Les enjeux économiques de la *blockchain*

Par Patrick WAELBROECK
Professeur à Télécom ParisTech – Institut Mines-Télécom

La *blockchain* est une technologie qui va bien au-delà de l'horodatage, du bitcoin et de la sécurisation des transactions financières. Le développement d'un écosystème autour des objets connectés intelligents ne pourra sans doute pas se faire sans la *blockchain* (sous une forme ou sous une autre). La *blockchain* ouvre les portes de la liquéfaction du monde physique, de l'économie de la micro-transaction en temps réel et du partage intelligent de bases de données. Cependant, il est essentiel de distinguer les différents types de *blockchain*, en particulier les *blockchains* publiques des *blockchains* privées, car leurs propriétés économiques respectives sont très contrastées. Par ailleurs, les problèmes de gouvernance des *blockchains* publiques laissent à penser que la technologie *blockchain* ne pourra à elle seule assurer la confiance.

Introduction

La *blockchain* est une technologie. Elle correspond à un cahier sécurisé numérique décentralisé. Lorsqu'un nœud du réseau concerné veut enrichir ce registre d'un élément, tous les autres nœuds de la *blockchain* sont mis à contribution pour acter cet ajout de façon indélébile. Chaque bloc contient l'empreinte du bloc précédent, formant ainsi une chaîne de blocs de données. Une nouvelle entrée ne peut donc être ni falsifiée ni antidatée, car la *blockchain* est copiée sur l'ensemble des nœuds du réseau.

Nous discuterons *infra* les éléments disruptifs de la *blockchain*. En effet, il ne s'agit pas seulement d'un outil permettant de générer de la confiance en permettant de stocker des données sécurisées. Si les banques s'intéressent beaucoup à la *blockchain*, c'est aussi parce qu'il est possible d'y inscrire des transactions, ce qui ne coûtera alors que quelques centimes – contre quelques euros actuellement. La *blockchain* permet ainsi d'attester de manière irréfutable et datée le moment où a été effectuée une transaction : il s'agit d'une technologie d'horodatage généralisée. Un tel registre peut également servir à référencer des titres de propriété intellectuelle ou des données cadastrales. Certaines *blockchains,* comme la *blockchain* Ethereum, permettent d'exécuter un code sur les éléments de la *blockchain*. Ces codes appelés *smart contracts* ouvrent de nouvelles perspectives à l'Internet des objets.

Il existe principalement deux types de *blockchain* : les *blockchains* publiques et les *blockchains* privées. Elles diffèrent entre elles au travers des autorisations qui sont accordées aux nœuds du réseau. Dans le cas d'une *blockchain* publique, tous les nœuds sont autorisés à écrire dans celle-ci, et à y lire les données. À l'opposé, seul un petit nombre de nœuds sont autorisés à écrire dans une *blockchain* privée. Ainsi, les règles de validation pour ajouter un nouveau bloc diffèrent elles aussi. Par exemple, dans le cas de la *blockchain* publique Bitcoin, l'incitation à sécuriser les éléments de la *blockchain* est liée à l'obtention de bitcoins à travers deux mécanismes : un montant fixe par bloc miné et un montant variable lié aux frais de transaction du minage. Pour une *blockchain* privée, les incitations sont plutôt liées à la gouvernance de la *blockchain* (nous proposons *infra* une analyse économique des différents types de *blockchain*).

Quelles sont les autres raisons pour lesquelles un économiste devrait s'intéresser à la *blockchain* ? Il en existe au moins trois (que nous détaillerons dans la suite de cet article).

Premièrement, les *blockchains* offrent une perspective intéressante pour l'économie de la sécurité en créant un système décentralisé d'incitations à sécuriser un système informatique (nous présenterons les éléments d'analyse économique *infra*).

Deuxièmement, les *blockchains* et les *smart contracts* permettent de mettre en relation des agents de manière décentralisée, redéfinissant ainsi la notion d'entreprise et la nature du travail. Ils ont également un impact sur l'organisation des industries, puisque des agents peuvent partager des ressources informatiques, ce qui permet de réduire les coûts fixes d'entrée dans des secteurs qui nécessitent d'importants investissements dans des serveurs et du matériel informatique. Les *blockchains* représentent aussi un contrepoids aux tendances centrifuges des plateformes à plusieurs versants concentrant le pou-

voir de marché de certains acteurs de l'Internet (nous y reviendrons).

Nous proposerons de retenir le bitcoin comme objet d'une étude de cas présentée *infra*. Il s'agira pour nous, dans un premier temps, de mieux comprendre l'offre et la demande de cette crypto-monnaie. Nous ferons un détour important par la gouvernance du bitcoin, car les problèmes soulevés par celle-ci se posent également aux autres *blockchains*. Nous serons alors en mesure d'analyser la valeur économique du bitcoin.

Ensuite, la *blockchain* est également une innovation technologique qui peut se diffuser plus ou moins rapidement dans l'économie. Cette question fait actuellement l'objet d'un débat que nous présenterons dans la suite de l'article. Il s'agit de savoir si cette technologie est suffisamment disruptive pour connaître une diffusion très rapide ou si, au contraire, il s'agit d'une innovation transformative dont la diffusion complète dans le tissu économique pourrait nécessiter plusieurs décennies.

Quels sont les éléments disruptifs de la *blockchain* ?

La *blockchain* s'applique bien sûr aux produits numériques ou facilement numérisables. Mais la *blockchain* va bien au-delà de son utilisation comme simple registre numérique permettant un horodatage. Trois aspects méritent d'être soulignés : les *tokens,* les *smart contracts* et la liquéfaction du monde physique.

L'économie des *tokens*

La *blockchain* rémunère le travail de sécurisation au moyen de l'émission de jetons (*tokens*). Ceux-ci peuvent correspondre à de la crypto-monnaie, mais ils peuvent également être assimilés à des droits de vote. La valeur des *tokens* augmente avec le nombre de leurs utilisations possibles : ainsi, par exemple, il existe des externalités de réseaux positives directes et indirectes entre ceux qui possèdent des bitcoins et ceux qui les acceptent (nous y reviendrons *infra*). Les jetons peuvent également servir pour garantir des droits de vote lors d'une assemblée générale ou lors d'élections politiques.

Les *smart contracts*

Les *smart contracts* sont des bouts de code, qui, exécutés sur la *blockchain*, permettront de valider des tâches et les rémunérations liées.

