HAL
open science

Risques et opportunités stratégiques d'une nouvelle grappe technologique : Les registres distribués numériques

Marc Lassagne, Laurent Dehouck

To cite this version:

Marc Lassagne, Laurent Dehouck. Risques et opportunités stratégiques d'une nouvelle grappe technologique : Les registres distribués numériques. Congrès Lambda Mu 21 " Maîtrise des risques et transformation numérique : opportunités et menaces ", Oct 2018, Reims, France. hal-02074330

HAL Id: hal-02074330

https://hal.science/hal-02074330

Submitted on 20 Mar 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Risques et opportunités stratégiques d'une nouvelle grappe technologique : Les registres distribués numériques

Risks and strategic opportunities of a new technology cluster: Distributed digital ledgers

Marc Lassagne
Ecole Nationale supérieure d'Arts et Métiers et
IAE de Paris (GREGOR, EA 2474)
Marc.lassagne@ensam.eu
151, boulevard de l'hôpital
75013 Paris

Laurent Dehouck.
Université de Rennes et
IAE de Paris (GREGOR, EA 2474)
laurent.dehouck@ens-rennes.fr
Ecole Normale Supérieure de Rennes
Campus de Ker Lann- Avenue Robert Schuman – 35170 Bruz – France

Résumé

Cet article porte sur les enjeux stratégiques, les risques et les opportunités de la grappe technologique des registres numériques distribués. Il propose une nouvelle méthodologie dans une perspective de gestion stratégique des risques pour en apprécier l'impact et bâtir des réponses adaptées.

Summary

This article examines the risks and opportunities associated with distributed ledgers technologies. A novel methodology is developed and presented in order to diagnose and manage their impacts using a strategic risk management perspective. Possible responses to the identified challenges are suggested.

Introduction

Le concept de chaîne de blocs (*blockchain*) a été développé dans un article en 2008 rédigé sous le pseudonyme de Satoshi Nakamoto (Nakamoto, 2008). Il visait la création de la première crypto-monnaie, le *bitcoin*, dont la première transaction a eu lieu en 2009. A cette époque, il fallait 10 000 bitcoins pour acheter une pizza quand aujourd'hui on a environ 1000 pizzas pour un bitcoin. La capitalisation des échanges est de 119 milliards environ et toutes les dix minutes de nouvelles transactions validées et infalsifiables s'ajoutent sur le registre et sont distribuées entre tous les détenteurs de *bitcoins*.

Cette technologie est une application d'un ensemble plus vaste d'innovations appelé Technologies de Registres Distribués (*distributed ledger technologies* ; nous y ferons désormais référence par leur abréviation TRD). Elle combine deux socles pivots :

- La confiance permise par l'usage de protocoles de cryptographie, qui valident des transactions partagées par tous les membres du réseau. En pratique les tiers de confiance indispensables à la garantie des transactions des actifs sont rendus obsolètes : les États, les banques et notamment les banques centrales, les assureurs, les notaires, etc.
- L'architecture distribuée du registre des transactions, qui empêche tout piratage, dans la mesure où il faudrait pouvoir pirater toutes les copies du registre de transaction, présentes sur un nombre potentiellement important d'ordinateurs.

Par analogie, de nombreux historiens de l'économie font de l'invention de la comptabilité en partie double en Italie en 1494 le moteur principal du développement de la Renaissance et de l'économie capitaliste (Sombart, 1902). Certains aujourd'hui comparent la « révolution blockchain » (Swan, 2015 ; Walport, 2015 ; Tapscott et Tapscott, 2016) à cette innovation comptable pour la société numérique qui se construit sous nos yeux. En revanche, d'autres auteurs considèrent avec beaucoup de réticence le *bitcoin* et sa technologie sous-jacente, comme par exemple Tirole (2017) et Krugman (2013).

Cet article décrypte les caractéristiques principales des TRD et leurs effets potentiels, en adoptant une démarche de gestion stratégique des risques. En effet, comme nous le verrons, tous les niveaux de l'entreprise sont susceptibles d'être soumis aux impacts de ces technologies. Ceci nous permettra, après avoir expliqué ce qu'elles recouvrent, de présenter quelques exemples de leur utilisation, de poser les bases d'un diagnostic stratégique, et d'envisager, à travers les risques et les opportunités associées aux TRD, des réponses stratégiques possibles.

Le concept

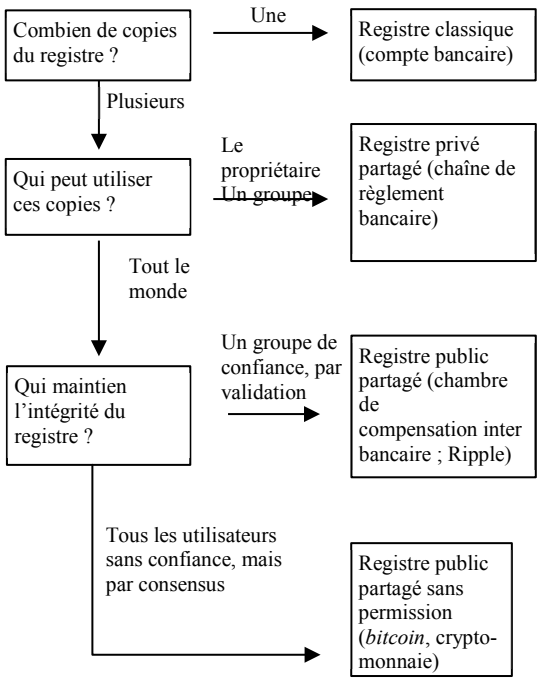
La grappe d'innovations des registres distribués[1], dont les applications « bitcoin », « ethereum » (avec la crypto-monnaie associée *Ether*) ou « ripple » constituent les exemples les plus médiatiques, combinent ensemble différents principes de fonctionnement qui apportent de la transparence, de la sécurité et de la traçabilité à faible coût.

