nuvis, 2013 (voir aussi www.lechocnumerique.fr).

parties prenantes peuvent participer à la décision, auditer les règles et en vérifier l'application. L'équivalent de ce phénomène en politique serait le « government as a platform », tel qu'il a été défini par Tim O'Reilly [32]. La blockchain est alors l'outil qui permet de gérer ces entreprises.

La DAO est un modèle de gouvernance théorique où des entités autonomes coopèrent entre elles selon des règles de travail qui sont infalsifiables. Pour atteindre cet objectif, une méthode est d'implémenter les règles en utilisant des logiciels open source qui sont distribués sur tous les ordinateurs des parties prenantes. Un exemple de codage de règles de gouvernance peut être trouvé sur le site d'Ethereum [33]. La représentation codée des règles peut paraître bizarre, mais il rend plus simple leur compréhension, et donc facilite leur audit. Un effet de bord de l'usage des blockchains serait de vérifier la cohérence des règles de gouvernance. Il est sûr que les codes sont remplis de contradictions, qui deviendraient alors décelables. Un effet intéressant est la possibilité, via la blockchain, de mettre en place une démocratie liquide, où chaque personne peut choisir un représentant pour voter à sa place dans un contexte qui peut être limité dans le temps et dans l'espace. Pour le lecteur intéressé par ce modèle, la start-up Boardroom [34] propose des outils de gestion d'une DAO.

Le cas Ethereum

Dans le monde Internet, très souvent le premier installé prend toute la place (« winner takes all »), à condition qu'il trouve le bon modèle économique. On l'a vu avec Google [35], Amazon, mais aussi Airbnb, Uber et bien d'autres. Dans le monde de la blockchain, une société émerge actuellement, qui offre une blockchain générique : Ethereum.

Ethereum est une fondation, basée à Toronto, et une entreprise, basée en Suisse, qui propose une blockchain permettant de gérer non seulement de la cryptomonnaie, mais aussi des *smart contracts*, au travers d'un automate de Turing. Son code est open source, sa monnaie, qui se nomme ether, vaut, en avril 2016, 900 millions de dollars [36].

32. Tim O'Reilly, « Government as a Platform », in Daniel Lathrop et Laurel Ruma (dir.), *Open Government. Collaboration, Transparency, and Participation in Practice*, O'Reilly Media, février 2010, chap. 2 (chimera.labs.oreilly.com/books/1234000000774/ch02.html).

33. « How to build a democracy on the blockchain », www.ethereum.org/dao.

34. Voir boardroom.to. Leur « livre blanc » résume assez bien les actions typiques d'une DAO : Nick Dodson, *BoardRoom: A Next-Generation Decentralized Governance Apparatus*, s.d. (boardroom.to/BoardRoom_WhitePaper.pdf).

35. AltaVista existait avant Google, mais n'a pas su trouver son modèle économique. Lors du rachat de Digital par Compaq, AltaVista n'a même pas fait partie de la valorisation de Digital.

36. Voir l'évolution en continu sur coinmarketcap.com/currencies/ethereum.

Ethereum ouvre dans plusieurs dimensions, à la fois sur ce qu'il faut faire pour miner et ce qu'il est possible de certifier, puisque l'ambition est d'avoir un automate Turing complet certifié. Le risque est d'empiler un tel niveau de complexité que d'autres problèmes risquent d'apparaître, alors qu'on est très loin d'avoir exploré tout ce qu'il est déjà possible de faire avec la blockchain. Mais il faut faire confiance à la capacité américaine pour résoudre les problèmes lorsqu'ils se présentent.
Microsoft vient de proposer une « blockchain as a service » basée sur les technologies Ethereum [37]. Savoir si Ethereum sera le prochain service quasi universel ou bien si Amazon va créer sa propre blockchain en continuation d'Amazon Elastic Compute Cloud (EC2) reste du domaine de la spéculation.

QUELQUES USAGES DE LA BLOCKCHAIN

Les usages sont déjà nombreux, et ce dans des domaines variés. Il n'est déjà plus possible de tous les lister, mais il est possible d'en donner quelques exemples. Il est probable que, dans moins d'un an (soit en 2017), le panorama des usages soit différent de ce qu'il est aujourd'hui. En revanche, toutes les expérimentations ne remplissent pas forcément l'ensemble des cinq promesses. On imagine mal une institution tiers de confiance créant tout de go une blockchain proposant les promesses de 1 à 5 sans penser à son nouveau rôle dans un monde où la blockchain assurerait la confiance dans les transactions, rendant le tiers inutile.

Finance

Le premier exemple d'usage de la blockchain a été, bien sûr, le bitcoin. Cette cryptomonnaie, qui respecte les cinq promesses de la blockchain, a été inventée en 2007 par un mystérieux Satoshi Nakamoto. Elle est limitée en quantité (21 millions) et commence à être bien installée dans le paysage : en mai 2016, on recense plus de 7 600 lieux dans le monde acceptant le bitcoin comme moyen de paiement [38] et la Securities and Exchange Commission (SEC) américaine a

37. Giulio Prisco, « Microsoft Launches Ethereum Blockchain as a Service (EBaaS) at Devcon, Boosts Ethereum », 11 novembre 2015, bitcoinmagazine.com (Bitcoinmagazine.com/articles/microsoft-launches-ethereum-la blockchain-as-a-service-ebaas-at-devcon-boosts-ethereum-1447277647).

38. Voir carte du monde actualisée sur https://coinmap.org/#/world/47.57652571/6.67968750/4.

même autorisé le bitcoin comme monnaie pour les dons des partis politiques. Le bitcoin a vite été rattrapé par d'autres cryptomonnaies : Wikipédia en recense plus de 600, dont 9 à plus de 10 millions de dollars[39].