Un premier exemple, celui d'Ubik. Dans le livre de Philip K. Dick (1969), Joe Chip, spécialiste de la traque des télépathes, habite dans un appartement loué. Il attend une visite et souhaite faire le ménage. Il appelle le service d'entretien de l'immeuble pour que celui-ci lui envoie des robots nettoyeurs. Tout le service de conciergerie est automatisé : le robot (ou le *chatbot*, dirait-on aujourd'hui) l'informe qu'il a une dette à éponger avant de pouvoir recruter les robots nettoyeurs. Comme il est sans le sou, il souhaite faire appel à un microcrédit en temps réel. Cependant, le robot l'informe également que la société de vente de crédits a abaissé sa note personnelle de crédit de triple G à quadruple G et bloque toute nouvelle demande de crédit. Il utilise une pièce de 10 *cents* pour mettre la cafetière en marche, mais il lui manque 5 *cents* pour pouvoir ouvrir la porte de son appartement pour faire entrer ses invités (qui finalement paient eux-mêmes pour ouvrir la porte). Il leur propose un café, mais le réfrigérateur est également automatisé et 10 *cents* sont nécessaires pour l'ouverture de la porte et 5 *cents* pour obtenir de la crème. Il s'agit d'une économie du micropaiement et de la microtransaction en temps réel (ici, l'emprunt bancaire). Cet univers économique a été présenté comme une alternative au *copyright* permettant de rémunérer les créateurs par Jason Lanier (2013). L'idée de la porte connectée d'Ubik est actuellement en développement chez Slock.it, qui réfléchit à une solution permettant de déverrouiller une porte sous condition de paiement.

Une liquéfaction du monde physique

La *blockchain* permet également de tracer et d'authentifier des personnes et des produits physiques grâce à des techniques d'empreinte, de reconnaissance numérique et à des capteurs. Il peut s'agir, par exemple, de tracer un numéro de série ou le « passeport » d'un objet physique dans la chaîne de production. Ces technologies font converger le monde physique avec le monde numérique en améliorant la traçabilité des produits et des services pour rendre l'économie plus « liquide ».

L'exemple d'un *daemon*. Un *daemon* est un programme informatique qui réside en mémoire et qui exécute des tâches lorsque certains événements se produisent. Il s'agit du prototype d'un *smart contract*, mais sans la dimension micropaiement. Daniel Suarez (2006) relate l'histoire d'un programmeur de jeux vidéo de génie, Matthew Sobol, qui orchestre après sa mort des exécutions automatiques sur des objets connectés : maison piégée, porte électrifiée, véhicule autoguidé tueur… Il ne s'agit pas vraiment d'intelligence artificielle, mais bien d'une exécution automatique conditionnelle distribuée. Le *daemon* auto-exécute des tâches grâce à des capteurs physiques qui lui permettent de détecter des événements réels. Il « suit » également les *news* sur Internet pour vérifier les séquences d'événements.

L'exemple d'Everledger. Everledger est une *blockchain* du diamant qui permet de tracer les transactions grâce à un système de passeport numérique attribué à chaque diamant. Les métadonnées de chaque diamant (sa taille, son diamètre, son poids, etc.) sont également enregistrées dans la *blockchain*.

Les propriétés économiques des *blockchains*

Les *blockchains* ont différentes caractéristiques économiques. Il est intéressant de les analyser en fonction des permissions de lecture et d'écriture, de rivalité et d'excluabilité, ainsi que d'externalités de réseau.

Les permissions d'écriture et de lecture

Il est important de distinguer les *blockchains* selon que l'on ait ou non besoin d'une permission pour y écrire des données et d'une permission pour en lire certaines des

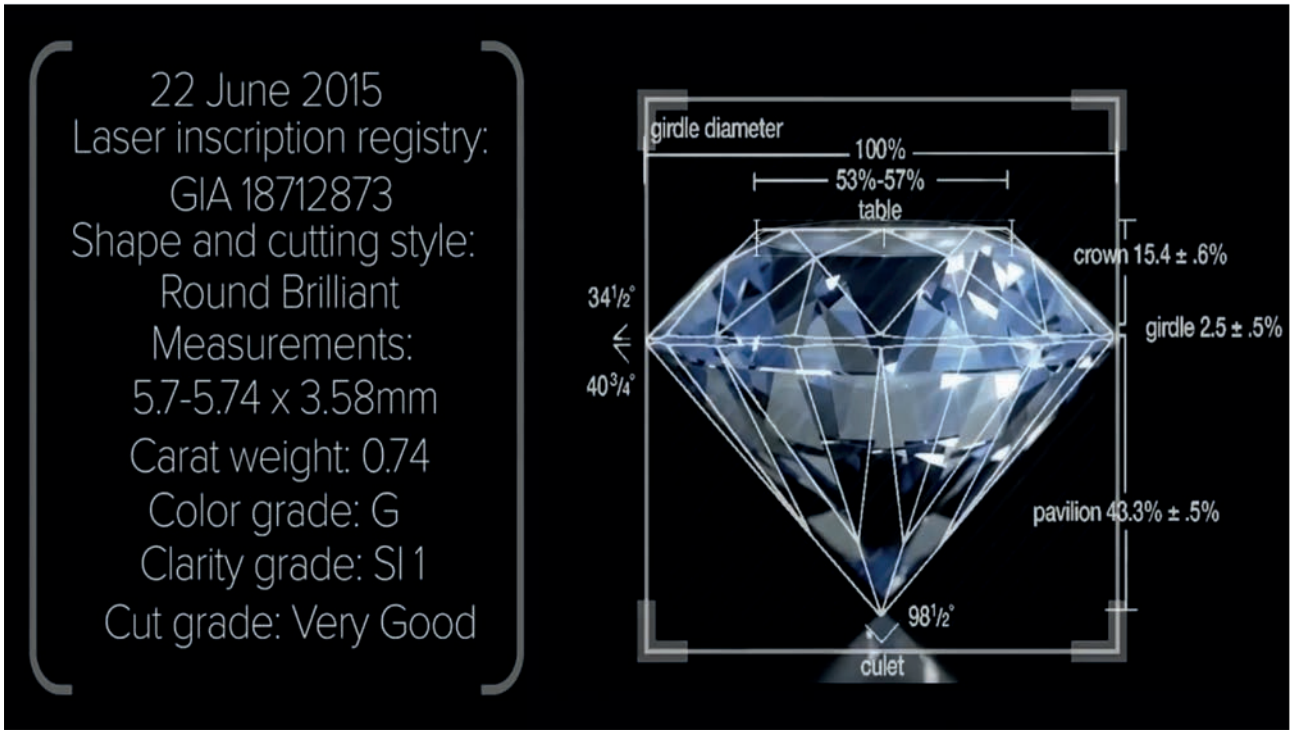

Figure 1 : Les spécifications quantitatives et qualitatives d'un diamant taillé répertorié dans la *blockchain* Everledger.
Source : https://www.altoros.com/blog/a-close-look-at-everledger-how-blockchain-secures-luxury-goods/ (consulté le 17 mai 2017).

données. Les quatre configurations des permissions possibles sont représentées dans le Tableau 1 ci-dessous.

	Permission de lecture	Sans permission de lecture
Permission d'écriture	*Blockchain* privée	*Blockchain* gouvernementale
Sans permission d'écriture	Surveillance/assurance	*Blockchain* publique

Tableau 1 : *Blockchains* avec ou sans permission de lecture et/ou d'écriture.

Deux configurations sont généralement discutées par les experts du domaine.

