BLOCKCHAIN POUR L'ÉNERGIE

Karim Beddiar
Fabien Imbault

CAMPUS
D'ENSEIGNEMENT SUPÉRIEUR
ET DE FORMATION PROFESSIONNELLE

BLOCKCHAIN POUR L'ÉNERGIE

Applications et mise en œuvre dans la ville du futur

DUNOD

Illustration de couverture : © Wenjie Dong/iStock

11 rue Paul Bert, 92240 Malakoff
www.dunod.com
ISBN 978-2-10-077675-7

Préface

Pression démographique, métropolisation, vieillissement de la population, révolution des usages insufflée par les innovations technologiques et digitales… La ville connaît des mutations profondes qui redessinent les contours de l'expérience urbaine.

D'ici 2050, 67 % de la population mondiale vivra en ville. Face à cette métropolisation du monde, se dressent des défis tant sociaux qu'environnementaux, mais aussi de mobilité et de qualité de vie en ville. Pour concevoir des solutions urbaines durables et harmonieuses, je suis convaincu que la bonne échelle de réflexion et d'action est celle des quartiers – vecteurs de vie, de mixité et de dialogue.

Pour accompagner cette transformation inéluctable des villes, le domaine de l'énergie va devoir s'adapter à la demande des clients, plus exigeants en matière d'empreinte carbone. Il devra également suivre les évolutions attendues du marché, avec l'ouverture à la concurrence des réseaux d'énergie en Europe, concomitante avec l'arrivée de nouveaux systèmes de gestion décentralisés (smartgrids). Le temps est venu pour les aménageurs urbains de favoriser l'émergence d'un nouveau modèle énergétique urbain durable.

À ce titre, l'autoconsommation collective à la maille d'un quartier permettrait sans doute de développer un nouvel écosystème urbain qui réduirait la consommation de ces îlots urbains, encouragerait la production locale d'énergies renouvelables autoconsommées localement et abaisserait les coûts d'investissement dans les infrastructures de réseau.

Apparue dans le secteur financier, la technologie blockchain apparaît comme une solution adaptée à cet enjeu et ouvre vraisemblablement de nouvelles perspectives dans le domaine de l'énergie, susceptibles de générer d'importantes économies.

En effet, la blockchain offre une structure idéale pour organiser des transactions instantanées, sécurisées et transparentes au sein d'une communauté d'utilisateurs : elle constitue sans doute le tremplin qui manquait pour permettre l'essor des smartgrids d'énergie propre.

Même si la blockchain est annoncée par certains comme un changement aussi important que l'apparition des ordinateurs dans les entreprises dans les entreprises il y a 60 ans, il faut raison garder et valider, dès à présent, sa pertinence dans des expérimentations, afin de lever les freins inhérents à ces nouveaux modèles : technologiques, adaptations réglementaires et modèles économiques innovants.

Bouygues immobilier a toujours été un pionnier sur les technologies de rupture qui apportent de la valeur d'usage à nos clients : bâtiments à énergie positive (Green Office) avec 10 ans d'avance sur la réglementation, premier smartgrid (IssyGrid) opérationnel en France, premier promoteur à généraliser la maquette numérique (BIM) sur tous ses projets, premier promoteur à livrer la totalité de ses logements connectés…

C'est la raison pour laquelle nous avons lancé une expérimentation blockchain (décrite dans cet ouvrage), sur le territoire de la Métropole du Grand Lyon, au sein d'un consortium « Eureka Confluence », regroupant la collectivité territoriale, des industriels référents, des startups spécialisées et des consommateurs. Seuls, nous n'aurions pas cette même force d'innovation.

Je vous encourage à lire, comme moi, cet ouvrage qui apporte toutes les clés de compréhension sur la technologie de la blockchain, qui pourrait contribuer à faire émerger de nouveaux modèles économiques, donc de nouveaux emplois, en particulier dans le domaine de l'énergie urbaine, enjeu majeur des prochaines années.

Bonne lecture !

Christian Grellier,
directeur Innovation, Groupe Bouygues Immobilier

Remerciements

Cet ouvrage est le fruit de plusieurs mois de recherches sur un sujet émergent et complexe.

Nous tenons d'abord à remercier le CESI, en particulier sa direction générale et celle de la région Ouest pour leur soutien et leurs encouragements.

Merci à Monsieur Christian Grellier, directeur Innovation du Groupe Bouygues Immobilier d'avoir accepté de préfacer cet ouvrage.

Merci aux entreprises ayant accepté de nous fournir des études de cas et des illustrations, parmi elles : Bouygues immobilier, Solcrypto, Lutecium…

Enfin, nous souhaitons particulièrement remercier nos familles pour leur patience et leur compréhension.