La finance est un exemple typique de modèle qui a du mal à muter. Non seulement le coût des transactions bancaires est énorme, mais elles ne sont pas fluides : il faut ainsi encore plusieurs jours pour effectuer un transfert intra-européen, pour un service rendu qui n'est pas de très grande qualité. Surtout, les banques sont plutôt frileuses en termes d'ouverture ; il a fallu l'arrivée de PayPal pour qu'elles commencent à ouvrir des API. Toute intervention humaine dans une transaction signifie ralentissement, donc plus faible capacité de traitement globale, donc mauvaise qualité de service. Le coût de la méfiance est énorme, c'est un des atouts de la blockchain que de permettre de passer à un modèle basé sur la confiance.

Côté clients, la grande force de la blockchain est d'accélérer les transactions tout en préservant la confiance collective. Côté institutions financières, la blockchain représente une énorme réduction des coûts et la possibilité d'offrir un meilleur service. Mais une blockchain qui remplit les promesses 1 à 5 rend *de facto* l'institution inutile. Les banques sont donc en train de construire des blockchains avec moins que les cinq promesses, avec comme objectifs la réduction des coûts et la plus grande fluidité transactionnelles. Actuellement, les institutions financières traditionnelles en sont à peine au début de l'expérimentation. Mais l'Estonie, par exemple, a décidé, avec l'aide du Nasdaq, de mettre sur une blockchain les systèmes de votes pour les actionnaires de toutes les entreprises du pays[40].

Santé

Notre système de santé date de l'Antiquité[41]. Il n'y a quasiment aucun transfert d'informations entre toutes les parties prenantes : médecin de ville, infirmière, hôpitaux ; et c'est encore le patient qui assure la fonction de communication en transportant son propre dossier. La construction du dossier médical personnalisé est un échec cuisant, pour des raisons purement politiques. La conséquence est une méfiance accrue dans l'institution.

Une blockchain aurait beaucoup d'avantages : tout d'abord plus de tiers de confiance qui gaspille l'argent du public pour fabriquer des systèmes complexes qui ne fonctionnent pas. La blockchain permet un système de santé

39. « List of cryptocurrencies », Wikipédia (en.wikipedia.org/wiki/List_of_cryptocurrencies, en anglais).
40. http://ir.nasdaq.com/releasedetail.cfm?releaseid=954654.
41. Voir le blog de Jean-Michel Billaut sur la e-santé : billaut.typepad.com/jm/e-sant%C3%A9/.

dont le coût de fabrication, et de fonctionnement, est plus faible, rendant ainsi la somme d'argent nécessaire au remboursement plus élevée. De plus, la possibilité de rentrer des « smart contracts » dans la blockchain permet une médecine beaucoup plus individualisée, où les dépenses et les remboursements seraient fonction du profil. Enfin, ce serait la communauté qui aurait une garantie de bon fonctionnement, au lieu d'une administration opaque.
Ce n'est pas une utopie : l'Estonie, pays connu pour investir énormément dans le numérique, est en cours de création d'une blockchain pour stocker tous les dossiers médicaux de ses citoyens[42].

Politique

La complexité des codes français n'est pas à démontrer. Le code du travail à lui tout seul représente entre 2 000 et 15 000 pages suivant que l'on considère le cœur du code ou bien la jurisprudence. Mais même 2 000 pages, cela fait beaucoup, surtout si l'on considère les conventions de branche, les statuts spéciaux, le droit européen, etc. Ne nous leurrons pas, aucune personnalité politique n'aura le courage de réduire le code du travail, un travail herculéen ; en revanche, il serait intéressant de le codifier en *smart contracts*, ce qui pourrait avoir comme effet intéressant de mettre à jour les contradictions, puis de placer ces *smart contracts* dans une blockchain, laquelle serait partagée par toutes les parties prenantes : entreprises, administrations, salariés… Les calculs seraient automatiques et le gain financier pour l'État, donc pour la collectivité, serait énorme en termes de contrôle.
D'une manière générale, toutes les règles de gouvernance, que ce soit pour une entreprise, une association ou un pays, peuvent être mises dans une blockchain (nous avons détaillé ceci dans la partie DAO). Dans la politique, cela conduit à mettre en œuvre le concept de « démocratie liquide ». Un débat a lieu actuellement sur les limites de ce système, dont le travers serait de conduire à la tyrannie du code (*rules of law* contre *tyrrany of code*)[43]. Certains partis politiques, comme le parti pirate au Royaume-Uni, ou bien Nous Citoyens en France, utilisent déjà la blockchain pour la gestion des votes[44] . En Australie, un parti politique, The Flux Party, a décidé de mettre sa gouvernance sur

42. « Guardtime Secures Estonian Health Records », e-estonia.com, 8 mars 2016 (e-estonia.com/guardtime-secures-estonian-health-records).

43. Voir Aaron Wright et Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, abstract, Social Science Research Network (SSRN), 10 mars 2015 (papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664).

44. Voir, pour le Royaume-uni, « The Democracy Interface: Time to Upgrade? », ppuk.org.uk, 10 juillet 2015 (www.ppuk.org.uk/tags/blockchain) ; pour la France, « La blockchain au service de la politique ? », nouscitoyens.fr, 8 avril 2016 (www.nouscitoyens.fr/blog/2016/04/08/frenchweb-la-blockchain-au-service-de-la-politique).

une blockchain[45]. Le principe est que les sénateurs du parti doivent appliquer les décisions prises par les membres par vote sur la blockchain. L'innovation est que les membres ont des crédits de votes, qu'ils peuvent échanger sur la blockchain pour se concentrer sur leurs propres sujets d'intérêt. Il s'agit d'une véritable implémentation des principes de démocratie liquide[46], avec la délégation sur certains sujets et le vote direct sur d'autres.