Premièrement, les ***blockchains* privées** nécessitent à la fois une permission pour lire les données stockées et une permission pour y écrire. Elles se développent très rapidement, car leur gouvernance est aisée et la confidentialité des données y est relativement garantie, puisqu'un nombre limité d'acteurs peuvent y accéder. Ce nombre limité d'acteurs permet également de déterminer facilement les responsabilités en cas de problème. Ce sont typiquement les *blockchains* correspondant à un usage spécifique, comme la *blockchain* Everledger (que nous avons citée supra).

À l'opposé, **les *blockchains* publiques** sont ouvertes à tous, ce qui pose des problèmes de gouvernance et de responsabilité. Ce sont les premières *blockchains* de crypto-monnaies, telles que le bitcoin et l'éther. La confidentialité de leurs données est garantie par l'utilisation de pseudonymes. Néanmoins, toutes les transactions correspondant à un pseudonyme sont visibles par tous et peuvent être explorées grâce à des outils de recherche, tels que *blockchain.info*. Les deux autres configurations de permission sont beaucoup moins répandues, mais elles sont également en train d'être développées. Comme exemple de *blockchains* sans permission d'écriture, mais avec permission de lecture, on peut penser à certaines *blockchains* gouvernementales, telles que des registres cadastraux. Ainsi, l'État américain du Delaware développe actuellement une initiative avec la *start-up* Symbiont.io pour automatiser son processus d'*Initial Public Offering* (IPO) (introductions en bourse) grâce aux *smart contracts*. En ce qui concerne les *blockchains* sans permission d'écriture, mais avec permission de lecture, on peut penser également aux *blockchains* de compagnies d'assurance qui monitorent les événements grâce à des objets connectés et qui déclenchent des remboursements automatiques grâce aux *smart contracts,* si les conditions sont satisfaites.

Rivalité et excluabilité

On considère qu'en général, les biens économiques présentent deux caractéristiques : leur rivalité et leur excluabilité. Les données stockées dans une *blockchain* restent non rivales. En revanche, le mode de gouvernance de la *blockchain* permet, dans certains cas, de priver certains utilisateurs du droit de lecture et/ou d'écriture des données. On est donc soit dans le cas de biens non rivaux et excluables, à savoir des biens de clubs, ou dans le cas de biens non rivaux et non excluables, c'est-à-dire des biens collectifs.

Considérons maintenant les jetons générés par la *blockchain*. Ces jetons sont des biens rivaux, une seule personne pouvant utiliser un jeton donné. En revanche, on peut empêcher certaines personnes d'y accéder (*blockchain* privée), auquel cas l'on a affaire à un bien privé. Si tout le monde peut accéder à la ressource, comme

dans le cas des *blockchains* publiques, on est en présence de biens communs.

Externalités négatives et externalités positives liées aux investissements en minage

Dans le cas des *blockchains* nécessitant un minage pour valider de nouveaux blocs, il existe deux types d'externalités de réseau directes.

Premièrement, il existe des externalités de réseau positives liées à la sécurisation de la *blockchain*. Ces externalités de réseau positives surviennent lorsque la valeur du produit ou du service augmente avec le nombre d'utilisateurs. Par exemple, la valeur d'un certain type de logiciel augmente avec le nombre de ses utilisateurs, car il est plus facile d'échanger des fichiers avec des amis, avec des collègues et avec d'autres contacts. Dans le cas de la *blockchain*, chaque nœud supplémentaire en renforce la sécurité, car il est plus difficile de mener des attaques de type 51 % ou de deviner le gagnant du processus de minage (attaques DOS – *Denial Of Service*) (nous développerons ce point *infra*).

Cependant, il existe aussi une externalité négative : chaque mineur, lorsqu'il investit dans du nouveau matériel, augmente son revenu marginal, mais il augmente aussi le coût global du minage, car la difficulté augmente avec le nombre des mineurs et avec leurs capacités de calcul (*hash-power*). Par exemple, pour le réseau bitcoin, la difficulté du problème de cryptographie à résoudre est validée par un consensus de *proof-of-work* qui augmente avec le *hash-power* global du réseau. Il y a donc un risque de surinvestissement dans la capacité de minage, car les mineurs individuels ne prennent pas en compte l'effet négatif sur l'ensemble du réseau.

Il est important de souligner qu'augmenter la difficulté du minage réduit les incitations à miner et augmente le temps de vérification, et donc l'efficacité même de la *blockchain*. Ce mécanisme rappelle la tragédie des communs dont les ressources partagées (le *hash-power*) dépérissent et ne sont entretenues que par une poignée de fermes et de *pools*, annulant de ce fait le principe même de la *blockchain* publique, qui se veut décentralisée. Il y a donc un risque que les capacités de minage soient fortement concentrées entre les mains d'un petit nombre d'acteurs, rendant caduc le principe même de la *blockchain*.

Les *blockchains* privées résolvent les externalités négatives de minage, au risque de créer une tragédie des anti-communs, qui traduit l'idée qu'il n'y aurait plus de ressources communes, mais uniquement des ressources privées protégées par le droit de la propriété privée.

Les externalités de réseau indirectes

Les *blockchains* mettent souvent en relation plusieurs groupes d'agents. C'est le cas des crypto-monnaies, qui apparient acheteurs et commerçants, ainsi que des plateformes mettant en relation emprunteurs et prêteurs, ou encore vendeurs et acheteurs de diamants (pour reprendre l'exemple d'Everledger). Ces différents types de marché partagent la caractéristique des marchés à plusieurs versants dans lesquels deux ou plusieurs groupes d'agents se rencontrent. Sur ce type de marché, il existe des externalités de réseau indirectes, souvent positives : la valeur du service proposé par la plateforme pour un groupe d'agents augmente avec le nombre des agents de l'autre groupe. Ces marchés sont typiquement très fortement concentrés dans l'économie numérique. On pense à des plateformes telles que YouTube, Google, Facebook, eBay, etc. Il est intéressant de souligner que les *blockchains* publiques ne sont pas centralisées, elles sont au contraire fortement décentralisées (nous reviendrons sur ce point *infra*).

Les différences entre *blockchains* privées et *blockchains* publiques

Comparons maintenant les avantages et les inconvénients des *blockchains* privées à ceux des *blockchains* publiques. Si la *blockchain* publique représente une solution de confiance décentralisée pour beaucoup, la *blockchain* privée peut être complètement centralisée entre un petit nombre d'acteurs, prenant le contrepied du rêve libertaire de la *blockchain* publique. Il est donc important de distinguer ces deux types de *blockchain*, qui diffèrent énormément sur le plan de la gouvernance.

L'une des différences majeures entre *blockchain* privée et *blockchain* publique est liée à la confidentialité des *smart contracts*, des transactions et des données.

Comme nous l'avons souligné précédemment, il est relativement facile de garantir la confidentialité des données stockées dans des *blockchains* privées, puisque seul un nombre limité d'acteurs peut y avoir accès, ce qui explique leur développement rapide.

