LES IMPACTS DES RESEAUX DISTRIBUÉS ET DE LA TECHNOLOGIE BLOCKCHAIN DANS LES ACTIVITÉS DE MARCHÉ

RAPPORT GROUPE FINTECH

PARIS EUROPLACE

*
* *

23 Octobre 2017

SYNTHESE

Le groupe de travail s'est attaché à étudier les impacts de la technologie blockchain dans deux activités financières : la gestion d'actifs et les activités de dépositaire / tenue de compte de titres. Ce choix a été dicté par l'importance des conséquences que cette nouvelle technologie pourrait avoir sur ces activités dans lesquelles la France concentre d'importants acteurs internationaux. Par ailleurs, la concomitance avec des consultations lancées par la Direction Générale du Trésor sur l'adaptation du droit français à la technologie de la blockchain en matière de droit des titres a conforté le groupe de travail dans son choix.

Si le présent rapport constitue une contribution au-delà du seul cas français et de son droit domestique, le groupe de travail a profité de la consultation lancée par la Trésor en matière de droit des titres pour y apporter sa contribution en Annexe. Il convient de noter à cet égard que la France est l'un des tous premiers pays, dans le monde, à légiférer en matière d'utilisation de la blockchain dans les activités de post marché et de droit des titres. Cette adaptation du droit français à cette nouvelle technologie s'est faite sans créer une nouvelle branche du droit, les principes généraux du droit civil et du droit commercial permettant d'appréhender la plupart des questions juridiques soulevées par la blockchain. En fait, le droit français s'est adapté à cette technologie, notamment à travers la notion de « compte de titres » qu'il a fallu redéfinir.

Plus fondamentalement, le groupe de travail est d'avis que l'objet de la régulation ne doit pas être une technologie ou une infrastructure en elle-même mais seulement ses usages.

S'agissant plus particulièrement des activités de gestion d'actifs, l'utilisation optimale de la technologie blockchain conduit à changer en profondeur la forme des actions et parts d'OPC en France pour basculer des titres au porteur au titres nominatif. Cela n'est pas sans conséquence pour les émetteurs de titres qui devront alors effectuer par eux-mêmes tout un ensemble de contrôles et se charger directement de mesures administratives et fiscales.

Quant au droit des titres, l'analyse conduit à ce qu'une adaptation du droit actuel pour les titres non cotés suffit à adapter celui-ci à l'utilisation de la technologie blockchain.

SOMMAIRE

INTRODUCTION

Les origines de la blockchain

La blockchain connaît, depuis le début des années 2010, un succès retentissant qui ne se dément pas. Ce terme est aujourd'hui sur toutes les lèvres, en particulier chez les acteurs du monde bancaire et financier dans lequel elle prend ses sources. Pléthore d'articles, de réflexions, de colloques, de débats sont organisés autour de ce thème. D'aucuns n'hésitent pas à parler de « *révolution blockchain* », au même titre que la démocratisation de l'Internet qui a changé la face du monde au début des années 1990. Cependant, au-delà de cette effervescence intellectuelle, il n'existe aujourd'hui que peu de concrétisation de la blockchain. N'est-elle qu'un phénomène de mode qui porte des espoirs qu'elle ne pourra réaliser ?

Pour comprendre cette technologie, il faut tout d'abord rappeler son origine. En effet, la blockchain n'a pas directement été conçue pour elle-même : cette technologie n'était initialement qu'un aspect du protocole Bitcoin, dont elle permettait le fonctionnement en toute sécurité. Mondialement connu, le Bitcoin est une crypto-monnaie créée au début de l'année 2009 dont la spécificité est d'être autonome et administrée par les membres de la communauté « Bitcoin ». Entièrement décentralisée, son fonctionnement est déterminé par des algorithmes mathématiques qui ont prévu *ab initio* ses modes de transfert, ses règles de consensus, ou encore le moment de ses émissions monétaires.

Tout transfert de Bitcoin doit ainsi obéir aux règles de consensus qui auront été fixées. Ce consensus ne peut être atteint que si les membres de la communauté valident le transfert, au vu d'un registre décentralisé de détention de Bitcoin, distribué auprès de chacun d'entre eux. De là est née la mécanique de ce qui est aujourd'hui appelé *blockchain*.