Table des matières

Introduction générale

Les grandes révolutions économiques interviennent toujours à la convergence de deux phénomènes : d'une part l'émergence d'une source d'énergie et d'autre part une révolution des modes de communication. Au XIX^e^ siècle, la machine à vapeur a transformé l'imprimerie et la prolifération de l'imprimé a permis l'instauration de l'éducation publique. Au XX^e^, l'électricité, le téléphone, la radio et la télévision ont donné naissance à la société de consommation. Mais *via* des systèmes très centralisés.

Aujourd'hui, avec Internet et les énergies renouvelables, nous vivons la troisième révolution industrielle théorisée par Jeremy Rifkin (2016). Cette révolution découle d'une convergence des technologies de la communication et des énergies renouvelables, qui permet celle de la communication distribuée (avec par exemple les technologies sans fil) et des formes d'énergies distribuées (comme les microcentrales en réseau qui fonctionnent grâce aux *smart grids*).

Le développement de l'Internet des objets dans le secteur énergétique se fait autour de trois axes impliquant chacun tout un écosystème industriel et technologique : (i) les objets physiques, (ii) la connectivité et (iii) le traitement des données.

La croissance de l'Internet des objets dans le secteur énergétique se fait au rythme soutenu des évolutions technologiques. La blockchain fait partie de ces grandes innovations de rupture majeure de notre époque. Elle est davantage sociétale que technologique et peut à cet égard être comparée à l'arrivée d'Internet, car elle permet de faire émerger des usages et des modèles économiques innovants, notamment dans le domaine énergétique. Mais cette technologie reste encore alambiquée et loin d'être adoptée par le public. Il convient par conséquent de la rendre plus accessible avant de mettre en exergue ses nombreux bénéfices. Et c'est l'ambition de cet ouvrage : dans ce domaine complexe et balbutiant, nous avons essayé de définir avec pédagogie les concepts de la blockchain et d'en expliquer le fonctionnement en ciblant l'application dans le domaine énergétique.

Ce travail pourra servir de point d'appui méthodologique pour les différents acteurs industriels qui s'intéressent de près ou de loin à la blockchain. Il servira également aux acteurs de la formation : enseignants, formateurs et étudiants.

Cet ouvrage est construit en quatre parties complémentaires :

- Le premier chapitre introduit la blockchain, définit les concepts et explicite son écosystème et ses domaines d'utilisation.
- Le deuxième chapitre, à visée technique et technologique, a pour objectif d'expliquer les briques de base de la blockchain (structures des données, outils cryptographiques, réseau…).
- Le troisième chapitre explore l'utilisation de la blockchain comme outil de gestion énergétique dans la construction. Il traite du développement de l'autoconsommation, de la décentralisation de l'énergie et du rôle de la blockchain dans la certification de la qualité de service d'exploitation des *microgrids* énergétiques. Plusieurs exemples sont dressés et commentés.
- Enfin, le quatrième chapitre est consacré à la présentation de cas réels et d'applications de cette technologie. Ces études de cas sont décrites sous diverses facettes. Un zoom particulier est fait sur les volets énergétiques. L'objectif de ce dernier chapitre est de montrer l'étendue de l'utilisation de la blockchain sur le terrain et de donner un aperçu de la grande variété des projets et des enjeux actuels auxquels elle est liée.

La blockchain représente de nombreux avantages, parmi lesquels sécurité, transparence, disponibilité et déclinaison en multitude de cas d'usage. Elle permet d'optimiser les processus et de réduire les coûts de gestion pour mieux servir le client final.

Dans le domaine énergétique, on compte aujourd'hui plusieurs dizaines d'expérimentations dont la plus médiatique est celle d'échange d'électricité photovoltaïque entre habitants de President Street, à Brooklyn, aux États-Unis.

La blockchain représente un enjeu d'avenir, un objet d'innovation et de progrès formidable. C'est une technologie puissante au service du citoyen et de la ville de demain. C'est, en somme, une des solutions permettant de réussir la mutation numérique que traverse notre société.

Notre objectif dans cet ouvrage est de mieux vous faire comprendre cette révolution en cours. Nous ne traitons pas des aspects de programmation informatique relatifs à la blockchain, pour lesquels le lecteur pourra se reporter à d'autres

sources complémentaires. Nous avons pour ambition de donner aux potentiels utilisateurs de la blockchain une grille de lecture la plus complète possible leur permettant d'appréhender les concepts et la réalité d'utilisation de cette puissante technologie dans leur vie quotidienne et leurs projets en ciblant le volet énergétique.