Ces objectifs étaient autrefois exclusivement remplis par une architecture informatique centralisée pilotée le plus souvent par un tiers de confiance. Pour la monnaie, il s'agissait des banques centrales, ce qui, par le relais des banques privées et de leurs agences, jusqu'à chaque client final, imposait (et impose encore dans la majorité des cas à l'heure actuelle) des architectures clients/serveurs pour piloter et contrôler les opérations et assurer ainsi la sécurité nécessaire pour tenir des registres fiables (les comptes bancaires). En cas de désaccord sur une transaction, la vérification repose sur le registre centralisé des transactions de la banque. C'est aussi le cas dans d'autres domaines, comme par exemple pour l'identité à travers les fichiers biométriques constituées pour les passeports dans de nombreux pays pour éviter le vol ou la contrefaçon des pièces d'identités.
L'intérêt du développement des TRD provient des réponses qu'elles apportent au principal écueil des bases de données centralisées[2] : la confiance que l'on accorde bon gré ou mal gré au gestionnaire de cette base de données. On peut illustrer cette idée par la question de la gestion des données personnelles. L'opérateur de la base de données peut en effet détourner aisément les données recueillies à des fins différentes de ceux et celles qui les ont produits (censure, corruption, perte de données, ventes des données…). À l'inverse, les TRD permettent de s'assurer que la base de

[1] Il convient d'insister sur le fait que les chaînes de blocs ne sont qu'une manière parmi d'autre de mettre en œuvre des TRD. Il existe en particulier en ce qui concerne la recherche du consensus (c'est-à-dire le fait que l'ensemble des participants au registre sont tous d'accord sur la valeur que prennent ses éléments, qu'il s'agisse de transactions financières ou d'autres données) d'autres algorithmes (comme par exemple le *hashgraph*).
[2] Nous utiliserons indifféremment le terme de registre et de base de données. Les nuances entre ces termes seront négligées pour des questions de clarté d'exposition.

données soit partagée sur un réseau de multiples sites, institutions, acteurs, tous garants de son intégrité. Tous les participants ont leur propre copie du registre et celui-ci est régulièrement vérifié et mis à jour (toutes les 10 minutes environ pour le *bitcoin*) par le biais d'algorithmes spécifiques. Par exemple, la chaîne de bloc du *bitcoin* fonctionne de la manière suivante : Lorsqu'une transaction est amorcée entre deux individus, le premier encrypte avec une clé privée le montant et la nature de la transaction, qui sera décryptée par le destinataire avec la clé publique correspondante. Afin de s'assurer que la personne émettrice dispose bien des fonds (ou ne procède pas à des doubles paiements avec la même somme), il s'agit de vérifier dans le registre (dont tout le monde dispose d'une copie) que c'est bien le cas, puis de valider la transaction. Le problème est alors de se prémunir contre la possibilité de validation de transactions incorrectes par des agents non-coopératifs : ceci justifie d'avoir une validation collective, qu'il s'agit toutefois d'organiser. Tout d'abord, pour des raisons d'optimisation, plusieurs transactions sont agrégées dans un bloc, auquel sera affecté un code appelé *hash*. Les nœuds du réseau entrent alors en compétition pour résoudre un problème mathématique fondé sur le *hash* du bloc et donc valider les transactions correspondantes. Un bloc de transactions pourra être considéré comme valide lorsque l'un des nœuds du réseau aura résolu ce problème, la vérification de cette résolution étant ensuite quasi-instantanée par l'ensemble des membres du réseau. Les participants à cette compétition sont appelés des mineurs, par analogie avec les efforts accomplis par les chercheurs d'or dans une mine, dans la mesure où celui qui résout le problème est rémunéré en *bitcoins*. Le coût en ressources de calcul pour résoudre le problème mathématique et le fonctionnement des règles de validation découragent, voire rendent impossible une fraude[3].

Cet exemple n'est qu'un point de départ auquel s'ajoutent de très nombreuses innovations complémentaires ou alternatives en termes de protocole algorithmique, de technique cryptographique, de règles de signatures digitales, ou d'opérations automatiques. Le registre peut par ailleurs comptabiliser toutes formes d'actifs : financiers, légaux, physiques ou électroniques. Il est également possible de spécifier des droits d'accès particuliers, comme l'illustre la typologie ci-après :



Parmi toutes les autres innovations qui constituent la grappe technologique des registres distribués, le concept de *smart contract* (contrat intelligent), qui désigne de manière abstraite l'automatisation d'une procédure contractuelle doit être souligné. Au lieu d'être stocké sous la forme traditionnelle d'un document juridique, le contrat est formalisé par un algorithme qui s'exécute automatiquement dans un registre distribué (et dont l'exécution est donc enregistrée par tous ceux qui disposent d'une copie du registre). Ceci permet de diminuer très fortement les coûts de conformité, d'exécution et donc de transaction. On peut d'ailleurs interpréter les crypto-monnaies comme une succession de « contrats intelligents [4] » qui permettent d'opérer des transferts de propriété : lorsqu'une transaction a lieu entre deux agents, un transfert de propriété s'opère, et tous les participants au système disposent d'un enregistrement de cette transaction.
Ces technologies sont à l'origine de nombreux développements, dont nous allons maintenant présenter quelques exemples.

Des exemples d'application

La combinaison innovante des TRD ouvre des possibilités d'applications dans de très nombreux domaines. Sans souci d'exhaustivité, nous allons décrire quelques exemples concernant l'assurance, la finance, le secteur public, l'industrie et la propriété intellectuelle.