Il est important de préciser d'emblée que l'essence "libertaire" du Bitcoin a été largement au fondement de la création de la blockchain. C'est en effet grâce à elle que les utilisateurs de cette crypto-monnaie pourront effectuer leurs échanges en toute confiance, sans devoir passer par une autorité régulatrice perçue comme une menace à leur liberté.

Cette technologie sous-jacente au Bitcoin a rapidement été déclinée dans de nombreux secteurs de la vie quotidienne. La blockchain s'est rapidement révélée être un formidable outil de certification qui, reposant sur la confiance mutuelle entre les membres d'une communauté, permettrait de rendre un processus de décision optimal. Réputée infalsifiable, la blockchain promet à ses utilisateurs de s'assurer de la véracité des informations présentées. A l'heure de la multiplicité des échanges en ligne, la blockchain constituerait donc un moyen privilégié pour répondre aux problématiques de cybersécurité.

Rapport entre les Fintechs et la blockchain

Si la blockchain dispose aujourd'hui d'une notoriété importante, c'est avant tout grâce aux travaux des Fintechs, i.e. l'ensemble des entreprises appliquant diverses innovations technologiques, dont la blockchain, aux services bancaires et financiers.

Dans une consultation publique intitulée *Fintech: a more competitive and innovative european financial sector*, la Commission Européenne souligne le potentiel des Fintechs en matière d'innovation financière :

> « *While technological innovation in finance is not new, investment in technology and the pace of innovation have increased significantly in recent years. Among other things, technological innovation is driving social networks, artificial intelligence, machine learning, mobile applications, distributed ledger technology (DLT)1 , cloud computing and big data analytics. They give rise to new services and business models by established financial institutions, technology companies and new market entrants. FinTech involves the entire financial sector, including front, middle and back-office activities, as well as services for both retail and wholesale markets.* »

Dans cette consultation, la Commission Européenne met en avant l'importance dans sa démarche de la neutralité technologique (*technological neutrality*), à savoir garantir qu'une même activité sera soumise à une même régulation peu importe les modalités technologiques de délivrance du service afin de permettre l'innovation et de préserver la concurrence.

La consultation servira de base aux développements futurs de la politique de la Commission en matière d'innovations technologiques dans les services financiers.

Initiatives menées par les régulateurs et les acteurs de place

En France, plusieurs initiatives relatives à l'utilisation de la blockchain dans le milieu bancaire et financier ont vu le jour, prouvant ainsi sa capacité à se décliner sur des sujets larges et variés.

Dès juillet 2016, la Banque de France, accompagnée entre autres par la start-up Labo Blockchain et la Caisse des Dépôts et Consignations, a mené une expérimentation sur la blockchain portant sur l'un des référentiels bancaires dont elle a la gestion, le référentiel Identifiants Créanciers SEPA. Une infrastructure blockchain de test a été déployée pour les besoins de cette expérimentation et a permis d'identifier les premières difficultés techniques et opérationnelles de la technologie.

De même, un consortium de place, comprenant les sociétés Euronext, BNP Paribas Securities Services, la Caisse des Dépôts et Consignations, Euroclear, S2iEM et la Société Générale, a été réuni pour développer une infrastructure blockchain pour le post-marché des Petites et

Moyennes Entreprises (**PME**). Cette initiative pan-européenne a vocation à proposer une solution attractive pour ces entreprises en termes de couts et d'efficacité opérationnelle résultant d'une simplification des mécanismes de post-marché.
La Caisse des Dépôts et Consignations a, elle aussi, lancé sa première expérimentation concrète sur la blockchain, le LaBChain, consacrée à l'identité numérique et aux problématiques de vérification de l'identité des clients (*know your costumer* – **KYC**).

Intervention du pouvoir réglementaire français

Le pouvoir réglementaire français a fait figure de précurseur en matière d'innovation financière lorsqu'a été promulguée l'ordonnance du 28 avril 2016 relative aux bons de caisse[1] instituant un nouveau titre hybride, le *minibon*, transférable au moyen d'une inscription dans ce que le législateur a défini comme un *« dispositif d'enregistrement électronique partagé »*[2].

Cette innovation réglementaire majeure a permis à la blockchain de recevoir une première définition légale en droit français.