Médias

Le monde de la musique et du cinéma voue à Internet un mélange d'amour et de haine. La rage que met surtout la Recording Industry Association of America (RIAA) à combattre les « pirates » est impressionnante. Nous ne rentrerons dans le débat juste pour dire que ce monde est dans une économie matérielle et que la fameuse loi « quand on partage un bien matériel, il se divise ; quand on partage un bien immatériel, il se multiplie » s'applique bien au cas de la musique.
En revanche, le problème de la répartition équitable des droits est un véritable problème transactionnel, qui nécessite de la confiance. Mais les majors, de par leur combat acharné contre le *peer to peer,* ont énormément perdu en e-réputation, surtout parmi la population des geeks, qui les accusent de ne pas donner assez aux créateurs et de ne pas offrir un service au niveau du pourcentage qu'ils se prennent. La tentation est grande alors d'utiliser une blockchain pour redistribuer l'argent à tout le monde, sans le tiers de confiance. La start-up Muse s'est créée sur cette idée[47]. Elle souhaite créer la blockchain mondiale de la musique, avec répartition des droits à toutes les parties prenantes.

Petites annonces

OpenBazaar[48] (actuellement en beta) est une plateforme de petites annonces en pure mode pair à pair. Au lieu de passer par un site, chaque utilisateur télécharge un logiciel sur son ordinateur et peut accéder aux offres, ou bien vendre son propre bien, sans aucune commission. C'est un concurrent de eBay ou du Bon coin.

45. Voir voteflux.org.

46. Dominik Schiener, « La démocratie liquide : une véritable démocratie pour le 21e siècle », s.d. (framablog.org/2015/12/09/democratie-liquide).

47. museblockchain.com.

48. openbazaar.org.

Transport

Le transport collaboratif possède aussi sa blockchain. Lazooz[49] propose de partager la route et, bien sûr, de gérer les transactions financières, sur une blockchain. Tout comme OpenBazaar, la première qualité est de baisser les coûts de transaction. Il restera néanmoins à voir précisément si, dans le cas du partage de voiture, l'existence d'un tiers de confiance externe vers qui l'utilisateur peut se retourner et qui est capable de mutualiser les risques – et donc de garantir la satisfaction client – ne reste pas un ingrédient nécessaire au succès.

LE FUTUR

Il existe une tension entre le besoin d'avoir une infrastructure unique et mondiale pour garantir l'existence d'une communauté plus large que des attaquants potentiels (cf. le quatrième ingrédient) et la multiplicité des opportunités que nous venons d'évoquer. Nous avons vu que l'idée de « mon petit blockchain à moi » ne fonctionne pas si l'on souhaite avoir l'ensemble des promesses de la blockchain. En revanche, dès qu'on accepte un tiers de confiance, il est facile d'instancier un sous-ensemble de ces technologies pour des cas particuliers. Par exemple, pour la certification de documents (cadastre, sinistres, propriétés…), un système plus simple, implémentant les promesses 1 à 3, est suffisant, sans le surcoût financier ou énergétique de la preuve de travail.

Néanmoins, l'utilisation de la blockchain pour créer un modèle « trust as a service » a beaucoup de sens. En effet, la beauté de l'approche blockchain est de permettre à un petit acteur inconnu, par exemple une start-up, d'offrir des garanties de transparence et de pérennité – caractéristiques de la confiance qui sont traditionnellement associées à des acteurs institutionnels et anciens (l'avantage compétitif des grosses institutions financières). Cette start-up, lorsqu'elle inscrit ses transactions dans la blockchain mondiale, offre une garantie de non-répudiation supérieure ou égale à celle d'un État ou d'une banque. En revanche, il n'est pas clair que l'infrastructure actuelle puisse héberger l'avalanche de demandes et d'opportunités que nous venons d'évoquer brièvement.

49. www.lazooz.net.

Nous voyons en conséquence émerger une structure arborescente : une grosse blockchain centrale, mondiale, certifiée par une communauté large, et des branches (blockchains ou autres) opérées de façon plus simple par des start-up ou des communautés restreintes d'intérêt. L'intérêt de cette approche est d'offrir à une start-up la capacité de mettre dans la grande blockchain le *ledger* de ses propres activités pour offrir confiance et transparence à ses propres clients, lui-même géré avec des techniques plus légères, qui permettent alors, par exemple, des coûts de fonctionnement ou une latence plus faible.

Cette approche a donné naissance à plusieurs développements technologiques, dont les sidechains. Une sidechain est une chaîne de transactions gérée par une sous-communauté, avec des techniques semblables de chiffrement et d'authentification mais avec un protocole plus simple permettant de plus grandes performances. La distribution du contrôle (la sidechain est sous le contrôle d'un groupe plus petit) donne plus d'agilité, mais l'extrémité de cette sidechain (le peg) est inscrite dans la blockchain pour que toute cette sous-chaîne hérite de la sécurité de blockchain [50].

Cette solution permet également d'étendre la blockchain avec des protocoles plus riches, ce qui fait dire à certain que le principe arborescent blockchain/sidechain est une meilleure façon de faire évoluer l'écosystème que la création de blockchains nouvelles et autonomes [51].

Peut-il exister un vrai mode pair à pair sans acteur de grande taille ? Pour Uber ou Airbnb, la valeur de la marque n'est pas la plateforme mais la promesse client. Et il faut des gens pour assurer le service après-vente. D'un autre côté, Internet fonctionne sans un tel acteur unique. Les détracteurs de l'Internet à ses débuts ont mis en avant le fait que l'absence d'un opérateur rendrait trop difficile l'accès aux non-initiés. C'est vrai, mais les mécanismes d'entraides communautaires ont parfaitement fonctionné et ont avantageusement remplacé les hotlines, beaucoup moins efficaces.

50. Pour approfondir le mécanisme des sidechains, voir Adam Back *et al*., « Enabling Blockchain Innovations with Pegged Sidechains », abstract, 22 octobre 2014 (blockstream.com/sidechains.pdf).