Les données stockées dans les *blockchains* publiques sont au contraire accessibles à tous, puisqu'il s'agit de construire un registre public décentralisé. Cela dit, il est possible d'obtenir certaines formes de confidentialité dans les *blockchains* publiques qui utilisent des pseudonymes (c'est le cas pour le réseau bitcoin). Par ailleurs, certaines solutions techniques sont développées sur des *blockchains* publiques pour protéger les données sensibles. Ainsi, le projet Enigma du MIT (*Massachusetts Institute of Technology*) propose une *blockchain* de données de santé dans laquelle un nœud du réseau ne peut accéder à l'ensemble des données en utilisant une infrastructure *Secure Multiplatform Computation* : ces données sont réparties sur les différents nœuds du réseau et ne peuvent pas être entièrement révélées dans leur intégralité lors d'une requête. D'autres initiatives sont basées sur une technique de *zero knowledge proof* qui permet de vérifier la validité de transactions dont les métadonnées sont cryptées.

Les *blockchains* privées et les *blockchains* publiques diffèrent également sur deux autres dimensions : l'efficacité de la preuve et la gouvernance.

Premièrement, le passage à l'échelle est difficile sur une *blockchain* publique utilisant un consensus basé sur le *proof-of-work* (comme celui utilisé par le réseau bitcoin), puisque celui-ci demande un *hash-power* qui croît avec la taille du réseau et nécessite plusieurs validations avant

l'ajout d'un nouveau bloc, ce qui peut prendre une heure. D'autres types de consensus sont étudiés, comme le *proof-of-stake*, sur le réseau Ethereum. Les *blockchains* privées utilisent des consensus qui permettent d'écrire un très grand nombre d'informations à la minute, comme dans le cas d'un consensus basé sur la *delegated proof-of-stake*.

Deuxièmement, la gouvernance d'une *blockchain* publique nécessite un accord de l'ensemble des nœuds du réseau pour valider un changement majeur du protocole de validation des données (nous développerons ce point important dans la suite de cet article). Une décision peut être prise par un très petit nombre de nœuds, dans le cas d'une *blockchain* privée.

Enfin, se pose la question ouverte de la responsabilité. Les spécialistes de la *blockchain* en France considèrent qu'il est beaucoup plus facile d'établir les responsabilités dans le cas d'une *blockchain* privée (en particulier si les contrats ressortissent d'un même droit national). Dans le cas d'une *blockchain* publique internationale, cette question fait l'objet d'analyses légales.

	Blockchains privées	*Blockchains* publiques
Gouvernance	+	-
Externalités indirectes (plateformes multi-versants)	0/+	+
Externalités de sécurité	0	+
Externalités négatives de minage	0	-
Efficacité de la preuve	+	-
Externalité de sécurisation	0	+
Responsabilité	+	-
Ouverture et interopérabilité	-	+
Confidentialité	+	0
Monétisation	+	0

Blockchains et économie de la sécurité

Nous allons étudier maintenant les facteurs qui peuvent influencer les décisions des entreprises en matière de sécurisation de leur infrastructure informatique. Nous montrerons dans un premier temps que les forces économiques poussent les entreprises à sous-investir en la matière. Nous analyserons ensuite en quoi la *blockchain* permet d'apporter des solutions aux enjeux économiques de la sécurité informatique.

Prenons l'exemple des données de clients. Tout d'abord, il existe des externalités négatives associées au manque de protection des données qui ne sont pas compensées par les mécanismes du marché. Cela peut conduire à des situations dans lesquelles les données des clients sont exposées à des fuites, à des fraudes ou à des vols. Ensuite, les entreprises développent des stratégies leur permettant d'atteindre rapidement une masse critique, au détriment de leur infrastructure de données. Enfin, l'asymétrie de l'information par rapport au niveau de sécurité de l'infrastructure de données permet aux entreprises de partager les données personnelles de leurs clients avec des tiers qui ne sont pas forcément inciter à les protéger.

Les biens publics

Les biens publics sont non rivaux et non excluables. Ces deux caractéristiques impliquent qu'un seul agent ne peut pas capturer le surplus total qu'il crée pour l'ensemble de la société. Il y aura donc sous-investissement de la part du secteur privé. De plus, dans un écosystème de sociétés partageant des données, les membres individuels bénéficient des efforts des autres membres qui sécurisent le système. Dans l'ensemble de l'écosystème, les données seront donc faiblement protégées.

Les externalités des réseaux

Moore et Anderson (2012) étudient l'effet des externalités du réseau sur le niveau de sécurité mis en œuvre par les fabricants de logiciels. Il est important pour une entreprise qui veut dominer un marché grâce à de fortes externalités de réseau positives d'atteindre rapidement la masse critique. Dans ce contexte, il existe très peu d'incitations à consacrer du temps et des efforts à la sécurisation des données personnelles. Au contraire, il est plus profitable de laisser d'autres trouver des *bugs* et des trous de sécurité, puis de résoudre ces problèmes au moyen de mises à jour et de correctifs logiciels.

Les modèles d'affaires basés sur des échanges de données

Lorsque les entreprises développent des stratégies commerciales basées sur la publicité, elles génèrent des revenus en vendant les données de leurs clients à des tiers. Ces entreprises sont incitées à rédiger des conditions de service très générales pour pouvoir utiliser (et réutiliser) de manière exhaustive les données de leurs clients. Lorsque les données personnelles sont transférées à des tiers, il est vraiment difficile pour le client de déterminer comment ses données sont utilisées, stockées et sécurisées. Les ventes aux enchères en temps réel de données sur les *ad exchanges* exacerbent ces problèmes, car les données personnelles disponibles dans les *cookies* sont transmises et appariées par d'autres plateformes ou/et des sociétés tierces.

Les solutions apportées par la *blockchain*

La *blockchain* apporte des solutions aux problèmes de l'économie de la sécurité en incitant explicitement à la sécurisation. Dans le cas de la *proof-of-work* du réseau bitcoin, les incitations sont directement monétaires sous la forme de gains en crypto-monnaie. Dans le cas du *proof-of-stake*, la sécurisation permet de s'engager davantage dans la gouvernance de la *blockchain* et d'obtenir des parts dans les droits de vote. La gouvernance des *blockchains* permet également aux nœuds du réseau de se coordonner afin de contrer des attaques (voir BÖHME *et al*., 2015).

Malgré ces objectifs atteints en termes d'incitations, l'algorithme de *hash* du bitcoin est basé sur une technologie SHA-256 (*Secure Hash Algorithm*) qui risque de devenir obsolète. Par ailleurs, contrairement à la terminologie utilisée, les *smart contracts* ne sont que des bouts de code, qui peuvent contenir des *bugs*, comme tout programme informatique. On peut mentionner à cet égard le *smart contract* DAO, sur le réseau Ethereum, qui contenait un *bug* qui a permis à un groupe de *hackers* de subtiliser 50 millions de dollars. Enfin, les données sont protégées par une clé privée qui, si elle est perdue, empêche l'ac-

cès aux données stockées, mais qui, si elle est extorquée, compromet la sécurité des données.