Dans le secteur de l'assurance, la technologie des contrats automatiques permet le déclenchement d'une indemnisation immédiate à partir du moment où le sinistre concerné se produit. C'est le cas par exemple de l'assurance fizzy, développée par Axa, qui vise à couvrir les retards aériens. Dans le cas du retard d'un avion, une indemnisation est automatiquement versée au souscripteur du contrat, sans qu'il y ait besoin de justification. En effet, en amont, la souscription donne lieu à un contrat stocké dans un registre distribué (ce qui empêche une modification ultérieure et assure sa sécurité), contrat dont le paramètre de déclenchement (le retard) est alimenté par des bases de données publiques d'heure d'arrivée des avions par rapport à leur heure prévue. De ce fait, l'indemnisation est simplifiée, plus rapide, et les coûts administratifs associés à la gestion du contrat se retrouvent fortement diminués.

De nombreuses initiatives voient également le jour en finance, dans trois domaines essentiellement : la validation des transactions financières, la distribution des produits bancaires, et le financement (de Vauplane, 2017). Sur ce dernier point, les ICO (*Initial Coin Offering*) sont des coupons numériques (jetons) émis par les entreprises sur une chaîne de blocs pour financer leur développement en contrepartie de paiement en *Ether* (le plus souvent) ou en produits de l'entreprise. Ces jetons représentent ainsi des monnaies privées, que l'on peut rapprocher par exemple de celles qui sont associées depuis longtemps aux cartes de fidélité qui permettent d'obtenir des bons d'achat dans le secteur de la distribution. Ils posent de nouveaux défis aux autorités des marchés financiers, car aucune des dispositions réglementaires habituelles pour l'émission, d'action ou d'obligations ne valent pour les ICO. Ils peuvent également être à l'origine d'un nouveau modèle de gouvernance des entreprises dans lesquels fondateurs, salariés, clients et fournisseurs détiennent tous des jetons et ont, par conséquent, un intérêt commun à développer le réseau et faire grimper la valeur du jeton. Ces changements ont poussé certains pays, comme la Chine, à interdire les ICO. Ces développements occasionnent des changements réglementaires : en France, par exemple, la réglementation monétaire et financière a introduit une nouvelle catégorie d'établissements financiers dans l'article L522-1 du code monétaire et financier : les établissements de paiement. Ce sont des « personnes morales autres que les établissements de crédit (…), qui fournissent à titre de profession habituelle des services de paiement ». Sur la base de l'autorisation de l'autorité de contrôle prudentiel et de résolution (ACPR) de la banque de France, ils peuvent offrir leurs services à l'échelle de l'Europe. A titre prospectif, on pourrait imaginer que le régulateur impose aux institutions financières un registre

[3] En supposant qu'aucun nœud du réseau ne dispose de plus de 50% des capacités totales de calcul de l'ensemble des mineurs.

[4] On devrait en réalité plutôt parler de « contrat automatique », mais nous emploierons ici la terminologie en vigueur, même si elle est assez impropre.

distribué de contrats intelligents, qui automatiserait les recapitalisations lorsque certaines règles prudentielles ne sont plus respectées (niveau en capital par exemple). Dans cette hypothèse la technologie servirait à diminuer le risque systémique bancaire.

Dans le secteur public, plusieurs pays commencent à lancer des projets : par exemple, le Ghana se propose de gérer son cadastre à l'aide d'une TRD ; l'Estonie développe un service public notarial. Plus généralement, les problématiques de gestion des données personnelles rendent l'usage de ces technologies particulièrement prometteur. Par exemple, l'association humanitaire Bitnation Refugee Emergency Response les utilise pour accompagner les réfugiés en les dotant de documents d'identité numérique. Dans le domaine de la santé, des applications d'archivage de dossier médicaux et de lutte contre la contrefaçon des médicaments sont testées. Enfin, en matière d'éducation, l'école d'ingénieurs Léonard de Vinci met en œuvre depuis 2016 un dispositif de certification de ses diplômes fondé sur une TRD.

Dans l'industrie, les premières applications des technologies de registres distribués portent sur la traçabilité des produits. Ainsi, Walmart a développé une application pour ses approvisionnements de produits alimentaires en Chine et aux États-Unis : chaque étape de la vie du produit (temps lors de la récolte, méthode d'abattage de l'animal, durée du transport…) correspond à un enregistrement ajouté au registre distribué. De la même manière, Everledger certifie grâce à une chaîne de blocs le parcours de diamants, depuis leur extraction jusqu'à leur usage, en enregistrant leur couleur, leur carat, leur type de certificat. En septembre 2017, 1,6 millions de diamants avaient été enregistrés. Dans le secteur du transport maritime de fret, Maersk a annoncé la mise en œuvre d'une coentreprise avec IBM en mars 2017 pour gérer les mouvements de marchandises et de douane entre différentes zones. A l'heure actuelle, les coûts administratifs représentent en effet environ 20% du coût global du transport de marchandise, et l'enjeu principal est une réduction drastique de ce montant, tout en conservant une sécurisation du transport. Le registre distribué utilisé intègre tous les acteurs du transport maritime (affréteurs, transitaires, transporteurs, autorités portuaires, douanes…), qui peuvent accéder à l'information dont ils besoin ; la sécurisation du processus repose sur le fait qu'aucun acteur ne peut supprimer ou ajouter un enregistrement sans validation du consensus. Un prototype est expérimenté sur la supply chain des conteneurs de fleurs entre Mombasa et Rotterdam.