51. Lire par exemple « Drivechain – the simple two way peg » (www.truthcoin.info/blog/drivechain).

CONCLUSION

Lorsque l'influence de la blockchain deviendra préoccupante pour les institutions en place, la tentation sera grande pour les responsables actuels de la casser, en l'interdisant, ou bien en en limitant les effets. Internet est né dans les cartons en 1969 et est devenu grand public en 1991. Ce n'est que vingt-cinq ans après que la plupart des politiques essayent de tuer l'innovation qui accompagne Internet [52].

Mais essayer de limiter Internet, c'est comme vouloir arrêter la pluie. La décentralisation du réseau, le fait que l'intelligence est aux extrémités et pas à l'intérieur du réseau, le désir de beaucoup de citoyens d'un autre modèle où ils sont bien plus engagés, et surtout la croissante complexité du monde, qui se caractérise par un nombre d'interactions de plus en plus élevé, feront forcément la bascule vers les modèles à confiance distribuée. Toute intervention humaine dans une transaction signifie ralentissement, donc plus faible capacité de traitement globale, donc mauvaise qualité de service. La grande force de la blockchain est d'accélérer les transactions tout en préservant la confiance collective, et ce à moindre coût.

Grâce à l'invention des technologies de l'Internet, le monde des télécommunications a vécu le passage d'un modèle centralisé avec des tiers de confiance (les opérateurs) qui justifiaient leur rôle avec la promesse de la « qualité totale », à un modèle décentralisé où tout le monde se connecte au réseau internet n'importe où et sans effort, et profite d'une offre de services universelle à très bas coût. Grâce à l'invention de la blockchain, il est fort probable que le monde de la transaction, pas seulement financière, va vivre le même bouleversement, avec la même douleur pour les opérateurs.

52. Pour des informations sur la censure du Net, voir https://en.wikipedia.org/wiki/Internet_censorship_and_surveillance_by_country.

Retrouvez sur notre site internet les vidéos des interventions lors de l'événement de la Fondation pour l'innovation politique,

LE PROGRÈS, C'EST NOUS ! 24 HEURES NON-STOP

LE 16 NOVEMBRE 2013 À LA MAISON DE LA MUTUALITÉ À PARIS.

Serge Soudoplatoff
sur le thème :
« Numérique et innovations »

http://www.fondapol.org/fondapol-tv/le-progres-cest-nous-serge-soudoplatoff-toile-a-tisser/

Élisabeth Grosdhomme-Lulin
sur le thème :
« Service public 2.0 »

http://www.fondapol.org/fondapol-tv/le-progres-cest-nous-elisabeth-grosdhomme-lulin-des-idees-pour-decider/

Idriss J. Aberkane
sur le thème :
« Économie de la connaissance »

http://www.fondapol.org/fondapol-tv/le-progres-cest-nous-idriss-aberkane-toile-a-tisser/

Pierre Pezziardi
sur le thème :
« La confiance par le numérique »

http://www.fondapol.org/fondapol-tv/le-progres-cest-nous-pierre-pezziardi-toile-a-tisser/

Pour la croissance, la débureaucratisation par la confiance
Pierre Pezziardi, Serge Soudoplatoff et Xavier Quérat-Hément, novembre 2013, 48 pages

La transformation numérique au service de la croissance
Jean-Pierre Corniou, juin 2011, 52 pages

Administration 2.0
Thierry Weibel, janvier 2011, 48 pages

Internet, politique et coproduction citoyenne
Robin Berjon, septembre 2010, 32 pages

NOS DERNIÈRES PUBLICATIONS

La gauche radicale : liens, lieux et luttes (2012-2017)
Sylvain Boulouque, mai 2016, 56 pages

Gouverner pour réformer : Éléments de méthode
Erwan Le Noan et Matthieu Montjotin, mai 2016, 64 pages

Les zadistes (2) : la tentation de la violence
Eddy Fougier, avril 2016, 44 pages

Les zadistes (1) : un nouvel anticapitalisme
Eddy Fougier, avril 2016, 44 pages

Régionales (2) : les partis, contestés mais pas concurrencés
Jérôme Fourquet et Sylvain Manternach, mars 2016, 52 pages

Régionales (1) : vote FN et attentats
Jérôme Fourquet et Sylvain Manternach, mars 2016, 60 pages

Un droit pour l'innovation et la croissance
Sophie Vermeille, Mathieu Kohmann et Mathieu Luinaud, février 2016, 52 pages

Le lobbying : outil démocratique
Anthony Escurat, février 2016, 44 pages

Valeurs d'islam
Dominique Reynié (dir.), préface par le cheikh Khaled Bentounès, PUF, janvier 2016, 432 pages

Chiites et sunnites : paix impossible ?
Mathieu Terrier, janvier 2016, 44 pages

Projet d'entreprise : renouveler le capitalisme
Daniel Hurstel, décembre 2015, 44 pages

Le mutualisme : répondre aux défis assurantiels
Arnaud Chneiweiss et Stéphane Tisserand, novembre 2015, 44 pages

L'Opinion européenne en 2015
Dominique Reynié (dir.), Éditions Lignes de Repères, novembre 2015, 140 pages

La noopolitique : le pouvoir de la connaissance
Idriss J. Aberkane, novembre 2015, 52 pages

Innovation politique 2015
Fondation pour l'innovation politique, PUF, octobre 2015, 576 pages

Good COP21, Bad COP21 (2) : une réflexion à contre-courant
Albert Bressand, octobre 2015, 48 pages

Good COP21, Bad COP21 (1) : le Kant européen et le Machiavel chinois
Albert Bressand, octobre 2015, 48 pages

PME : nouveaux modes de financement
Mohamed Abdesslam et Benjamin Le Pendeven, octobre 2015, 44 pages