La loi du 9 décembre 2016 dite « Sapin II »[3] a poursuivi cette dynamique en habilitant dans son article 120 le gouvernement français à prendre toute les mesures législatives utiles pour adapter le droit applicable aux titres financiers et aux valeurs mobilières afin de permettre la représentation et la transmission au moyen de la technologie blockchain des titres financiers ni admis aux opérations d'un dépositaire central, ni livrés dans un système de règlement-livraison d'instruments financiers.

En mars 2017, la Direction Générale du Trésor français a lancé une consultation de place sur un projet d'ordonnance visant à adapter la législation française à la technologie blockchain dans le cadre de l'habilitation susmentionnée par la loi Sapin II[4].

[1] Ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse.

[2] Article L223-12 du Code monétaire et financier

[3] Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique

[4] Consultation publique sur le projet de réformes législative et réglementaire relatif à la Blockchain, DG Trésor, 24 mars 2017

OBJECTIFS DU RAPPORT

Etablir un état des lieux en matière d'activités de gestion d'actifs et post-marché / conservation d'actifs

La Place de Paris dispose d'une compétence internationalement reconnue en matière d'activités post-marché, i.e. l'ensemble des opérations sur titres postérieures à la transaction entre un acheteur et un vendeur de titres opérée de gré à gré ou sur les marchés financiers en vue de réaliser une transaction : confirmation, compensation, règlement-livraison, inscription en compte, *asset servicing*, etc. Trois des dix plus grands acteurs mondiaux dans ce domaine sont français. Or, la technologie blockchain pourrait conduire à une évolution importante de ces activités. Les acteurs français en matière de conservation d'actifs ne s'y sont pas trompés en axant une partie importante de leurs recherches et développement sur les cas d'usage de cette technologie.

A côté de ces activités post-marché, la Place de Paris constitue également un centre mondial en matière de gestion d'actifs. Près de 650 sociétés de gestion de portefeuille (SGP) exercent leur activité en France. Quatre groupes français figurent dans le top 20 au niveau mondial. Le marché français se distingue également par un tissu entrepreneurial important, plus des deux tiers des SGP, ce qui accroit sa capacité d'innovation en termes du renouvellement des offres/services et des business model. Les professionnels de la gestion gèrent, en France, 3 800 mds € dont 1 800 mds € sous forme de fonds de droit français et 2 000 mds € en gestion sous mandat et fonds de droit étranger. L'activité de gestion génère plus de 85 000 emplois, dont 26 000 propres aux sociétés de gestion. Avec 28% de parts de marché[5], La France est *leader* en Europe continentale, loin devant l'Allemagne (15%), et la tendance devrait s'accentuer si Paris bénéficie d'un transfert d'activités depuis Londres à la suite de la sortie du Royaume-Uni de l'Union Européenne. Or, les sociétés de gestion expriment depuis longtemps la nécessité de mieux connaitre leurs investisseurs finaux, mais aussi de mieux contrôler la distribution des organismes de placement collectifs (**OPC**). Là encore, la blockchain peut apporter des réponses intéressantes, comme le démontrent les récentes initiatives à Paris et sur d'autres places financières en Europe.

Enfin, la Place de Paris est l'un des centres européens les plus actifs en matière de capital investissement (*private equity*), avec 14.7 milliards d'euros levés et 12.4 milliards d'euros de fonds propres investis en 2016. La blockchain pourrait ici encore apporter des solutions en matière de tenue de compte et de transfert simplifié des titres détenus par les acteurs de cette industrie.

Pour l'ensemble de ces raisons, la place de Paris semble avoir une carte à jouer en examinant des éléments de compétitivité que la blockchain pourrait susciter, d'autant plus qu'elle dispose déjà d'un écosystème particulièrement important dans la technologie blockchain.

[5] « *Asset Management in Europe* », 9ème édition, mai 2017, EFAMA

Elargir la réflexion au-delà du post-marché sur d'autres activités financières

L'utilisation de la technologie blockchain ne saurait se réduire aux activités mentionnées ci-dessus dans le domaine financier. De nombreux autres domaines de la finance peuvent être affectés par cette technologie, que ce soit dans le monde des marchés financiers, du financement du commerce international ou de l'assurance. Un certain nombre des développements, réflexions et recommandations peuvent inspirer, voire s'appliquer à ces activités, raison pour laquelle le rapport propose de s'arrêter brièvement sur certaines d'entre elles.