Enfin, la blockchain étant une technologie balbutiante, la littérature, principalement anglophone, est riche avec des éclairages différents qui peuvent sembler parfois contradictoires sur certains aspects. Le lecteur souhaitant aller plus loin trouvera une bibliographique assez complète à la fin de cette ouvrage.

1

Les principes et enjeux de la blockchain

Ce premier chapitre dresse les principes et enjeux qui font de la blockchain une technologie de rupture. La décentralisation et la désintermédiation sont des tendances de fond de notre société, dont les conséquences se font sentir aussi dans nos habitudes et comportements énergétiques.

Nous essaierons ainsi de répondre aux quelques questions suivantes : Qu'est-ce que la blockchain ? Quels types de problèmes peut-elle résoudre aujourd'hui ? Qui sont ses acteurs et quelles sont leurs logiques économiques ? Quels sont les projets blockchain en lien avec l'énergie ?

Il est largement admis aujourd'hui que la blockchain dispose d'un potentiel pouvant révolutionner les marchés et redéfinir les règles de l'économie dans sa globalité. Les chiffres parlent d'eux-mêmes : depuis 2015 ce sont plus de 2 500 brevets qui ont été déposés sur la base de cette technologie. Rien que sur le premier trimestre 2016, plus de 1 milliard de dollars a été investi dans les start-up de la blockchain et, selon le World Economic Forum, 10 % du PIB mondial pourrait être créé sur des plates-formes blockchain en 2025. Rien d'étonnant donc à ce que le développement massif de cette technologie suscite des interrogations.

Pourquoi autant d'intérêt et d'engouement pour la blockchain ? Elle apparaît comme une innovation de rupture majeure de notre société, davantage sociétale que technologique, en permettant la décentralisation. À l'instar d'Internet, la blockchain ne présente pas d'innovation technologique qui lui soit propre, mais agglomère des technologies existantes de manière judicieuse pour faire émerger des cas d'usage et de modèles d'affaires innovants dans de nombreux domaines, notamment celui de l'énergie.

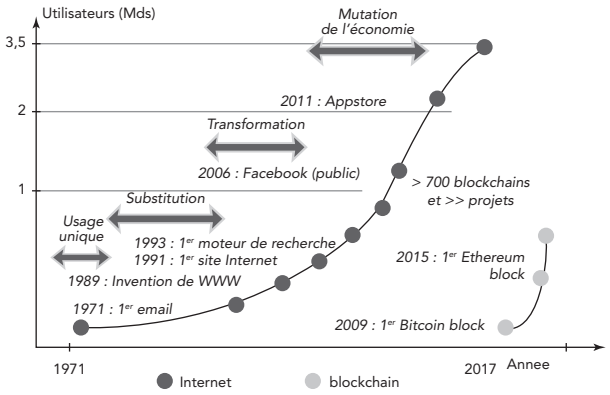

Figure 1.1 Parallèle entre le développement d'Internet et de la blockchain (Source : « The truth about blockchain and CGI Business Consulting Analysis », *Harvard Business Review*)

1.1 Qu'est-ce que la blockchain ?

La blockchain (littéralement : chaîne de blocs) est une solution technologique fondée sur les principes de la cryptographie, de l'informatique distribuée et de l'économie. Ces principes ont été initiés dès les années 1990 (Haber & Stornetta, 1990 ; Une, 2001) et popularisés à partir de 2008 grâce à l'essor du bitcoin. Fondamentalement, la partie la plus importante des chaînes de blocs n'est pas la partie technique, mais le réseau de liens entre les personnes. Il s'agit d'un concept apparenté à la confiance, mais dans une acception plus étroite. Par exemple, la confiance dans vos proches n'est généralement pas fondée sur la responsabilité – votre entourage ne s'attend pas à ce que vous produisiez des rapports précis sur tout ce que vous avez fait au cours de votre journée. Par conséquent, ce type de relation ne semble pas se prêter à une solution fondée sur une blockchain, ou une solution technologique en général.

L'obligation de rendre compte a déjà déclenché des révolutions économiques. Le système moderne de comptabilité en partie double a été largement adopté en Italie au XIII^{e} siècle et est devenu un fondement essentiel de l'essor européen pendant la Renaissance. À Florence, Giovanni de Medici a fondé une banque sur ces nouveaux principes comptables. Son fils Cosimo est devenu le souverain de Florence, et trois générations plus tard, l'un des arrière-petits-fils de Cosimo est devenu le Pape Léon X.