Blockchains, nature de la firme et économie industrielle

La *blockchain* n'a pas seulement un impact sur l'économie de la sécurité. Elle peut remettre en question la définition même de l'entreprise, du travail et de l'organisation des industries numériques. Chaque industrie du numérique est aujourd'hui dominée par une entreprise en situation de quasi-monopole. Cette situation résulte principalement de deux forces économiques : premièrement, les investissements réalisés par les entreprises en place dans le matériel et l'infrastructure génèrent des coûts fixes de production et d'entrée sur le marché qui créent eux-mêmes des rendements d'échelle croissants ; deuxièmement, les externalités de réseau positives directes et indirectes présentes sur les plateformes à plusieurs versants créent une force centrifuge générant un « effet boule de neige ». Ces deux forces sont remises en question par la *blockchain*.

Smart contracts et *Dencentralized Autonomous Organizations*

La *blockchain* permet un système de vote décentralisé. Cela peut remettre en question le rôle même des structures hiérarchiques, dans lesquelles les décisions des travailleurs se situant au bas de l'échelle hiérarchique sont déléguées à un supérieur, en remontant successivement jusqu'au PDG. Grâce au système de vote permis par la *blockchain*, tous ces travailleurs pourraient, en principe, prendre eux-mêmes les décisions stratégiques. En poussant le raisonnement à l'extrême, on pourrait même se passer de PDG...

Il est souvent accepté, après les travaux de R. Coase (1937), que la taille de l'entreprise est déterminée par les coûts de transaction pour effectuer une tâche en interne ou en externe. La *blockchain* permet d'étendre les relations contractuelles à des fournisseurs et à des travailleurs à plus faible coût. En poussant le raisonnement plus loin, la *blockchain* a deux conséquences sur l'entreprise et le travail salarié. Premièrement, la notion d'entreprise est elle-même menacée : une industrie serait alors organisée autour d'une *blockchain* et de *smart contracts* conclus entre différentes unités de tailles relativement petites. Deuxièmement, le travail salarié serait également remplacé par du travail indépendant. Cette tendance est déjà visible sur des plateformes centralisées comme Uber, mais elle n'est pas contredite par l'avènement de solutions décentralisées comme les *blockchains*.

Entrée sur le marché et contestabilité

Si les coûts fixes liés à l'infrastructure informatique et matérielle découragent l'entrée sur le marché, la *blockchain* permet à des agents indépendants de mettre leurs ressources en commun pour exécuter des tâches automatisées. Les marchés redeviennent contestables et l'entrée de nouveaux consortiums pourrait représenter un défi pour les entreprises existantes (même pour celles disposant d'un quasi-monopole).

Décentralisation des marchés

Enfin, la *blockchain*, à travers la décentralisation des tâches et du travail, est à contre-courant de plateformes telles qu'Uber ou Airbnb. Reprenons l'exemple d'Ubik et de la porte intelligente : de fait, tout objet doté d'un verrou intelligent permet, par exemple, d'automatiser une location, de sécuriser des armes ou de gérer des coffres-forts. Cependant, même si certains observateurs avancent l'idée que la *blockchain* pourrait finir par « ubériser Uber », rien n'est moins sûr. En effet, Uber pourrait également développer sa propre *blockchain* pour automatiser ses contrats avec les chauffeurs. De la même manière, Airbnb pourrait développer sa *blockchain* pour automatiser le paiement des locations et de la conciergerie.

Étude de cas : l'exemple emblématique du bitcoin

Le réseau bitcoin est le premier réseau *blockchain* public à s'être développé de manière massive. On comptait, en mai 2017, près de 7 000 nœuds sur ce réseau. Chacun de ces nœuds peut cacher des *pools* (des ressources partagées) et des fermes de plusieurs milliers d'unités ASIC (*Application Specific Integrated Circuit*) développées pour miner les blocs. Les principaux *pools* et fermes sont localisés en Chine.

Le consensus basé sur le *proof-of-work* prévoit une augmentation de la difficulté du problème cryptologique à résoudre en fonction du *hash-power* global du réseau. Ainsi se pose, dans un premier temps, la question du coût de la *blockchain* publique. Le second point que nous aborderons sera celui de la gouvernance. Enfin, nous terminerons sur la valeur économique du bitcoin.

Le coût de la *blockchain* bitcoin

L'électricité représente la principale composante (entre 90 % et 95 %) du coût total d'une ferme de minage.

En 2015, Böhme *et al* (2015) évaluaient la consommation du réseau bitcoin à plus de 173 mégawatts d'électricité de manière continue. Cela représentait environ 20 % de la production d'une centrale nucléaire et un montant de 178 millions de dollars annuellement (au prix de l'électricité résidentielle aux États-Unis). Ce montant peut paraître important, mais Pierre Noizat estime que ce n'est pas plus que le coût annuel en électricité d'un réseau de DAB (distributeurs automatiques de billets) mondial, évalué à 400 mégawatts (http://e-ducat.fr/2015-11-28-cop21-et-blockchain/).

La gouvernance

La question de la gouvernance est cruciale pour comprendre le futur des crypto-monnaies. En effet, en cas de désaccord sur l'évolution du protocole de communication, le réseau risque de se diviser en plusieurs réseaux (*hard fork*) avec des monnaies incompatibles entre elles. La question la plus importante est liée au choix de la règle de consensus pour la validation de nouveaux blocs. Il faut parvenir à un consensus sur le consensus, ce que la technologie seule ne semble pas pouvoir fournir.