Enfin, en matière de propriété intellectuelle, deux exemples sont particulièrement éclairants. Le premier d'entre eux touche à une offre de musique fondée sur un registre distribué et des contrats intelligents permettant des séquences automatiques de paiements, dont la principale inspiratrice est l'artiste Imogen Heap (Heap, 2017). L'idée de ce dispositif est de transformer la répartition de la valeur créée entre les différents acteurs (plates-formes de streaming, producteurs, artistes…) au profit des artistes. En effet la complexité des mises sur le marché des morceaux musicaux et des droits associés rend opaques et tardives les rémunérations. Ainsi, les droits diffèrent selon que le fichier musical est utilisé en streaming payant, gratuit, par abonnement, dans des vidéos, dans des films, des reportages, à la radio ou dans des publicités. Dans le système mis en place par Imogen Heap, des contrats intelligents attachés à un morceau (en l'occurrence pour l'instant la chanson « Tiny human ») permettent de déclencher un paiement automatique (et variable suivant le support) lors de chaque diffusion de ce morceau.
De manière similaire, Kodak propose de préserver les droits des photographes et d'assurer la traçabilité totale des photos en utilisant le principe des contrats intelligents et d'un paiement en crypto-monnaie. Un jeton spécifique, le Kodakcoin, serait associé à ce projet, afin que les photographes puissent automatiquement percevoir une rémunération lors d'une utilisation de leurs clichés.

Ces applications permettent de mettre en évidence trois propriétés fondamentales des TRD :

- Elles répondent de manière sûre aux menaces de cybercriminalité : vol de données, intrusion, etc…
- Elles permettent la transparence, le suivi du déroulé d'une chaîne logistique et donc d'une chaîne de valeur avec une traçabilité irréversible.
- Elles offrent des garanties de confiance décentralisée qui éteignent la nécessité d'une autorité transcendante de contrôle ou de validation des transactions.

Des polémiques ?

L'émergence multiforme de cette grappe technologique a toutefois été mise en cause par de nombreuses polémiques qui empêchent de prendre le recul nécessaire à une appréciation des risques raisonnables. Les débats peuvent être regroupés dans 3 catégories :

- Les dévoiements de l'usage des TRD
- Les limites techniques des TRD
- Les enjeux politiques associés aux TRD

Avant de préciser ce qu'elles recouvrent, notons que ces polémiques proviennent largement de deux causes : d'une part, du concept de décentralisation, interprété comme une absence totale d'autorité, de contrôle, voire de propriétaire vers lequel se tourner dans l'hypothèse d'un dysfonctionnement ; d'autre part d'une confusion entre registres publics et registres privés. Il existe en effet tout un spectre de modèles possibles avec différents degrés de centralisation et différentes catégories de contrôle d'accès, qui répondent à des besoins économiques différents comme les exemples, ci-dessus, l'ont illustré. Le *bitcoin,* par exemple, est, en effet, un registre distribué public, ouvert à chacun dès lors qu'il adopte le dispositif et personne n'en est propriétaire. A l'inverse, les registres à autorisation d'accès peuvent avoir un ou plusieurs propriétaires qui sont les seuls à pouvoir ajouter des données et vérifier le registre. Des innovations technologiques se proposent, en outre, de combiner chaînes privées et chaînes publiques de blocs pour profiter à la fois de la puissance de certification d'une chaîne de blocs publique (en raison du grand nombre d'utilisateurs) et de la faible puissance de calcul à mobiliser pour une transaction sur une chaîne de blocs privés. C'est le cas de Bitcoin Lightning network, par exemple, qui a levé des fonds à hauteur de 55 millions de dollars en février 2016 pour explorer ces pistes de développement. Cette confusion autour du concept de décentralisation et l'absence de prise en compte de la différence entre registres distribués publics et registres distribués privés permet d'expliquer nombre de ces polémiques, certains n'hésitant pas à ignorer le potentiel de ces technologies pour les entreprises au motif qu'elles suscitent des débats ou que leur usage est dévoyé dans certaines de leurs applications.

La première de ces polémiques est justement associée à un détournement de l'usage des TRD à des fins criminelles. Le *bitcoin* a été vivement critiqué en raison du fait qu'il était utilisé comme monnaie sur le « dark web ». Des plateformes d'échange comme « Silk Road » ou « Sheep momentum », qui utilisaient le *bitcoin*, facilitaient ainsi des activités criminelles comme la vente d'armes, de drogues ou le blanchiment d'argent[5]. Cette situation particulière est liée à l'usage de pseudonymes et de dispositifs cryptographiques sur certaines plateformes, qui permettent une anonymisation des participants aux transactions qui s'y déroulent (même si les autorités de lutte contre la cybercriminalité ont développé des méthodes permettant de contourner cet anonymat). Toutefois, si certains peuvent faire usage de la TRD à des fins criminelles, il en est de même pour, plus généralement, les dispositifs cryptographiques non nécessairement associés aux TRD. Il convient ainsi de distinguer d'une part, la confiance que l'on peut avoir dans la sécurisation d'un système d'échanges, de, d'autre part, la confiance que l'on peut avoir dans la nature des transactions qui s'y déroulent et la possibilité d'en tracer les participants. De ce point de vue et par analogie, il ne viendrait à personne l'idée de bannir l'usage de l'argent liquide au motif qu'il rend, cette fois-ci réellement,

[5] Ces deux plateformes ont été fermées par les autorités publiques.

impossible la traçabilité d'une transaction, et permet ainsi des activités criminelles ! La question qui se pose alors est celle de savoir si les bénéfices associés aux propriétés des TRD que nous avons évoquées plus haut, et en particulier les bénéfices pour l'activité économique et le fonctionnement des entreprises, sont inférieurs aux coûts de potentielles déviances dans leur usage.