La plupart des applications de la technologie de l'information moderne dans les entreprises reposent sur des principes informatisés de ces mêmes

concepts : l'important est de disposer d'une source de vérité unique pour être sûr de savoir qui a acheté et vendu quoi, à quel prix. La banque joue ici un rôle central pour la confiance en la monnaie de tous les acteurs du système. Les sites web d'achats en ligne vérifient que vous pouvez faire un virement bancaire en échange du bien acheté et mettent à jour leur grand livre (ou « *ledger* ») des opérations comptables. En quoi une blockchain diffère-t-elle de cette architecture informatique usuelle ? Comment permet-elle de nouvelles formes de responsabilité entre les personnes (physiques ou morales) ?

Un mot-clé est la décentralisation. La blockchain permet d'avoir un grand livre distribué entre tous les acteurs et ne nécessite pas une autorité centrale qui dise : « Ces données sont fiables. » La *Distributed Ledger Technology* (DLT, ou technologie de registre distribué) désigne ce nouveau type de système. Les transactions entre utilisateurs s'effectuent non pas à partir d'une architecture client-serveur gérée de façon centralisée, mais de pair à pair, sans intermédiation.

La blockchain est donc une technologie de stockage d'informations protégées contre la falsification, la modification et la destruction. La cryptographie et la validation de toutes les transactions par l'ensemble des utilisateurs assurent la sécurité des données.

Le mathématicien Jean-Paul Delahaye utilise la métaphore du cahier pour permettre de mieux appréhender le concept : selon lui, la blockchain est « un grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible » (Fines Schlumberger, 2016).

Ce grand livre distribué offre un certain nombre d'avantages par rapport aux systèmes centralisés :

- **Transparence** : les grands livres centralisés sont sujets à la fraude et à l'abus, comme en témoigne une série de scandales financiers récents. Les blockchains offrent des enregistrements transparents et vérifiables pour chaque transaction, protégeant les détenteurs contre les systèmes pyramidaux ou l'utilisation de fausses pièces et d'autres formes de valeur frauduleusement dupliquée.
- **Immutabilité** : les grands livres centralisés offrent de riches cibles pour les pirates informatiques, qui attaquent régulièrement de tels systèmes, ce qui coûte à l'économie mondiale des centaines de milliards de dollars chaque année. Avec la technologie de la chaîne de blocs, une attaque sur un seul nœud a peu de ramification à l'échelle du réseau. Étant donné que chaque membre du réseau, ou nœud, détient une copie identique du grand livre partagé, les tentatives visant à pirater ou à modifier le grand livre seront rejetées par le

réseau élargi. En raison de ce processus cumulatif, l'enregistrement historique contenu dans une blockchain est immuable : les blockchains fournissent une « histoire commune » ou « vérité partagée » qui ne peut pas être modifiée.

- **Anonymat** : les données qui existent dans la chaîne de blocs sont anonymes et cryptées, ce qui rend l'information de peu de valeur pour la coercition, l'extorsion ou l'espionnage d'entreprise.

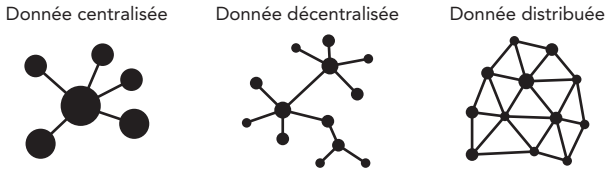

Figure 1.2 Différents types de distribution de la donnée
(Source : Peters *et al*. 2017)

Pour mieux comprendre les grands livres distribués, prenons du recul par rapport au contexte des ordinateurs et des systèmes numériques. Nous adaptons librement ici l'idée de prendre un exemple historique pour mieux illustrer le propos (Olavi Ojala, 2018). Le 4 juillet 1776, Étienne Girard, aventurier, orphelin d'origine bordelaise, débarque à Philadelphie (deux ans plus tard, il prend la nationalité américaine et change son prénom pour Stephen.) D'abord épicier, il sera successivement négociant, armateur et banquier et, après des années de travail acharné, il deviendra le premier millionnaire américain. L'écrivain Philippe Simiot a conté son parcours dans deux livres, *Carbec l'Américain* et *Le Banquier et le Perroquet* (Albin Michel, 2006).