Vive l'automobilisme ! (2) Pourquoi il faut défendre la route
Mathieu Flonneau et Jean-Pierre Orfeuil, octobre 2015, 44 pages

Vive l'automobilisme ! (1) Les conditions d'une mobilité conviviale
Mathieu Flonneau et Jean-Pierre Orfeuil, octobre 2015, 40 pages

Crise de la conscience arabo-musulmane
Malik Bezouh, septembre 2015, 40 pages

Départementales de mars 2015 (3) : le second tour
Jérôme Fourquet et Sylvain Manternach, août 2015, 56 pages

Départementales de mars 2015 (2) : le premier tour
Jérôme Fourquet et Sylvain Manternach, août 2015, 56 pages

Départementales de mars 2015 (1) : le contexte
Jérôme Fourquet et Sylvain Manternach, août 2015, 44 pages

Enseignement supérieur : les limites de la « mastérisation »
Julien Gonzalez, juillet 2015, 44 pages

Politique économique : l'enjeu franco-allemand
Wolfgang Glomb et Henry d'Arcole, juin 2015, 36 pages

Les lois de la primaire. Celles d'hier, celles de demain.
François Bazin, juin 2015, 48 pages

Économie de la connaissance
Idriss J. Aberkane, mai 2015, 48 pages

Lutter contre les vols et cambriolages : une approche économique
Emmanuel Combe et Sébastien Daziano, mai 2015, 56 pages

Unir pour agir : un programme pour la croissance
Alain Madelin, mai 2015, 52 pages

Nouvelle entreprise et valeur humaine
Francis Mer, avril 2015, 32 pages

Les transports et le financement de la mobilité
Yves Crozet, avril 2015, 32 pages

Numérique et mobilité : impacts et synergies
Jean Coldefy, avril 2015, 36 pages

Islam et démocratie : face à la modernité
Mohamed Beddy Ebnou, mars 2015, 40 pages

Islam et démocratie : les fondements
Aḥmad Al-Raysuni, mars 2015, 40 pages

Les femmes et l'islam : une vision réformiste
Asma Lamrabet, mars 2015, 48 pages

Éducation et islam
Mustapha Cherif, mars 2015, 44 pages

Que nous disent les élections législatives partielles depuis 2012 ?
Dominique Reynié, février 2015, 4 pages

L'islam et les valeurs de la République
Saad Khiari, février 2015, 44 pages

Islam et contrat social
Philippe Moulinet, février 2015, 44 pages

Le soufisme : spiritualité et citoyenneté
Bariza Khiari, février 2015, 56 pages

L'humanisme et l'humanité en islam
Ahmed Bouyerdene, février 2015, 56 pages

Éradiquer l'hépatite C en France : quelles stratégies publiques ?
Nicolas Bouzou et Christophe Marques, janvier 2015, 40 pages

Coran, clés de lecture
Tareq Oubrou, janvier 2015, 44 pages

Le pluralisme religieux en islam, ou la conscience de l'altérité
Éric Geoffroy, janvier 2015, 40 pages

Mémoires à venir
Dominique Reynié, janvier 2015, enquête réalisée en partenariat avec la Fondation pour la Mémoire de la Shoah, 156 pages

La classe moyenne américaine en voie d'effritement
Julien Damon, décembre 2014, 40 pages

Pour une complémentaire éducation : l'école des classes moyennes
Erwan Le Noan et Dominique Reynié, novembre 2014, 56 pages

L'antisémitisme dans l'opinion publique française. Nouveaux éclairages
Dominique Reynié, novembre 2014, 48 pages

La politique de concurrence : un atout pour notre industrie
Emmanuel Combe, novembre 2014, 48 pages

Européennes 2014 (2) : poussée du FN, recul de l'UMP et vote breton
Jérôme Fourquet, octobre 2014, 52 pages

Européennes 2014 (1) : la gauche en miettes
Jérôme Fourquet, octobre 2014, 40 pages

Innovation politique 2014
Fondation pour l'innovation politique, PUF, octobre 2014, 554 pages

Énergie-climat : pour une politique efficace
Albert Bressand, septembre 2014, 56 pages

L'urbanisation du monde. Une chance pour la France
Laurence Daziano, juillet 2014, 44 pages

Que peut-on demander à la politique monétaire ?
Pascal Salin, mai 2014, 48 pages

Le changement, c'est tout le temps ! 1514 - 2014
Suzanne Baverez et Jean Sénié, mai 2014, 48 pages

Trop d'émigrés ? Regards sur ceux qui partent de France
Julien Gonzalez, mai 2014, 48 pages

L'Opinion européenne en 2014
Dominique Reynié (dir.), Éditions Lignes de Repères, avril 2014, 284 pages

Taxer mieux, gagner plus
Robin Rivaton, avril 2014, 52 pages

L'État innovant (2) : Diversifier la haute administration
Kevin Brookes et Benjamin Le Pendeven, mars 2014, 44 pages

L'État innovant (1) : Renforcer les think tanks
Kevin Brookes et Benjamin Le Pendeven, mars 2014, 52 pages

Pour un new deal fiscal
Gianmarco Monsellato, mars 2014, 8 pages

Faire cesser la mendicité avec enfants
Julien Damon, mars 2014, 44 pages

Le low cost, une révolution économique et démocratique
Emmanuel Combe, février 2014, 52 pages

Un accès équitable aux thérapies contre le cancer
Nicolas Bouzou, février 2014, 52 pages

Réformer le statut des enseignants
Luc Chatel, janvier 2014, 8 pages

Un outil de finance sociale : les social impact bonds
Yan de Kerorguen, décembre 2013, 36 pages

Pour la croissance, la débureaucratisation par la confiance
Pierre Pezziardi, Serge Soudoplatoff et Xavier Quérat-Hément, novembre 2013, 48 pages