Analyser le cadre juridique applicable à la blockchain

Une technologie n'a pas besoin en elle-même du droit pour innover et se développer. La matière financière est cependant strictement réglementée et encadré au niveau national, communautaire et mondial. L'application de la technologie blockchain à l'exercice d'activités régulées, qui en bouleversera nécessairement les usages et pratiques, nécessite donc d'en préciser les contours juridiques, que ce soit pour proposer des évolutions souhaitables du droit applicable ou, au contraire, pour confirmer que le droit positif ne vient pas freiner l'utilisation de cette technologie.

Proposer des mesures d'adaptation de la réglementation française

L'objectif principal du rapport est d'identifier, dans le domaine des activités post-marché, les évolutions législatives et réglementaires nécessaires afin de permettre un usage le plus large possible de cette nouvelle technologie, et dans les activités de gestion d'actifs les enjeux de cette technologie.

L'accompagnement du législateur par les acteurs financiers est en effet primordial tant la matière s'avère aussi technique que floue. Il ne cessera en effet d'être rappelé que la technologie blockchain est aujourd'hui loin d'avoir atteint son point de maturité. Il est particulièrement difficile de prévoir son évolution dans le futur, tant du point de vue technique que conceptuel. Nombreux seraient ainsi les écueils d'une législation élaborée sans idée précise des résultats recherchés. Il est par conséquent nécessaire de sensibiliser le législateur à prendre en compte l'aspect évolutif de la technologie et de ne pas contraindre l'épanouissement de cette technologie par des règles trop strictes.

La France a été le premier pays au monde à légiférer sur la blockchain pour la définir et en reconnaitre l'usage. Si l'ordonnance relative aux minibons permettant de recourir à la blockchain pour leur transfert est passée relativement inaperçue dans l'hexagone, elle a toutefois braqué les projecteurs sur la France au sein de la communauté blockchain.

Il appartient au législateur français de maintenir la dynamique qu'il a initiée et de soutenir le développement des Fintechs en France. Nourrissant l'ambition de devenir l'un des pionniers du

secteur, c'est en se donnant les moyens de concevoir une législation audacieuse et résolument tournée vers la pratique des nouvelles technologies financière que la France pourra atteindre son objectif.

*

* *

I. LES PRINCIPES DE FONCTIONNEMENT DE LA BLOCKCHAIN

Il n'est pas ici question de formuler ce que de nombreux rapports et livres ont déjà pu détailler sur le fonctionnement de la technologie blockchain. Il s'agira, d'une part, de rappeler les principes de fonctionnement essentiels de l'ensemble technologique qu'on désigne par ce terme, mais aussi et surtout, d'autre part, de s'attarder sur des aspects peu traités ou évoqués en dehors de la communauté des experts et spécialistes.

A cet égard, il convient de préciser que les blockchains peuvent être considérées comme des cas particuliers de *registres distribués*, et que pour cette raison un amalgame est souvent fait entre ce qu'on peut appeler la technologie blockchain et la technologie des registres distribués (*Distributed Ledger Technology* – ***DLT***). Dans la mesure où la notion de registre est cruciale en matière d'activités post-marché, on comprend l'intérêt des blockchains pour celles et ceux qui réfléchissent à l'architecture du système financier et aux moyens potentiels de l'améliorer.

Les registres distribués (*distributed ledgers*) permettent aux utilisateurs d'un réseau électronique d'enregistrer et de gérer les données relatives au fonctionnement du réseau. Les informations gérées par ce registre partagé peuvent varier suivant le *design* du système mais porteront typiquement sur différentes données transactionnelles : prix d'échange de titres ou d'actifs physiques, identifiants virtuels de ces derniers, etc. Ces informations sont réparties entre les utilisateurs, qui peuvent ensuite les utiliser pour régler leurs transferts sans avoir à se reposer, dans un modèle de fonctionnement distribué, sur un système central de validation de confiance.