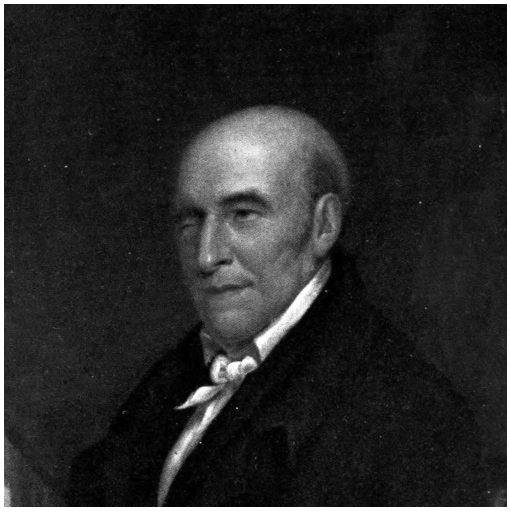

Figure 1.3 Stephen Girard
(Portrait posthume de Stephen Girard par J. R. Lambin)

En 1812, Stephen Girard est donc un homme riche, déterminé à aider les Américains dans leur lutte contre les Anglais. Il finance la lutte armée et ouvre le 18 mai sa propre banque aux États-Unis, la « Girard Bank ». Un jour d'août, un homme débarque à Philadelphie et se présente à lui avec un mandat pour une somme considérable en francs Napoléon. Le nom de la banque française indiqué sur le cachet officiel est bien connu de Stephen Girard : en échange d'une ligne de crédit confortable en France, il s'est engagé à accepter les mandats de ses partenaires français et à en honorer les montants dans les colonies américaines. Mais comment, dans ce climat troublé, faire confiance à un inconnu, qui pourrait très bien être un espion anglais ?

Dans les locaux parisiens de la banque, il y a un grand livre qui prouve que le compte de cet homme contient bien la somme demandée. Stephen Girard n'a cependant pas de copie de ce livre et demander des preuves de l'autre côté de l'Atlantique prendrait des mois. Comment distribuer l'information contenue dans ce grand livre sans avoir à envoyer des lettres à chaque demande ? Il y a deux façons de procéder.

Tout d'abord, la banque française peut envoyer les mêmes informations par plusieurs voies. En fait, c'est ce que les Français et Stephen Girard sont convenus de faire. Ils ont baptisé ce protocole « mécanisme de consensus à distance ». Pour tout mandat-poste, la banque enverra sur un autre navire une deuxième copie de la facture, confiée personnellement au capitaine. Lorsque (ou si) le deuxième navire arrive et que le capitaine se présente à la Girard Bank pour se porter garant de la facture avec une autre copie estampillée en main, son authenticité sera établie.

Une autre façon de distribuer le grand livre serait d'envoyer des factures vérifiées cryptographiquement. La banque et Stephen Girard partagent un livre de codes. La banque insère ainsi un message dans le mandat qui ne peut être décodé que par quelqu'un possédant une copie du livre de codes.

Le climat guerrier incite à beaucoup de prudence dans les affaires. La banque utilise donc d'une part la cryptographie pour rendre ses mandats vérifiables par le destinataire et d'autre part le consensus, en envoyant une copie des données par un homme de confiance – dans ce cas, le capitaine du deuxième navire qui a été payé par la banque pour prêter son autorité à la copie de la commande.

Aujourd'hui, l'envoi d'un message de l'autre côté de l'Atlantique et l'obtention d'une réponse sont instantanés, mais les problèmes de partage des grands livres n'ont pas disparu. Notre scénario de 1812 ne concernait qu'un mandat et quatre personnes : Stephen Girard, la banque française, l'inconnu demandant le

paiement et le capitaine du deuxième navire. Aujourd'hui, des milliards de transactions sont effectuées tous les jours. Les banques modernes gèrent ces grands livres de manière informatisée et décident qui peut payer ou recevoir de l'argent en continu. Elles agissent donc comme des tiers de confiance pour assurer la valeur des transactions.

Mais ce système si bien huilé ne fonctionne pas toujours. Des frais de transfert internationaux peuvent être prohibitifs. De nombreux pays ne disposent pas d'un système bancaire fiable. Certains sont ravagés par des guerres ou des catastrophes naturelles. Lorsque Médecins sans frontières réalise une intervention sanitaire, comment faire pour distribuer l'argent nécessaire aux actions d'urgence ? La blockchain permet de répondre à ces enjeux, avec un système qui ne dépend pas d'institutions de confiance. Elle combine deux caractéristiques que nous avons déjà vues dans le scénario de 1812 – le consensus et la vérification cryptographique – et les combine d'une manière inédite pour créer un système véritablement décentralisé où de multiples acteurs peuvent être des sources de vérité, avec des incitations partagées pour arriver à une vérité unique qui est ensuite enregistrée de façon permanente et par tous. Ces informations validées collectivement sont stockées dans des blocs identifiés de manière unique, et l'enregistrement permanent et mutuellement convenu constitue une « chaîne » où chaque bloc pointe vers le bloc précédent – d'où la dénomination « blockchain ».