Les valeurs des Franciliens
Guénaëlle Gault, octobre 2013, 36 pages

Sortir d'une grève étudiante : le cas du Québec
Jean-Patrick Brady et Stéphane Paquin, octobre 2013, 40 pages

Un contrat de travail unique avec indemnités de départ intégrées
Charles Beigbeder, juillet 2013, 8 pages

L'Opinion européenne en 2013
Dominique Reynié (dir.), Éditions Lignes de Repères, juillet 2013, 268 pages

La nouvelle vague des émergents : Bangladesh, Éthiopie, Nigeria, Indonésie, Vietnam, Mexique
Laurence Daziano, juillet 2013, 40 pages

Transition énergétique européenne : bonnes intentions et mauvais calculs
Albert Bressand, juillet 2013, 44 pages

La démobilité : travailler, vivre autrement
Julien Damon, juin 2013, 44 pages

LE KAPITAL. Pour rebâtir l'industrie
Christian Saint-Étienne et Robin Rivaton, avril 2013, 40 pages

Code éthique de la vie politique et des responsables publics en France
Les Arvernes, Fondation pour l'innovation politique, avril 2013, 12 pages

Les classes moyennes dans les pays émergents
Julien Damon, avril 2013, 38 pages

Innovation politique 2013
Fondation pour l'innovation politique, PUF, janvier 2013, 652 pages

Relancer notre industrie par les robots (2) : les stratégies
Robin Rivaton, décembre 2012, 40 pages

Relancer notre industrie par les robots (1) : les enjeux
Robin Rivaton, décembre 2012, 52 pages

La compétitivité passe aussi par la fiscalité
Aldo Cardoso, Michel Didier, Bertrand Jacquillat, Dominique Reynié et Grégoire Sentilhes, décembre 2012, 20 pages

Une autre politique monétaire pour résoudre la crise
Nicolas Goetzmann, décembre 2012, 40 pages

La nouvelle politique fiscale rend-elle l'ISF inconstitutionnel ?
Aldo Cardoso, novembre 2012, 12 pages

Fiscalité : pourquoi et comment un pays sans riches est un pays pauvre…
Bertrand Jacquillat, octobre 2012, 40 pages

Youth and Sustainable Development
Fondapol/Nomadéis/United Nations, juin 2012, 80 pages

La philanthropie. Des entrepreneurs de solidarité
Francis Charhon, mai / juin 2012, 44 pages

Les chiffres de la pauvreté : le sens de la mesure
Julien Damon, mai 2012, 40 pages

Libérer le financement de l'économie
Robin Rivaton, avril 2012, 40 pages

L'épargne au service du logement social
Julie Merle, avril 2012, 40 pages

L'Opinion européenne en 2012
Dominique Reynié (dir.), Éditions Lignes de Repères, mars 2012, 210 pages

Valeurs partagées
Dominique Reynié (dir.), PUF, mars 2012, 362 pages

Les droites en Europe
Dominique Reynié (dir.), PUF, février 2012, 552 pages

Innovation politique 2012
Fondation pour l'innovation politique, PUF, janvier 2012, 648 pages

L'école de la liberté : initiative, autonomie et responsabilité
Charles Feuillerade, janvier 2012, 36 pages

Politique énergétique française (2) : les stratégies
Rémy Prud'homme, janvier 2012, 40 pages

Politique énergétique française (1) : les enjeux
Rémy Prud'homme, janvier 2012, 48 pages

Révolution des valeurs et mondialisation
Luc Ferry, janvier 2012, 36 pages

Quel avenir pour la social-démocratie en Europe ?
Sir Stuart Bell, décembre 2011, 36 pages

La régulation professionnelle : des règles non étatiques pour mieux responsabiliser
Jean-Pierre Teyssier, décembre 2011, 36 pages

L'hospitalité : une éthique du soin
Emmanuel Hirsch, décembre 2011, 32 pages

12 idées pour 2012
Fondation pour l'innovation politique, décembre 2011, 110 pages

Les classes moyennes et le logement
Julien Damon, décembre 2011, 40 pages

Réformer la santé : trois propositions
Nicolas Bouzou, novembre 2011, 32 pages

Le nouveau Parlement : la révision du 23 juillet 2008
Jean-Félix de Bujadoux, novembre 2011, 40 pages

La responsabilité
Alain-Gérard Slama, novembre 2011, 32 pages

Le vote des classes moyennes
Élisabeth Dupoirier, novembre 2011, 40 pages

La compétitivité par la qualité
Emmanuel Combe et Jean-Louis Mucchielli, octobre 2011, 32 pages

Les classes moyennes et le crédit
Nicolas Pécourt, octobre 2011, 32 pages

Portrait des classes moyennes
Laure Bonneval, Jérôme Fourquet et Fabienne Gomant, octobre 2011, 36 pages

Morale, éthique, déontologie
Michel Maffesoli, octobre 2011, 40 pages

Sortir du communisme, changer d'époque
Stéphane Courtois (dir.), PUF, octobre 2011, 672 pages

L'énergie nucléaire après Fukushima : incident mineur ou nouvelle donne ?
Malcolm Grimston, septembre 2011, 16 pages

La jeunesse du monde
Dominique Reynié (dir.), Éditions Lignes de Repères, septembre 2011, 132 pages

Pouvoir d'achat : une politique
Emmanuel Combe, septembre 2011, 52 pages

La liberté religieuse
Henri Madelin, septembre 2011, 36 pages

Réduire notre dette publique
Jean-Marc Daniel, septembre 2011, 40 pages

Écologie et libéralisme
Corine Pelluchon, août 2011, 40 pages

Valoriser les monuments historiques : de nouvelles stratégies
Wladimir Mitrofanoff et Christiane Schmuckle-Mollard, juillet 2011, 28 pages

Contester les technosciences : leurs raisons
Eddy Fougier, juillet 2011, 40 pages