Les TRD font également l'objet de débats sur un plan technique : en particulier, la question du « passage à l'échelle » a été largement débattue, notamment autour du *bitcoin*. Afin d'éviter des attaques de type *denial-of-service*, la taille d'un bloc de la chaîne associée au *bitcoin*[6] a été fixée à 1 Mo. Il s'est agi en quelque sorte de fixer une limite au nombre maximum de transactions qui pouvaient être réalisées avant que soit nécessaire une validation soumise à la résolution d'un problème cryptographique. En effet, une taille de bloc plus importante augmente d'autant la probabilité que des transactions se déroulent sans avoir été validées, ou qu'un blocage des validations puisse être tenté par un attaquant malveillant. Ceci aboutit *in fine* à ce que la capacité maximale de la chaîne de blocs *bitcoin* soit comprise entre 3,3 et 7 transactions par seconde et le plus souvent entre 3 et 5 transactions par seconde. Par comparaison, le réseau des cartes Visa peut en moyenne traiter 2 000 transactions par seconde et connaître des pics à 56 000 transactions par seconde. De fait, il existe donc un facteur limitant à l'usage du *bitcoin* comme monnaie alternative.
Toutefois, des techniques (comme par exemple SegWit) permettent de dépasser cette limite et il est vraisemblable que les progrès technologiques permettront de s'en affranchir entièrement à l'avenir. Par ailleurs, cette limite ne vaut pas pour toutes les chaînes de blocs, et en particulier pour les registres distribués privés, qui ne nécessitent pas une telle scalabilité.

La troisième grande polémique associée aux TRD se structure autour de questions d'ordre politique, à travers la mise en cause par le *bitcoin* de l'approche théorique de la monnaie, de la banque centrale et de l'État (Atzori, 2015). Le *bitcoin* pourrait ainsi être le premier exemple de monnaie privée, qu'appelait de ses vœux Hayek (1976), matérialisant ainsi une forme d'idéologie libertarienne, masquée par une fascination technologique ; Tirole (2017) et Krugman (2013) s'y opposent sur 3 arguments.
Tout d'abord, ils mettent en évidence le fait que la valeur actuelle du *bitcoin* repose uniquement sur la confiance et qu'elle pourrait n'être qu'une bulle spéculative. En effet, la fonction de réserve de valeur du *bitcoin*, contrairement à la monnaie « classique » (assise sur l'État et de la banque centrale, comme prêteur en dernier ressort et garant de la stabilité de la monnaie) ne repose que sur une technologie numérique, un mélange de cryptographie, l'annonce d'une limite absolue d'émission de 21 millions de *bitcoins* et un protocole de transparence irréversible partagé.
Le deuxième argument concerne la notion de bien commun. Toute émission monétaire produit une rente de situation pour l'émetteur de ladite monnaie, que l'on peut qualifier de rente seigneuriale : autrement dit, lorsque l'État émet de la monnaie, il s'octroie des ressources supplémentaires, au bénéfice de tous. Or, dans le cas du *bitcoin*, les créateurs à l'origine de la chaîne de blocs s'arrogent ce droit, et les mineurs se le disputent. Si l'on suit le raisonnement de Hayek (1976), on peut supposer que l'émergence d'une compétition libre entre les monnaies privées peut permettre comme dans tous les marchés (en théorie) de diminuer le niveau de la rente seigneuriale à zéro. Rien n'est moins sûr toutefois, les contraintes technologiques pouvant laisser penser qu'une monnaie prévale sur les autres.
Enfin, les banques centrales qui décident de la politique monétaire influencent avec cet instrument l'économie réelle : le niveau de l'investissement, la croissance, l'inflation. Dans un monde de crypto-monnaies cet instrument politique disparaît. Pour Tirole, le contrôle exercé par les tiers de confiance (l'État, les institutions financières réglementées) est un bien public ; ce bien public est privatisé dans le cas du *bitcoin*.

[6] Chaque bloc de la chaîne comprend un nombre variable (en fonction de leur importance), mais fini, de transactions.

Au total, si les polémiques que nous venons de présenter sont légitimes, il n'en reste pas moins qu'elles portent quasi-uniquement sur l'application des TRD aux crypto-monnaies, et non sur ces technologies sous-jacentes elles-mêmes. Il s'agit maintenant de voir comment elles sont susceptibles d'avoir un impact, positif ou négatif, sur les entreprises et de réfléchir à la façon d'en tirer profit dans une logique stratégique de gestion des risques et opportunités qui leur sont associées.

Le diagnostic : un cadrage stratégique

La caractérisation de la grappe technologique que nous venons de décrire présente indiscutablement des conséquences sur la probabilité de survie de très nombreuses organisations. Le temps d'un diagnostic clinique s'impose donc à toutes les organisations. Cette partie suggère plusieurs pistes méthodologiques pour penser les impacts des TRD, dans la mesure où ils ne touchent pas seulement un service ou une partie de l'organisation mais sa globalité. De plus ces impacts ne se limitent pas au court terme ou des questions tactiques. Il s'agit donc de formuler un diagnostic stratégique.

Les écoles stratégiques (Mintzberg *et al.*, 1998) sont souvent regroupées autour de deux logiques analytiques : la première part d'un décryptage de l'environnement qui détermine une logique stratégique organisationnelle de réponse (Porter, 1979) dans la tradition darwinienne de l'adaptation des organismes à leurs niches environnementales par sélection naturelle ; la seconde part des ressources et des compétences internes et produit logiquement des choix d'activité économique, un environnement construit (Wernerfelt. 1984 ; Hamel et Prahalad, 1990), en suivant l'idée de Jean-Baptiste Say que « l 'offre en quelque sorte crée sa propre demande et l'amène à son niveau ». La première logique peut être illustré par les difficultés de General Motors, incapable de s'adapter à l'évolution technologique et à la demande. On peut, *a contrario*, citer la résistance de Ferrari sur la niche des voitures de sports de luxe. La seconde pourrait s'illustrer dans ce même secteur à la fois par le succès de Toyota dans le secteur automobile ou par l'exemple d'Elon Musk avec le lancement de Tesla. Dans ces deux cas, en effet, le succès repose sur des développements technologiques et organisationnels mobilisant de nouvelles ressources et compétences.