Cette chaîne de blocs est très difficile à falsifier *a posteriori*. Le 22 mai 2010, Laszlo Hanyecz, un développeur habitant en Floride, a payé un utilisateur du forum *Bitcointalks* en bitcoins (BTC, le premier exemple de blockchain) pour deux pizzas de la marque Papa John's :

« Je paierai 10 000 bitcoins pour deux pizzas… peut-être deux grosses pizzas, pour qu'il m'en reste pour le lendemain. J'aime avoir des restes de pizza à grignoter plus tard. Vous pouvez cuisiner la pizza vous-même et l'apporter chez moi ou la commander, mais mon but est d'obtenir en échange de bitcoins de la nourriture livrée que je n'aie pas à commander ni à préparer moi-même, un peu comme commander un "plateau de petit-déjeuner" dans un hôtel ou autre : ils vous apportent juste quelque chose à manger et vous êtes heureux !

J'aime les oignons, les poivrons, les saucisses, les champignons, les tomates, les poivrons, etc. : les ingrédients standard, sans garniture de poisson bizarre ou quoi que ce soit de ce genre. J'aime aussi les pizzas au fromage ordinaires qui peuvent être moins chères à préparer ou à acquérir.

Si vous êtes intéressé, faites-le moi savoir et nous pourrons trouver un accord. »

« Pouvoir échanger [ces bitcoins] contre une pizza était extrêmement cool. […] Personne ne pensait que ça allait devenir aussi important. » – Laszlo Hanyecz

Laszlo Hanyecz a tout de même dû attendre trois jours avant de trouver quelqu'un prêt à lui vendre les pizzas pour la somme de 10 000 BTC. À ce moment, le système comptait encore très peu d'utilisateurs, manquait de liquidités, et le nombre de transactions était vraiment très faible.

Huit ans plus tard, le phénomène Bitcoin a pris une ampleur considérable. Au début 2018, avec un bitcoin valant 8 000 euros, les deux pizzas de Laszlo rapporteraient l'équivalent de 80 millions d'euros… De quoi donner des idées au *hacker* suffisamment doué pour arriver à modifier l'historique de transactions et s'approprier les bitcoins du pizzaiolo frauduleusement. Seulement, pour y parvenir, il faudrait modifier l'intégralité des blocs et c'est quasi impossible.

Les attaques sur Bitcoin où l'on tente d'inverser des transactions historiques qui datent de plus de quelques jours sont extrêmement coûteuses. Imaginons deux minutes que Laszlo Hanyecz soit maintenant un méchant et qu'il veuille inverser cette transaction regrettable pour son porte-monnaie. Pour réussir, il aurait besoin d'infiltrer le réseau bitcoin, de le contrôler et de recalculer les blocs pendant des centaines de jours afin de faire reculer la chaîne suffisamment loin avec ses propres données pour y remplacer des informations. Le coût d'exploitation du réseau Bitcoin pendant des centaines de jours serait de plusieurs milliards de dollars ; le système Bitcoin rend donc cette attaque économiquement impossible.

Cet exemple illustre pourquoi il est très difficile de modifier (on dit aussi « forger », de l'anglais « *to forge* ») l'histoire de la blockchain au fil du temps et pourquoi la structure de la chaîne est importante. En effet, même si vous réussissez à forger un bloc, vous devez forger aussi le précédent, sinon les autres nœuds peuvent facilement voir le changement par un contrôle facile du bloc précédent. Et ainsi de suite… Le système Bitcoin est ainsi optimisé pour des vérifications aisées par les utilisateurs lambda du réseau, et très cher pour les attaquants qui voudraient modifier les données *a posteriori*. Laszlo Hanyecz a donc bien payé les pizzas les plus chères de l'histoire de l'humanité et rentrera probablement dans le Guinness Book, le registre distribué Bitcoin fournissant la preuve infalsifiable de cette transaction.

Bien que nos exemples aient porté jusqu'à présent sur le transfert d'argent, n'oubliez pas qu'il s'agit en fait d'une question de transfert de valeur entre les personnes fondé sur la confiance. Les comptes et les valeurs représentés dans le registre distribué ne représentent pas nécessairement une opération financière. Il peut s'agir plus généralement de toute situation dans laquelle un ou plusieurs

acteurs observent un événement au sujet d'un autre acteur sur le réseau. Le principe de la blockchain est donc applicable à de multiples situations, bien au-delà des cryptomonnaies telles le bitcoin.

Dans la pratique, les événements que l'on peut stocker sur une blockchain se divisent principalement en deux catégories : la propriété et les promesses. Ce qu'une chaîne de blocs particulière prend en charge dépend de son protocole. Il en existe de très nombreuses variantes. Les premières blockchains largement déployées ne concernaient qu'un seul type de valeur (ou d'actif), les comptes contenant ces valeurs et les enregistrements des transactions entre ces comptes. Le grand livre de Bitcoin enregistre la propriété, et c'est tout.