Contester les technosciences : leurs réseaux
Sylvain Boulouque, juillet 2011, 36 pages

La fraternité
Paul Thibaud, juin 2011, 36 pages

La transformation numérique au service de la croissance
Jean-Pierre Corniou, juin 2011, 52 pages

L'engagement
Dominique Schnapper, juin 2011, 32 pages

Liberté, Égalité, Fraternité
André Glucksmann, mai 2011, 36 pages

Quelle industrie pour la défense française ?
Guillaume Lagane, mai 2011, 26 pages

La religion dans les affaires : la responsabilité sociale de l'entreprise
Aurélien Acquier, Jean-Pascal Gond et Jacques Igalens, mai 2011, 44 pages

La religion dans les affaires : la finance islamique
Lila Guermas-Sayegh, mai 2011, 36 pages

Où en est la droite ? L'Allemagne
Patrick Moreau, avril 2011, 56 pages

Où en est la droite ? La Slovaquie
Étienne Boisserie, avril 2011, 40 pages

Qui détient la dette publique ?
Guillaume Leroy, avril 2011, 36 pages

Le principe de précaution dans le monde
Nicolas de Sadeleer, mars 2011, 36 pages

Comprendre le Tea Party
Henri Hude, mars 2011, 40 pages

Où en est la droite ? Les Pays-Bas
Niek Pas, mars 2011, 36 pages

Productivité agricole et qualité des eaux
Gérard Morice, mars 2011, 44 pages

L'Eau : du volume à la valeur
Jean-Louis Chaussade, mars 2011, 32 pages

Eau : comment traiter les micropolluants ?
Philippe Hartemann, mars 2011, 38 pages

Eau : défis mondiaux, perspectives françaises
Gérard Payen, mars 2011, 62 pages

L'irrigation pour une agriculture durable
Jean-Paul Renoux, mars 2011, 42 pages

Gestion de l'eau : vers de nouveaux modèles
Antoine Frérot, mars 2011, 32 pages

0ù en est la droite ? L'Autriche
Patrick Moreau, février 2011, 42 pages

La participation au service de l'emploi et du pouvoir d'achat
Jacques Perche et Antoine Pertinax, février 2011, 32 pages

Le tandem franco-allemand face à la crise de l'euro
Wolfgang Glomb, février 2011, 38 pages

2011, la jeunesse du monde
Dominique Reynié (dir.), janvier 2011, 88 pages

L'0pinion européenne en 2011
Dominique Reynié (dir.), Édition Lignes de Repères, janvier 2011, 254 pages

Administration 2.0
Thierry Weibel, janvier 2011, 48 pages

0ù en est la droite ? La Bulgarie
Antony Todorov, décembre 2010, 32 pages

Le retour du tirage au sort en politique
Gil Delannoi, décembre 2010, 38 pages

La compétence morale du peuple
Raymond Boudon, novembre 2010, 30 pages

L'Académie au pays du capital
Bernard Belloc et Pierre-François Mourier, PUF, novembre 2010, 222 pages

Pour une nouvelle politique agricole commune
Bernard Bachelier, novembre 2010, 30 pages

Sécurité alimentaire : un enjeu global
Bernard Bachelier, novembre 2010, 30 pages

Les vertus cachées du low cost aérien
Emmanuel Combe, novembre 2010, 40 pages

Innovation politique 2011
Fondation pour l'innovation politique, PUF, novembre 2010, 676 pages

Défense : surmonter l'impasse budgétaire
Guillaume Lagane, octobre 2010, 34 pages

0ù en est la droite ? L'Espagne
Joan Marcet, octobre 2010, 34 pages

Les vertus de la concurrence
David Sraer, septembre 2010, 44 pages

Internet, politique et coproduction citoyenne
Robin Berjon, septembre 2010, 32 pages

Où en est la droite ? La Pologne
Dominika Tomaszewska-Mortimer, août 2010, 42 pages

Où en est la droite ? La Suède et le Danemark
Jacob Christensen, juillet 2010, 44 pages

Quel policier dans notre société ?
Mathieu Zagrodzki, juillet 2010, 28 pages

Où en est la droite ? L'Italie
Sofia Ventura, juillet 2010, 36 pages

Crise bancaire, dette publique : une vue allemande
Wolfgang Glomb, juillet 2010, 28 pages

Dette publique, inquiétude publique
Jérôme Fourquet, juin 2010, 32 pages

Une régulation bancaire pour une croissance durable
Nathalie Janson, juin 2010, 36 pages

Quatre propositions pour rénover notre modèle agricole
Pascal Perri, mai 2010, 32 pages

Régionales 2010 : que sont les électeurs devenus ?
Pascal Perrineau, mai 2010, 56 pages

L'Opinion européenne en 2010
Dominique Reynié (dir.), Éditions Lignes de Repères, mai 2010, 245 pages

Pays-Bas : la tentation populiste
Christophe de Voogd, mai 2010, 43 pages

Quatre idées pour renforcer le pouvoir d'achat
Pascal Perri, avril 2010, 30 pages

Où en est la droite ? La Grande-Bretagne
David Hanley, avril 2010, 34 pages

Renforcer le rôle économique des régions
Nicolas Bouzou, mars 2010, 30 pages

Réduire la dette grâce à la Constitution
Jacques Delpla, février 2010, 54 pages

Stratégie pour une réduction de la dette publique française
Nicolas Bouzou, février 2010, 30 pages

Iran : une révolution civile ?
Nader Vahabi, novembre 2009, 19 pages

Où va l'Église catholique ? D'une querelle du libéralisme à l'autre
Émile Perreau-Saussine, octobre 2009, 26 pages

Agir pour la croissance verte
Valéry Morron et Déborah Sanchez, octobre 2009, 11 pages