Nous proposons de dépasser ces deux schémas trop déterministes en développant un cadrage qui accepte d'emblée l'incertitude des modèles et des hypothèses opérées dans ces raisonnements. En effet, dans le premier cas on caricature un déterminisme de l'environnement externe vers l'organisation alors qu'au contraire dans le second cas, on renverse le déterminisme de l'organisation vers son environnement.
En pratique, l'espace de l'action stratégique se situe dans l'interaction entre environnement et organisation, modelée par les stratèges. Elle constitue un espace d'appréciation subjective et de jugement sur les risques parce que l'objectif est l'augmentation de la probabilité de survie de l'organisation. En la matière, construire la pérennité ou la résilience de l'organisation n'est jamais le résultat certain d'une démonstration purement logique. Les choix, les actions, les orientations stratégiques intègrent nécessairement une dimension d'appétit pour le risque, de prise de risque sensible du côté des ressources et des compétences comme du côté de l'environnement. C'est la mise en relation entre l'environnement et l'organisation que construisent les stratèges.

Cette proposition analytique permet d'apprécier plus finement les risques et les opportunités des registres distribués dont tout un chacun convient ignorer à ce jour les conséquences ultimes, entre effondrement lors d'un krach d'une bulle technologique illusoire et nouvelle révolution industrielle d'une ampleur comparable à la révolution industrielle du XIXe siècle. Il s'agit donc à présent d'apprécier les risques et opportunités associés à la technologie des registres distribués et notamment lorsqu'elle intègre des contrats intelligents.

La méthode d'enquête suivante que l'on peut structurer à dire d'expert ou d'acteurs concernés (direction, équipe de direction, parties prenantes d'un projet…) peut permettre de procéder à ce diagnostic, pour une TRD donnée :

1. La TRD va-t-elle influencer la probabilité de la performance de l'activité de l'entreprise ? Le concept de performance pouvant prendre de très nombreuses formes selon la nature de l'activité en question ; il convient *a minima* de se concentrer sur la question de la survie.

2. Cette probabilité de performance est-elle en relation directe avec l'environnement compétitif de l'activité ? En reprenant, par exemple, le modèle de Porter cela signifie de s'interroger sur l'impact de la TRD sur :
   - les relations avec les compétiteurs,
   - les rapports de force avec les clients,
   - les rapports de force avec les fournisseurs,
   - le contexte réglementaire,
   - les substituts à la technologie utilisée par l'entreprise pour ses produits
   - l'existence de nouveaux entrants

3. Le pôle ressources et compétences est également questionné par ce cadrage. Quels sont les effets de la TRD sur les ressources et compétences sur lesquelles reposent le modèle de création de valeur ? A nouveau si l'on fait référence à Porter, cela signifie de s'interroger sur l'impact de la TRD en matière de :
   - ressources et compétences primaires (logistique externe, interne, les opérations industrielles, la mise sur marché (marketing) et les services associés)
   - ressources et compétences de soutien (organisation, talents, technologies, approvisionnement)

4. Enfin le point déterminant reste bien sûr la manière dont s'articulent les relations entre les ressources et compétences d'une part et l'environnement compétitif d'autre part, qui forment un système complexe d'interactions modelé en partie au moins par le top management. En s'inspirant de D'Aveni (1994), on aboutit ainsi aux questionnements suivants : quelles sont les conséquences de la TRD sur les quatre arènes suivantes de la compétition ?
   - l'évolution du rapport qualité / prix des produits et/ou services.
   - le rythme de l'évolution des « savoir-faire » clé sur lesquels reposent la compétitivité.
   - les places-fortes à défendre ou attaquer
   - la profondeur des capacités financières disponibles

Répondre à ces quatre questionnements, au niveau stratégique pertinent permet d'identifier le risque des TRD, de l'apprécier et de fixer une politique à son égard. C'est ce que nous allons maintenant présenter.

Que faire ? une analyse des enjeux

Au-delà des singularités du diagnostic propres à chaque organisation, nous proposons de réfléchir aux risques et aux enjeux, multi-scalaires et systémiques, des TRD à quatre niveaux en interaction : la société, l'industrie, les organisations, et les acteurs.

Au niveau sociétal tout d'abord, on peut considérer (Caseau et Soudoplatoff, 2016), qu'il est possible de comparer les effets des TRD à ceux de l'Internet : l'Internet a permis et permet de communiquer de l'information de pair à pair entre tous et partout à coût très faible. Au-delà de cet échange d'informations, les TRD pourraient permettre, à de nombreuses conditions technologiques toutefois aujourd'hui encore non résolues, d'échanger des actifs de pair à pair entre tous et partout à coût très faible, garantis par la confiance intrinsèque associée à une infrastructure distribuée. À terme les objets numériques pourraient d'ailleurs s'insérer dans les échanges. Ceci pourrait se traduire par la disparition des tiers de confiance que nous avons déjà évoquée, mais aussi celle des plateformes de type « Uber » ou « AirBnB », grâce à la relation directe entre fournisseurs de prestations et clients, par le truchement d'une TRD.
On observe d'ailleurs la même effervescence et la même énergie entrepreneuriale dans le secteur des TRD qu'au moment de la diffusion d'Internet dans le grand public, à la fin des années 1990. Des sociétés se créent et disparaissent des nouveaux services émergent et disparaissent sans que l'on puisse précisément connaître leur pérennité.