D'autres exemples permettent de comprendre la diversité des systèmes d'échange de valeur. Pensez à un simple échange entre voisins, sans blockchain pour l'instant. Au Japon, une économie déconnectée de la monnaie nationale existe pour s'occuper des personnes âgées. Le *Fureai Kippu*, ou « ticket de relation cordiale », est un système de soutien fondé en 1994 par Tsutomu Hotta, ancien ministre de la Justice.

L'unité de base du compte est une heure de service effectuée auprès d'une personne âgée. Par exemple, si vous faites des courses pour une femme âgée ne conduisant plus, vous obtenez un crédit en fonction du nombre d'heures que vous y passez. Il est apparu que les personnes âgées ont tendance à préférer les services fournis par des gens payés en *Fureai Kippu* plutôt qu'en yens. Cela est dû à la confiance entre les membres du réseau, qui partagent une même éthique communautaire et sociale.

Le *Fureai Kippu* correspond aussi à une forme de promesse. Les aînés peuvent s'entraider et obtenir des crédits, mais il est aussi possible à un jeune habitant à Tokyo d'aider une personne âgée de son quartier pour obtenir des crédits et les transférer à ses parents qui vivent ailleurs. Ces crédits s'accumulent ; les utilisateurs peuvent aussi les conserver lorsqu'ils deviennent eux-mêmes malades ou âgés, puis les utiliser à leur tour en échange de services.

Ce genre de promesse peut être stockée dans une blockchain, qui sert ainsi de protocole distribué pour le réseau de soutien. Un jeton (ou « *token* » en anglais) représentant l'heure passée à aider une personne âgée peut permettre de vendre ou d'échanger avec quelqu'un d'autre sur la blockchain, qui est alors un moyen de matérialiser l'accord indéniable que nous devons faire les courses pour une voisine âgée, afin que nos parents reçoivent eux-mêmes un service.

Il existe une forme avancée de promesse que l'on appelle le contrat intelligent ou « *smart contract* », grâce auquel il est possible d'obtenir des participants un

comportement qui est automatiquement appliqué par la blockchain elle-même. On promet par exemple que si l'on reste coincé dans l'ascenseur, le réparateur qui interviendra en moins d'une heure gagnera 500 €, mais seulement 100 € sinon. Les incitations peuvent être très variées. Un autre *smart contract* pourrait faire en sorte que l'ascensoriste veille à limiter le nombre de pannes. Par exemple, s'il y a plus de cinq pannes par an dans la copropriété, la réparation pourrait devenir gratuite. Ces limites sont appliquées par la définition du *smart contract* qui est automatiquement traitée par les participants de la blockchain. Dans ce cas précis, un des participants peut même être une machine : l'ascenseur. Les règles sont visibles pour tous et ne peuvent pas être changées unilatéralement, d'où l'usage du terme contrat. La blockchain permet donc de penser de nouveaux usages, en particulier lorsqu'il y a de nombreux intervenants. L'intermédiation d'un assureur pour les pannes d'ascenseur pourrait être remplacée par un réseau mutualiste d'habitants et d'ascensoristes, avec des conditions préalablement négociées sous forme de *smart contracts*.

C'est d'ailleurs un des objectifs principaux de cet ouvrage : expliquer ce qui est possible (ou non) grâce à ces nouvelles technologies, dans le domaine de l'énergie plus spécifiquement.

1.2 Défis et enjeux

1.2.1 La diffusion des technologies blockchain

De nombreux cas d'usage sont envisageables. La plupart sont en émergence ou en cours de déploiement. Il est cependant difficile de dire actuellement si la blockchain permettra des transformations majeures dans tous les secteurs de l'économie et si ses avantages lui donneront un impact important tant au niveau de l'utilisateur particulier qu'à celui de l'industrie ou des services. Comme le souligne A. Lafuma, cofondateur de Blockchain Partner : « De manière générale, il faudra attendre un certain temps avant que des produits fonctionnels et innovants soient mis en place par de grandes entreprises. L'innovation arrivera plus probablement des start-up, et ce d'autant plus que le développement de projets blockchain au sein du système informatique des grandes banques affronte plusieurs obstacles, qui impliquent des efforts dont le retour sur investissement est aujourd'hui très difficile à évaluer. Ces limites tiennent en particulier au fait que les pratiques et processus habituels de sécurité (logiciels audités et autorisés en interne, par exemple) sortent des sentiers battus avec les projets blockchain. Par exemple, le fait que ces derniers soient fondés sur des réseaux *peer-to-peer* renverse la logique des environnements traditionnels qui reposent sur une architecture client-serveur » (Lafuma, 2017).