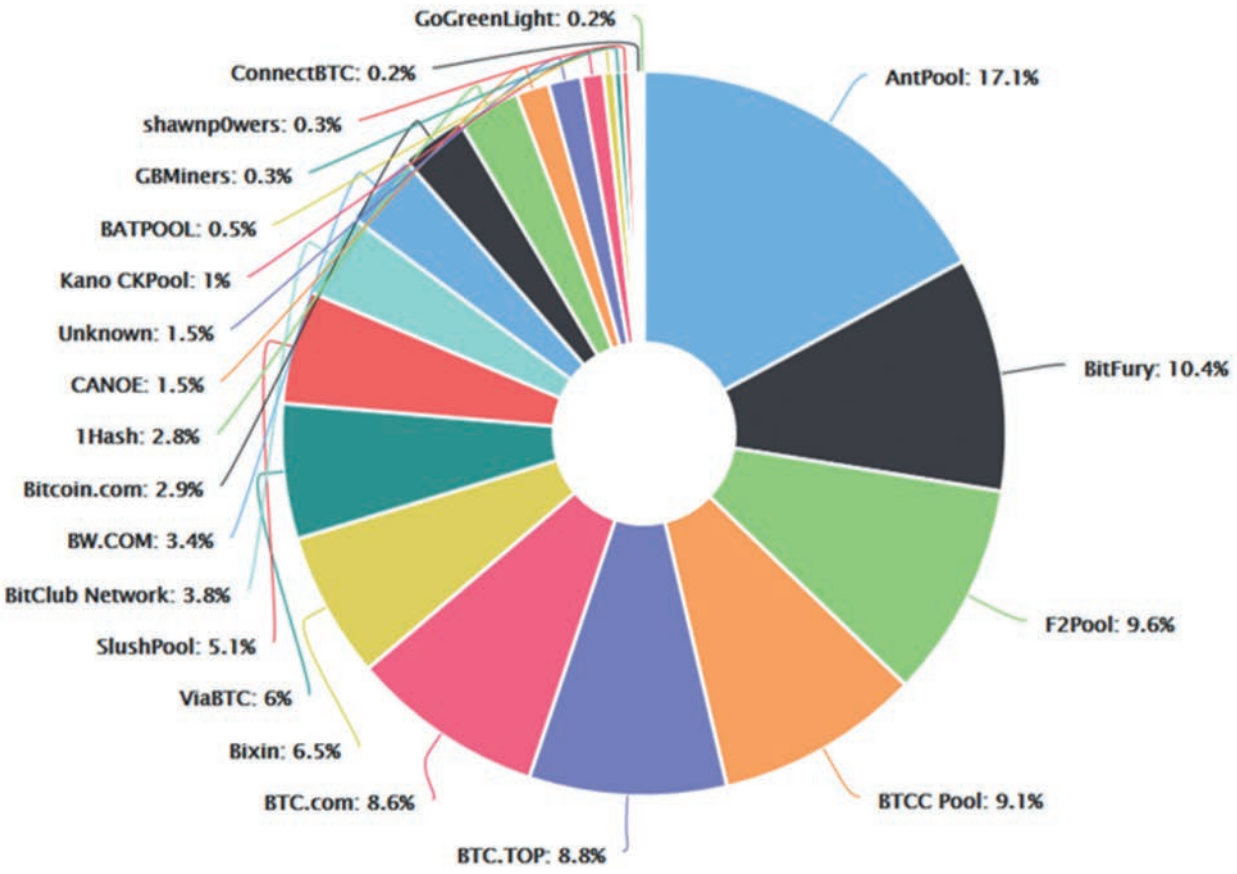

Figure 2 : Les partenaires *blockchain* du bitcoin.
Source : blockchain.info (consultée le 22 mai 2017).

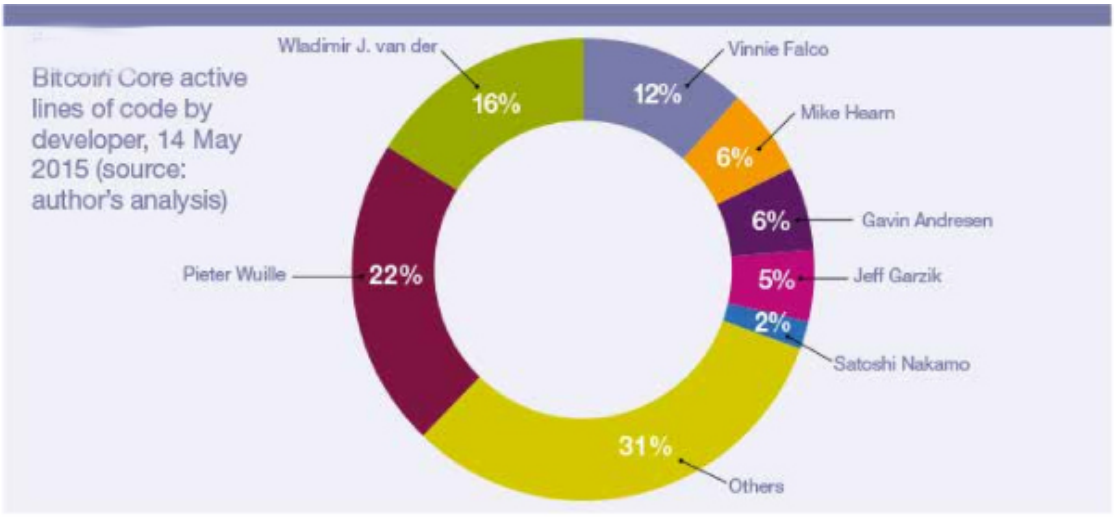

Figure 3 : Les principaux codes régissant le bitcoin et leurs développeurs (en mai 2015).
Source : WALPORT M. (2016).

Il faut noter que la répartition des *pools* indique clairement que le *hash-power* est concentré entre les mains d'une dizaine de *pools*, qui ont donc un pouvoir important lors de processus de décision en matière de changement des règles du protocole. Un protocole est l'équivalent de la grammaire pour une langue parlée. On peut ajouter ou retirer des règles, mais c'est au risque que les personnes ne se comprennent plus. Dans le cas du réseau bitcoin, on parle de *soft fork* et de *hard fork* lorsque l'on veut qualifier ces changements dans les règles.

Il existe plusieurs implémentations du protocole bitcoin : *bitcoin Core*, *Libbitcoin*, *bitcoin* XT, *bitcoin Classic*. Toutes ces implémentations sont globalement gouvernées par les core-développeurs. Par exemple, *Bitcoin Core* est gouvernée par un processus méritocratique d'évaluation par les pairs à travers un processus *Bitcoin Improvement Proposal* modéré par Wladimir Van Der Laan, lequel contribue de manière significative au codage du protocole bitcoin.

La gouvernance du protocole bitcoin est, quant à elle, décidée par les nœuds qui décident d'adopter tel ou tel changement d'implémentation. Le changement de protocole peut toucher les quatre couches du réseau bitcoin : la règle de consensus, la couche P2P, l'API (*Application Programming Interface*) et les applications (par souci de brièveté, nous ne discuterons que de la règle de consensus).

Pour ajouter une règle *soft fork*, une majorité de 95 % du *hash-power* est nécessaire ; les anciens blocs deviennent invalides et les nœuds *non upgradés* perdent en sécurité et en efficacité (*hash-power*). Pour forcer les mineurs à respecter les utilisateurs, une *soft fork* pourrait rendre le matériel de minage obsolète à travers un nouvel algorithme de minage. Pour retirer une règle *hard fork*, il est nécessaire que tous les nœuds complets adoptent le changement, sinon il y a un risque de voir le réseau bitcoin se diviser en deux réseaux non compatibles entre eux.

En conclusion, la technologie seule ne peut assurer la gouvernance. Il s'agit d'une situation paradoxale, dans la mesure où la technologie permet la décentralisation des vérifications et des exécutions automatiques, mais elle ne peut en garantir la gouvernance.