À l'échelle d'une industrie, la question des interactions peut être abordée sous son angle le plus large, celui des coûts de transaction (Coase, 1937, Williamson, 1975).
Comme Williamson l'a montré, l'intégration des coûts de transaction dans la fonction de coût total change l'appréhension que l'on peut avoir dans la comparaison institutionnelle de deux systèmes d'échange. Les questions stratégiques cruciales sont modifiées : faire ou faire faire ? comment fixer les frontières de la firme, son cœur d'activité ? quel système d'incitation peut-il être associé à une stratégie d'intégration verticale ?
Williamson distingue les coûts de transaction *ex ante* des coûts de transaction *ex post*. *Ex ante*, ces coûts sont ceux associés à la rédaction, à la négociation et à la garantie d'un accord contractuel. Il s'agit *a priori* de préciser dans le contrat qui régule l'échange toutes les réactions à des contingences. *Ex post*, ces coûts vont correspondre essentiellement à la réalisation de contingences non prévues :

- Coûts de mauvaises adaptations liées aux désajustements des transactions. Par exemple, malgré des besoins de distribution d'un produit plus complexe (nouveaux services associés), le réseau de distribution ne fait pas évoluer ses comportements.
- Coûts de marchandages *ex post* liés à des désaccords et des tentatives bilatérales de les dépasser (pour améliorer la performance d'un réseau de distribution, requalification du travail et des incitations contractuelles)
- Coûts d'organisation et de fonctionnement des structures de gouvernance qui permettent de résoudre les conflits (tribunaux ou médiation),
- Coûts d'établissement d'engagements sûrs : Les deux parties investissent dans leur réputation par la diffusion d'information sur des pratiques qui garantissent le respect mutuel des accords passés. (comme par exemple dans le dialogue syndicat/direction)

Ces coûts sont interdépendants, mais d'autres éléments pertinents complètent également l'analyse : par exemple, les coûts de transaction ne peuvent être traités indépendamment des coûts de production, car il existe souvent des arbitrages entre ces deux catégories. La conception, la nature du bien ou service échangé, comme les conditions de formation de la demande et de l'offre jouent dans ce calcul comparatif, qui permet de déterminer s'il est préférable de coordonner les individus par des mécanismes de marché ou par des systèmes hiérarchiques, suivant le montant des coûts de transaction (dans le cas du marché) au regard des coûts administratifs (dans le cas d'une coordination hiérarchique).
Les TRD changent tous ces coûts et donc tous les arbitrages délibérés ou non entre les institutions organisées d'échange. L'enjeu n'est rien moins que la place du marché de concurrence pure et parfaite tel qu'il est défini par la théorie économique, la place et la théorie de la firme et du salariat, et l'émergence de nouvelles formes de réseaux entre le marché et la hiérarchie. Les exemples d'innovations fondées sur les TRD concernant la chaîne de valeur, les droits de propriétés ou la logistique illustrent bien les risques et les opportunités à saisir.

À l'échelle de l'entreprise, nous pouvons à nouveau partir des travaux de D'Aveni (1994). En effet, la notion d'hypercompétition qu'il développe, met en évidence le caractère interactif des dynamiques stratégiques. Un mouvement d'une entreprise, sur l'une des arènes de la compétition ne reste jamais sans réactions des concurrents, des nouveaux entrants, et des autres acteurs qui influent sur l'industrie.
Il n'existe donc pas, à cet égard, d'avantage compétitif durable. Chacun des acteurs est ainsi conduit à prendre des risques à anticiper, surprendre… pour obtenir un avantage temporaire dans ses affaires. D'Aveni recommande ainsi sept tactiques de ruptures fondamentales qui constituent autant de mouvements stratégiques potentiels devant l'émergence des TRD. Nous les reprenons ici en les illustrant par les exemples exposés plus hauts :

- La première option stratégique consiste à innover radicalement en jouant sur la satisfaction des besoins des parties prenantes. Imogen Heap, propose ainsi de changer la répartition de la chaîne de valeur au profit des créateurs.
- La mieux-disance stratégique consiste à transformer la nature de la compétition sur une des arènes. Maersk, en associant à son registre distribué toutes les parties concernées, diminue les coûts administratifs du transport de fret maritime dans l'intérêt de toutes les parties prenantes.
- Proposer un changement des règles de la compétition. Dans le secteur bancaire des transferts de fonds à l'étranger, qui constitue un secteur vital pour de très nombreux pays, la concurrence que Western Union subit par des acteurs s'appuyant sur les TRD est d'ores et déjà une réalité. Les coûts de transactions sont radicalement diminués tout comme les délais de transaction.
- La vitesse et la surprise constituent également des options tactiques extrêmement intéressantes aux yeux de D'Aveni. C'est le cas des ICO (financement innovant) et de nombreuses offres alternatives du secteur des « Fintech » (Islem Ben Taher, 2017).
- Lancer une initiative stratégique est également une option stratégique à mettre en valeur. Les exemples cités peuvent tous s'inscrire dans cette catégorie.
- Enfin les annonces des acteurs du secteurs transforment également la situation de la compétition. Annoncer sa volonté de vendre un actif, ou de se développer dans tel ou tel secteur transforme les positionnements stratégiques. De telles annonces sont quasi-quotidiennes dans le secteur des assurances et de la banque en matière de TRD.

Enfin, si l'on descend à l'échelle du métier, on peut distinguer deux grandes orientations. La première est la disparition de certains métiers. Comme l'ont illustré les exemples que nous avons cités et la promesse de réduction des coûts de transaction grâce aux TRD, les métiers associés au support administratif, aux enregistrements aujourd'hui centralisés (notariat…), à certaines fonctions dans la banque ou les assurances ne peuvent être qu'amenés à disparaître (Collomb et Sok, 2017 ; Dehouck et Thomas, 2017). Ils seront remplacés par des enregistrements numériques et des contrats intelligents, tout comme par le passé, les machines à calculer ont remplacé les calculateurs humains. La deuxième orientation correspond à une modification en profondeur d'autres métiers : par exemple, en matière de maîtrise des risques, la gestion du REX post-accidents pourrait bénéficier de l'usage des TRD : la comptabilisation d'événements de manière distribuée et l'impossibilité de falsifier les enregistrements permettrait d'assurer leur fiabilité. Cela permettrait ainsi de se focaliser sur l'exploitation de ces événements, en changeant, par la décentralisation de la collecte des informations, la manière également dont cette exploitation peut être réalisée.