La confiance dans les processus mis en œuvre est ici un antécédent à une adoption généralisée de la blockchain. Son effectivité résultera d'un niveau de maturité suffisant, reposant sur le recours à la régulation et à la norme. Cependant le travail normatif s'appliquant à ce secteur est peu développé car la blockchain et les DLT sont encore en émergence (Kost de Sèvres, 2017 ; Peyrat & Legendre, 2017).

Face aux risques induits par l'utilisation de cette technologie, l'une des missions centrales des régulateurs est d'assurer la protection des utilisateurs. Ainsi en mai 2016 l'autorité des marchés (AMF) s'est associée à la publication d'une étude sur les DLT de l'Institut Louis Bachelier, qui permet de comprendre le rôle et le fonctionnement des DLT et d'analyser les enjeux liés à leur développement sur les marchés financiers.

En juin 2016, l'ESMA (*European Securities and Markets Autority*) a publié un Discussion Paper (La technologie de registre distribué appliquée aux marchés de titres) qui analyse les apports et les risques que les DLT engendrent sur les marchés de titres (ESMA, 2016).

Le Trésor britannique a publié de son côté un rapport en 2016 (« *Distributed Ledger Technology: beyond blockchain* »), qui souligne la nécessité d'établir pour les DLT un cadre réglementaire qui devra évoluer conjointement au développement des nouvelles implémentations et applications. Une régulation proportionnée, non figée, est ici envisagée afin d'accompagner les acteurs dans leurs activités sans ajouter de coût supplémentaire et contraindre le développement de l'innovation[1].

Aux États-Unis le Financial Stability Oversight Council (FSOC), qui regroupe des régulateurs dont la Securities and Exchange Commission (SEC) et le Treasury Department, a indiqué que du fait des risques et incertitudes liés à cette technologie et à ses applications, elle fera l'objet d'une surveillance par les acteurs du marché et les régulateurs financiers. « Les régulateurs doivent être en mesure de la maîtriser, d'exploiter ses avantages et de remédier rapidement à ses potentielles failles. » (Kara Stein, commissaire de la SEC, novembre 2015.)

En mars 2016, le commissaire du régulateur Commodity Futures Trading Commission (CFTC), C. Giancarlo, a proposé d'adopter une approche réglementaire de type « *Do no harm* », injonction éthique dont le but est d'éviter de renforcer

1. « Distributed Ledger Technology: beyond blockchain », A report by the UK Government Chief Scientific Adviser, 2016.

les causes de tensions. L'intervention établirait des principes pouvant inciter à l'investissement et à l'innovation en matière de DLT.

D'autres agences américaines telles que la Federal Trade Commission (FTC) et le Consumer Financial Production Bureau (CFPB) ont émis des avertissements concernant les risques associés aux monnaies virtuelles.

Ces discussions sur les risques supposés ou réels continuent régulièrement d'agiter les milieux financiers, avec des études des banques centrales ou des autorités de régulation.

1.2.2 Les enjeux de gouvernance

Une gouvernance efficace permettrait *a priori* de garantir une mise en œuvre de la blockchain qui protégerait les utilisateurs tout en s'assurant que le système résisterait aux risques systémiques et protégerait la vie privée.

Cependant, si la blockchain suscite l'intérêt des gouvernements et des banques centrales, ses impacts économiques étant de plus en plus prégnants, la façon dont la loi traite cette technologie reste largement à préciser (Plisson Fénéron, 2017 ; Markiewicz, 2017).

Deux grandes questions se posent ici : d'une part la gouvernance de la blockchain et d'autre part la valeur juridique des opérations conduites par le biais de cette technologie. L'enjeu majeur au plan des États est de garder une souveraineté effective sur la blockchain privée ou publique pour que le contrôle technique et le droit applicable à cette technologie ne soient pas imposés d'outre-Atlantique, comme ce fut le cas pour le GPS ou Internet.

Dans une blockchain privée, le droit à l'écriture est attribué par une organisation centralisée, l'autorisation de lecture pouvant être limitée ou publique comme on le voit pour des banques centrales ou des organismes de règlement et de livraison de titres. La chaîne fonctionne selon des règles internes opposables aux participants.

Une blockchain publique est au contraire caractérisée par une ouverture complète et décentralisée : chacun peut y accéder, effectuer des transactions et participer au processus de consensus. Il n'y a pas de tiers de confiance. Les opérations effectuées n'ont pas d'autre valeur juridique que celle donnée par les acteurs de la chaîne. C'est le modèle du bitcoin, marqué par une approche communautaire de l'économie. La cryptomonnaie n'a pas de valeur légale et les transactions sont uniquement reconnues opposables entre l'acheteur et le vendeur.