La valeur du bitcoin

Une crypto-monnaie n'a de valeur que si elle est considérée comme une monnaie par l'ensemble des participants au système monétaire. Elle nécessite donc d'être rare, au sens où elle ne peut pas être facilement copiée (problème équivalent à celui des faux billets, pour les monnaies traditionnelles). Cette propriété est satisfaite par le réseau *blockchain*, qui garantit l'absence de double dépense. En plus de cette valeur liée à l'acceptation, le bitcoin a de la valeur au travers de différents mécanismes économiques qui ne sont pas exclusivement monétaires. Nous les regrouperons à travers l'analyse de la demande et de l'offre de bitcoins. Nous commencerons par l'analyse des externalités de réseau et nous conclurons par une remarque sur le rôle joué par les monnaies alternatives dans un système monétaire.

Les externalités de réseau liées à la sécurité

Premièrement, le niveau de sécurité augmente avec le nombre des nœuds du réseau, car il faut d'autant plus de puissance de calcul pour compromettre la sécurité de la *blockchain* (à travers une attaque 51 %, *double spending* ou DOS). Par ailleurs, une attaque DOS est d'autant plus difficile à mener qu'il est difficile de deviner qui en est le bénéficiaire. Il existe donc des externalités de réseaux positives : la valeur du bitcoin augmente avec le nombre des nœuds participant au réseau.

Externalités de réseau indirectes positives liées au moyen de paiement

Le bitcoin est un moyen de paiement, au même titre que les espèces, les cartes bancaires ou les cartes Visa/Mastercard/American Express. Le bitcoin peut donc être appréhendé par la théorie des marchés à plusieurs versants qui modélise des situations dans lesquelles deux groupes d'agents économiques bénéficient d'externalités croisées. En effet, quand un consommateur choisit un moyen de paiement, il sera d'autant plus satisfait que ce dernier est accepté par le commerçant avec lequel il effectue une transaction. À l'inverse, pour un marchand, il est d'autant plus intéressant de proposer un moyen de paiement qu'il y a de clients qui le possèdent. Dès lors, la dynamique des marchés à plusieurs versants se traduit par des cycles vertueux qui peuvent connaître une phase d'amorce lente suivie d'une phase de déploiement très rapide. Si le bitcoin devait connaître une telle phase, sa valeur entrerait dans une phase d'accélération.

Par ailleurs, la commission payée par le consommateur ou le commerçant n'est pas contrôlée par une plateforme servant d'intermédiaire, mais par les mineurs (nous reprenons ce point dans la section suivante).

L'émission de monnaie sur le marché primaire

La création monétaire est divisée par 2 tous les 210 000 blocs pour arriver à un total de bitcoins en circulation (hormis ceux perdus) de 21 millions. Cette règle monétaire est contrôlée par le protocole bitcoin modifiable par le consortium *Bitcoin Foundation*, comme nous l'avons vu. La règle monétaire peut donc être modifiée pour répondre à des conditions de marché fluctuantes, au risque d'un *hard fork*. Par ailleurs, à demande constante, cette tendance à la baisse de l'offre de nouveaux bitcoins augmente automatiquement le prix du bitcoin. À terme, l'offre devenant inélastique, le prix du bitcoin (hors considérations spéculatives) est essentiellement déterminé par la demande.

La demande de crypto-monnaie

La demande de crypto-monnaie est issue de plusieurs préoccupations. Elle est également affectée par les incertitudes pesant sur sa pérennité.

Financial privacy

Les gouvernements limitent de plus en plus l'utilisation des espèces pour afficher leur lutte contre le blanchiment d'argent et le développement des marchés au noir. Le

cash est le seul moyen de paiement 100 % anonyme. Le bitcoin et les autres crypto-monnaies arrivent en deuxième position. En effet, le système de pseudonymat utilisé par le protocole bitcoin permet de masquer l'identité des personnes effectuant des transactions. Ainsi, certaines cryptomonnaies, comme le Zcash, masquent toutes les métadonnées d'une transaction.

Pourquoi utiliser un moyen de paiement anonyme ? Il existe de nombreuses raisons. Premièrement, l'utilisation d'un moyen de paiement anonyme permet d'éviter de laisser des traces qui peuvent être utilisées à des fins de surveillance par l'État, les employeurs et certaines entreprises (en particulier, les banques et les compagnies d'assurance). Ainsi, les entreprises et les banques pratiquent des stratégies de discrimination par les prix qui peuvent parfois se retourner contre les consommateurs. Laisser des traces par le paiement peut également pousser les entreprises à solliciter davantage les clients sur de nouvelles offres commerciales et la diffusion de publicités ciblées qui peuvent être considérées comme des nuisances par certains. Deuxièmement, payer avec un moyen de paiement anonyme limite également la sousveillance (ou surveillance inverse) par les proches. Ce sera le cas pour un paiement effectué à partir d'un compte commun. L'anonymat permet de limiter les externalités liées aux traces laissées lors d'un achat, il a donc une valeur économique. Le bitcoin, en permettant le pseudonymat, génère aussi de la valeur par ce biais.

Le bitcoin fonctionne en périodes de crise et permet donc d'éviter le contrôle des capitaux

Le bitcoin est apparu juste après la crise financière de 2008. Cette période a témoigné du pouvoir des gouvernements et des banques centrales en matière de contrôle des retraits d'espèces et du capital en circulation. Il n'existe que très peu de moyens d'échapper à ces deux contraintes institutionnelles. Le bitcoin en est un. En effet, même si les retraits d'espèces sont interdits, les possesseurs de bitcoins peuvent toujours payer en utilisant leur clé privée.

Les risques

Parmi les facteurs réduisant la demande de bitcoins, les risques liés à la réglementation et à la régulation ressortent tout particulièrement. D'une part, un État pourrait demander à ce que soient déclarées les plus-values générées par l'achat et la vente de bitcoins. Par ailleurs, les bitcoins peuvent être utilisés dans des secteurs réglementés (comme l'assurance ou la banque) et leur utilisation pourrait de ce fait également être réglementée. Enfin, il existe toujours le risque de perdre les données du disque dur sur lequel la clé privée est stockée, et donc de perdre les bitcoins associés, ou encore qu'un État impose son accès aux clés privées pour une question de sécurité.

La valeur du bitcoin sur le marché secondaire

Le bitcoin peut également être acheté et vendu sur une plateforme d'échanges. La valeur du bitcoin est alors plus proche de celle d'un investissement financier dont les acteurs anticipent les perspectives de gains et certains facteurs pouvant entraîner une appréciation du bitcoin.

Le bitcoin permet de discipliner les gouvernements

Le bitcoin (il en va de même pour les autres crypto-monnaies) peut être considéré comme une monnaie alternative non contrôlée par une banque centrale. Certains économistes, comme F. Hayek, considèrent que ces monnaies alternatives qui concurrencent la monnaie officielle permettent de discipliner les gouvernements qui seraient tentés de financer leur dette par l'inflation. Dans ce cas de figure, les consommateurs et les investisseurs se détourneraient de la monnaie officielle pour acheter la monnaie alternative et créeraient ainsi une pression déflationniste sur la monnaie officielle.