L'économie allemande à la veille des législatives de 2009
Nicolas Bouzou et Jérôme Duval-Hamel, septembre 2009, 10 pages

Élections européennes 2009 : analyse des résultats en Europe et en France
Corinne Deloy, Dominique Reynié et Pascal Perrineau, septembre 2009, 32 pages

Retour sur l'alliance soviéto-nazie, 70 ans après
Stéphane Courtois, juillet 2009, 16 pages

L'État administratif et le libéralisme. Une histoire française
Lucien Jaume, juin 2009, 12 pages

La politique européenne de développement : Une réponse à la crise de la mondialisation ?
Jean-Michel Debrat, juin 2009, 12 pages

La protestation contre la réforme du statut des enseignants-chercheurs : défense du statut, illustration du statu quo.
Suivi d'une discussion entre l'auteur et Bruno Bensasson
David Bonneau, mai 2009, 20 pages

La lutte contre les discriminations liées à l'âge en matière d'emploi
Élise Muir (dir.), mai 2009, 64 pages

Quatre propositions pour que l'Europe ne tombe pas dans le protectionnisme
Nicolas Bouzou, mars 2009, 12 pages

Après le 29 janvier : la fonction publique contre la société civile ? Une question de justice sociale et un problème démocratique
Dominique Reynié, mars 2009, 22 pages

La réforme de l'enseignement supérieur en Australie
Zoe McKenzie, mars 2009, 74 pages

Les réformes face au conflit social
Dominique Reynié, janvier 2009, 14 pages

L'Opinion européenne en 2009
Dominique Reynié (dir.), Éditions Lignes de Repères, mars 2009, 237 pages

Travailler le dimanche: qu'en pensent ceux qui travaillent le dimanche ?
Sondage, analyse, éléments pour le débat
Dominique Reynié, janvier 2009, 18 pages

Stratégie européenne pour la croissance verte
Elvire Fabry et Damien Tresallet (dir.), novembre 2008, 124 pages

Défense, immigration, énergie : regards croisés franco-allemands sur trois priorités de la présidence française de l'UE
Elvire Fabry, octobre 2008, 35 pages

Retrouvez notre actualité et nos publications sur www.fondapol.org

SOUTENEZ LA FONDATION POUR L'INNOVATION POLITIQUE

Pour renforcer son indépendance et conduire sa mission d'utilité publique, la Fondation pour l'innovation politique, institution de la société civile, a besoin du soutien des entreprises et des particuliers. Ils sont invités à participer chaque année à la convention générale qui définit ses orientations. La Fondation pour l'innovation politique les convie régulièrement à rencontrer ses équipes et ses conseillers, à discuter en avant-première de ses travaux, à participer à ses manifestations.

Reconnue d'utilité publique par décret en date du 14 avril 2004, la Fondation pour l'innovation politique peut recevoir des dons et des legs des particuliers et des entreprises.

Vous êtes une entreprise, un organisme, une association

Avantage fiscal : votre entreprise bénéficie d'une réduction d'impôt de 60 % à imputer directement sur l'IS (ou le cas échéant sur l'IR), dans la limite de 5‰ du chiffre d'affaires HT (report possible durant 5 ans) (art. 238bis du CGI).

Dans le cas d'un don de 20 000 €, vous pourrez déduire 12 000 € d'impôt, votre contribution aura réellement coûté 8 000€ à votre entreprise.

Vous êtes un particulier

Avantages fiscaux : au titre de l'IR, vous bénéficiez d'une réduction d'impôt de 66 % de vos versements, dans la limite de 20 % du revenu imposable (report possible durant 5 ans) ; au titre de l'ISF, vous bénéficiez d'une réduction d'impôt de 75 % de vos dons versés, dans la limite de 50 000 €.

Dans le cas d'un don de 1 000 €, vous pourrez déduire 660 € de votre IR ou 750 € de votre ISF. Pour un don de 5 000 €, vous pourrez déduire 3 300 € de votre IR ou 3 750 € de votre ISF.

contact : Anne Flambert +33 (0)1 47 53 67 09 anne.flambert@fondapol.org

LA BLOCKCHAIN, OU LA CONFIANCE DISTRIBUÉE

Par Yves CASEAU et Serge SOUDOPLATOFF

Les grandes innovations sont le fruit du croisement de nouvelles possibilités technologiques et d'un contexte sociologique propice qui transforme ces technologies en usages. Ainsi, la blockchain est née, d'une part, de la rencontre de la cryptographie asymétrique et des systèmes distribués, et, d'autre part, d'un terreau sociologique opportun. Ce dernier résulte de la crise de confiance des citoyens envers les institutions, les amenant à chercher de nouvelles formes de gouvernance.

L'avènement d'Internet a démontré l'effectivité d'un système mondial de communication sans le besoin d'opérateurs de télécommunications. Désormais, il est possible de se connecter en quelques secondes à n'importe quel réseau Wi-Fi dans le monde. La blockchain permet la même révolution, mais appliquée aux transactions. Elle permet à des personnes de réaliser entre elles des opérations, notamment financières, qui sont garanties sans l'interaction d'un tiers de confiance. De ce fait, les échanges sont plus rapides et moins coûteux. Par conséquent, la blockchain remet totalement en question le rôle des institutions, banques, études notariales, et modifie en profondeur l'administration. Les premières expérimentations, qui vont bien au-delà du bitcoin, comme les organisations décentralisées autonomes, montrent le caractère radicalement disruptif de la blockchain.

La Fondation pour l'innovation politique

Les données en open data

data.fondapol

Le site internet

www.fondapol.org

Les médias

fondapol.tv

Linked in

Trop libre
Une voix libérale, progressiste et européenne

11, rue de Grenelle
75007 Paris – France
Tél. : 33 (0)1 47 53 67 00
contact@fondapol.org

9782364081048

ISBN : 978 2 36408 104 8

3 €