Conclusion : des questions qui restent en suspens

L'objet de cet article était d'exposer en quoi les TRD sont susceptibles de changer la manière dont les entreprises fonctionnent et, en les utilisant comme prétexte, de proposer un cadrage de gestion stratégique des risques et opportunités associés. Il va de soi qu'il ne prétendait en aucune manière épuiser le débat autour des TRD, qui reste mouvant et en perpétuelle évolution. Au moins quatre questions structurantes restent à résoudre.
Tout d'abord, nous avons exposé en quoi la nature même des TRD et les dispositifs cryptographiques associés permettent d'assurer une diminution des risques de cyber-sécurité classiques. Toutefois, les évolutions technologiques actuelles ou à venir, et notamment les ordinateurs quantiques, pourraient rendre obsolète le fondement même du fonctionnement des TRD, à savoir la résolution de problèmes cryptographiques. Ces développements sont toutefois encore incertains et, à l'heure actuelle, la cyber-sécurité reste plutôt une préoccupation aux interfaces des TRD : si la nature même du fonctionnement des TRD les rend robustes, la manière dont vont être sécurisées les données qui nourrissent le registre (par exemple les éléments qui permettent le déclenchement d'un contrat intelligent) reste un enjeu important.
La deuxième question, qui reste à résoudre, est celle de l'interfaçage avec le monde physique des TRD. Ce problème apparaît de manière immédiate pour les crypto-monnaies, lorsque se pose la question de la conversion en monnaie physique. Dans un autre registre, cette question du lien avec le monde physique peut se retrouver par exemple dans la problématique de la maîtrise des risques : nous avons ainsi évoqué l'usage des TRD dans ce domaine pour la gestion du REX ; la problématique, en aval, de l'implémentation des mesures qui découleraient de ce REX ne peut être résolue par les TRD. En d'autres termes, la question se pose de savoir jusqu'où des technologies informationnelles peuvent améliorer la gestion des risques (technologiques, naturels, etc…) du monde réel.
La troisième question qui reste à explorer par rapport à la problématique de la gouvernance est celle de l'initiative de la création de registres distribués. En effet, on peut s'interroger sur les effets d'un registre distribué dans une industrie, suivant qu'il a été créé par un acteur de l'industrie ou un nouveau venu.
Enfin, la temporalité de cette innovation et de son adoption par l'industrie reste un enjeu majeur. En effet, les TRD constituent sans doute un des rares domaines où les avancées technologiques précèdent leur demande. Il y a donc autant d'usages à inventer, tirés par le progrès technologique.

Références

Atzori, M. (2015), Blockchain technology and decentralized governance: Is the state still necessary?, Journal of Governance and Regulation, vol. 6, n°1, pp. 45-62.
Ben Taher, I. (2017), Stratégie et technologie : quel est l'impact de la blockchain sur la stratégie des compagnies d'assurance grand public dans le marché français ?, Mémoire de recherche Arts et Métiers ParisTech.
Caseau Y., Soudoplatoff S. (2016), La blockchain ou la confiance distribuée, Fondation pour l'innovation politique, disponible à http://www.fondapol.org/wp-content/uploads/2016/06/083-SOUDOPLATOF-2016-05-26-webDEF.pdf
Coase, R.H. (1937, The Nature of the Firm, Economica, Vol. 4, n°16, pp. 386-405.
Collomb A., Sok, K. (2017), Blockchain une révolution monétaire et financière, L'économie politique, n°75, pp. 70-82.
D'Aveni R. (1994), Hyper-competition: managing the dynamics of strategic maneuvering, New York, Free Press.
Dehouck L., Thomas A. (2017), Les risques de la blockchain, Économie et Management, n°164, pp 42-48.
Hamel G., Prahalad C.K. (1990), The core competence of the corporation, Harvard Business Review, May June, pp 3-15.

Hayek F. (1976), Denationalisation of money, Londres, The institute of economic affairs.
Imogen Heap (2017), Blockchain Could Help Musicians Make Money Again, Harvard Business Review, disponible à https://hbr.org/2017/06/blockchain-could-help-musicians-make-money-again
Krugman P. (2013), Bitcoin is evil, The New York Times, 28/12/2013, disponible à https://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/
Mintzberg H., Ahlstrand B., Lampel J. (1998), Strategy safari: a guided tour through the wilds of strategic management, New York, Free Press.
Nakamoto S. (2008), Bitcoin : a peer-to-peer electronic cash system, disponible à https://bitcoin.org/bitcoin.pdf.
Porter M. (1979), How competitive forces shape strategy, Harvard Business Review, Mars-Avril, pp. 137-145.
Sombart W. (1902), Der moderne Kapitalismus, München, Aufl. Duncker & Humblot.
Swan, M. (2016), Blockchain, Blueprint for a New Economy, Sebastopol (CA), O'Reilly.
Tapscott D., Tapscott A. (2016), Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world, New York, Penguin.
Tirole J. (2017), Les nombreuses raisons de se méfier du bitcoin, Le nouvel Économiste, 5/12/2017, disponible à https://www.lenouveleconomiste.fr/financial-times/un-nobel-contre-le-bitcoin-61918/
de Vauplane H. (2017), Les impacts des réseaux distribués et de la technologie blockchain dans les activités de marché, rapport groupe Fintech, Paris Europlace.
Walport M. (2015), Distributed Ledger Technology: beyond block chain-A report by the UK government chief scientific adviser, Royaume-Uni, Government Office for Science, disponible à https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf
Wernerfelt B. (1984), A resource-based view of the firm, Strategic Management Journal, vol. 5, n°2, pp 171-180.
Williamson, O. E. (1975), Markets and Hierarchies : Analysis and Antitrust Implications, New York, Free Press.