Perspectives économiques

La *blockchain* est inéluctable, car elle seule permettra le développement de l'Internet des objets. Cependant, la vitesse à laquelle cette transformation aura lieu est l'objet de débats entre spécialistes. Deux visions s'opposent : la vision de ceux qui pensent que la technologie prendra

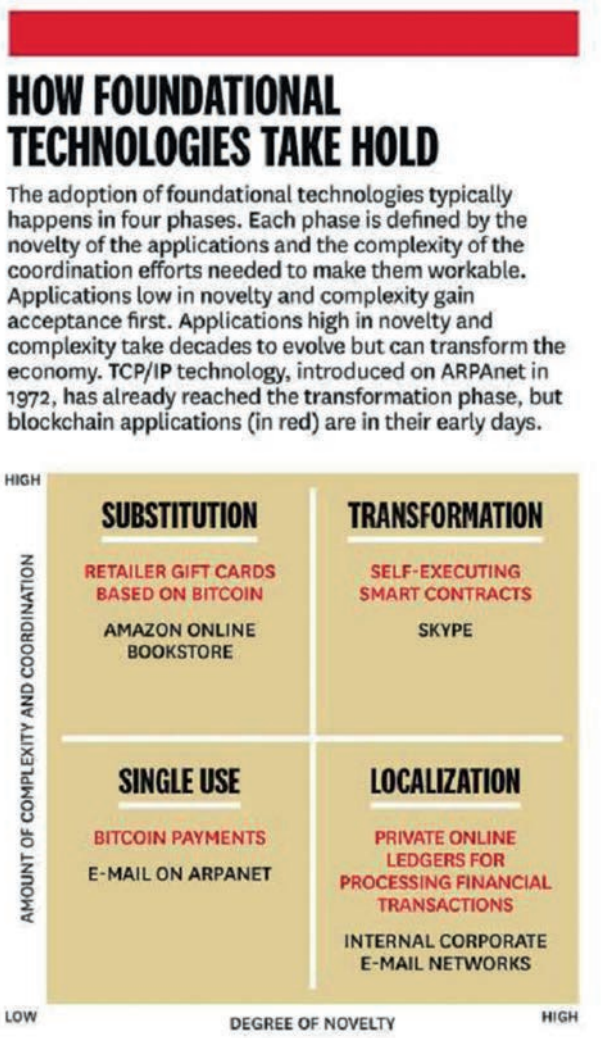

Figure 4 : Les quatre phases de l'adoption des technologies fondamentales : substitution, transformation, à des fins d'utilisation individuelle, à des fins de localisation (exemples illustratifs d'applications et de serveurs).
Source : LANSITI et LAKHANI (2017).

des décennies pour se diffuser et se transformer dans le tissu industriel, et la vision de ceux qui pensent qu'il s'agit d'une technologie disruptive.

La *blockchain* : est-elle transformative…

Lansiti et Lakhnani (2017) ont récemment suggéré que l'on pouvait établir un parallèle entre la diffusion d'une technologie transformative comme le protocole TCP/IP et la diffusion de la *blockchain*. Dans les deux cas, cette diffusion s'effectue en quatre phases qui peuvent prendre des décennies pour parvenir à la dernière, à savoir la phase transformative.

… ou disruptive ?

Au contraire, les spécialistes d'IBM voient dans la *blockchain* une technologie disruptive aux applications multiples allant de la logistique aux transactions financières.

Vectors of disruption	Liquification of the physical world
Unlock excess capacity of physical assets	Instantly search, use and pay for available physical assets
Create liquid, transparent marketplaces	Real-time matching of supply and demand for physical goods and services
Enable radical re-pricing of credit and risk	Digitally manage risk and assess credit, virtually repossess and reduce moral hazard
Improve operational efficiency	Allow unsupervised usage of systems and devices, reduce transaction and marketing costs
Digitally integrate value chains	Enable business partners to optimize in real-time, crowdsource and collaborate

Figure 5 : Cinq facteurs de disruption (1 – contre la puissance excessive des avoirs physiques ; 2 – en faveur de marchés plus liquides et transparents ; 3 – permettant une réévaluation drastique du crédit et du risque ; 4 – améliorant l'efficience opérationnelle ; et 5 – intégrant digitalement les chaînes de valeur) et leurs effets en termes de liquéfaction du monde physique.
Source : PURESWARAN et BRODY (2014).

Analyse

En première analyse, le protocole TCP/IP est à la fois similaire à la *blockchain* d'un certain point de vue et différent d'un autre. En effet, le protocole TCP/IP est un protocole ouvert, tout comme l'est la *blockchain* publique. En revanche, le protocole TCP/IP était au départ une affaire de spécialistes, alors que le bitcoin et la deuxième génération de la *blockchain* ont été très rapidement adoptés par des millions d'utilisateurs. Au final, la *blockchain* représente plus une technologie disruptive vouée à être adoptée massivement, qu'une technologie à diffusion lente. Mais il reste des verrous, qu'il est nécessaire de faire sauter (que nous présentons dans notre conclusion, ci-dessous).

Conclusion

En conclusion, la *blockchain* est une technologie révolutionnaire qui n'est pas limitée exclusivement au bitcoin. Le développement d'un écosystème autour des objets connectés intelligents ne pourra sans doute pas se faire sans la *blockchain* (sous une forme ou sous une autre). La *blockchain* ouvre les portes de la liquéfaction du monde physique, de l'économie de la micro-transaction en temps réel et du partage intelligent de bases de données. Cependant, un certain nombre de verrous doivent encore sauter. Premièrement, il s'agit d'établir clairement les responsabilités et le droit applicable aux *blockchains* publiques. Deuxièmement, il faudra garantir en Europe l'application de la protection des données personnelles (*General Data Protection Regulation* – GDPR). Troisièmement, il faudra déterminer le statut fiscal et juridique des crypto-monnaies. Enfin, quatrièmement, il faudra réfléchir à la manière d'articuler les *smart data* issues des *blockchains* avec le principe de neutralité du *Net* en Europe.

Bibliographie

BÖHME R., CHRISTIN N., EDELMAN B. & MOORE T. (2015), "Bitcoin: Economics, technology, and governance", *The Journal of Economic Perspectives* 29(2), pp. 213-238.

BRODY P. & PURESWARAN V. (2014), *Device democracy: Saving the future of the internet of things*, IBM, September.

COASE R. H. (1937), *The Nature of the Firm*, Economica 4(16), pp. 386-405.

DICK P. K. (1969), *Ubik,* trad. Alain Domrémieux (1999), Éditions 10/18.

LANIER J. (2013), *Who Owns the Future?*, Simon & Schuster.

LANSITI M. & LAKHANI K. R. (2017), *The truth about blockchain*, Harvard Business Review 95(1), pp. 119-127.

MOORE T. & ANDERSON R. (2012), *Internet security, The Oxford Handbook of the Digital Economy,* Oxford University Press.

SUAREZ D. (2006), *Daemon,* Verdugo Press.

WALPORT M. (2016), *Distributed Ledger Technology: Beyond Blockchain,* UK Government Office for Science.