Le fonctionnement d'un registre distribué tel qu'une *blockchain* implique les éléments suivants:

- un réseau pair-à-pair (*peer to peer*) soit public, soit totalement ou partiellement privé ;

- une base de données distribuée servant de « *grand livre* » où sont inscrites toutes les transactions et autres informations utiles pour les membres du réseau ;

- un ensemble d'outils et de méthodes cryptographiques assurant la sécurité du réseau – en particulier contre toute attaque ou tentative de corruption du registre distribué – et l'intégrité des échanges entre ses membres ;

- un algorithme de consensus réglant la mise à jour et l'évolution du registre et permettant d'automatiser par un ensemble de règles le processus de validation des transactions entre membres du réseau ; et

- Un mécanisme d'incitations inscrit dans le protocole de fonctionnement du réseau, qui nécessaire pour rémunérer les membres actifs du réseau, à savoir ceux qui se chargent

d'assurer la bonne marche et la sécurité du réseau, en particulier et surtout si ce dernier est complètement ouvert.

A. QU'EST-CE QU'UNE BLOCKCHAIN ?

Le terme *blockchain* (chaîne de blocs), très usité durant ces deux dernières années, renvoi à différents concepts plus ou moins précis suivant les usages et les interlocuteurs. *Stricto sensu*, la première blockchain fut celle du réseau Bitcoin utilisant le protocole éponyme. Il s'agit d'une base de données structurée en chaîne de blocs d'information, où les blocs sont reliés les uns aux autres par un chaînage cryptographique destiné à rendre immuable le stockage des données.

Ce registre agit comme le grand livre comptable du réseau sur lequel toutes les transactions valides seront enregistrées. Il est *distribué* en cela que tout participant actif (ou *nœud*) du réseau dispose de sa propre copie et peut le consulter et éventuellement le modifier en résolvant un problème cryptographique. Aucun organe central de contrôle n'est ainsi requis et l'ajout d'un nouveau bloc d'informations à ce registre s'effectue environ toutes les dix minutes, selon un protocole de consensus permettant à tous les membres actifs du réseau de vérifier la validité des transactions proposées.

Depuis le lancement du réseau Bitcoin en janvier 2009, de nombreuses autres initiatives de réseaux électroniques pair-à-pair ont vu le jour avec une base de données distribuée et structurée de manière similaire, i.e. en chaîne de blocs d'information. On parlera ainsi aujourd'hui de *blockchains* au pluriel[6], ce terme étant souvent utilisé comme synecdoque particularisante où un tout – l'ensemble d'un réseau et son protocole de fonctionnement – est désigné par une de ses parties – la base de données distribuée proprement dite. Si l'on peut ainsi définir de manière formelle une blockchain comme une base de données distribuée qui sert à enregistrer les transactions d'un réseau pair-à-pair[7], le terme évoquera également dans l'usage courant tout l'écosystème qu'elle porte.

Mais toutes les bases de données distribuées n'ont pas forcément une structure en chaîne de blocs, et les blockchains ne sont *stricto sensu* que des cas particuliers des registres distribués. On parlera ainsi dans le monde anglo-saxon de manière générique de *distributed ledger technology*, tandis que l'ordonnance susmentionnée relative aux minibons évoque la notion de

[6] On peut par exemple citer Nxt (https://nxtplatform.org) ou Ethereum (https://ethereum.org), ou consulter le site CoinMarketCap (https://coinmarketcap.com) qui référence une myriade d'écosystèmes alternatifs de type blockchain.

[7] Plus précisément, cette base de données est structurée en blocs d'information, avec un chaînage cryptographique d'un bloc à son suivant. Ce chaînage cryptographique est important car il permet de détecter facilement toute altération de la structure de données.

« dispositif d'enregistrement électronique partagé » qui inclus également les registres partagés n'étant pas structuré en chaîne de blocs[8].

B. MODELE CENTRALISE CONTRE MODELE DISTRIBUE

Les premières architectures informatiques et les premiers modèles de gestion d'une base de données servant un réseau étaient centralisés, les réseaux informatiques étant généralement structurés autour d'une unité centrale (*mainframe*) à laquelle étaient connectés des terminaux passifs.

Avec le développement d'Internet, l'environnement client-serveur est devenu prévalent avec une architecture de réseau décentralisée – un ou plusieurs *serveurs* répondant aux requêtes de leurs *clients* – mais un modèle centralisé de gestion des données. Si l'architecture client-serveur, surtout dans ses versions plus évoluées, a constitué un progrès dans la décentralisation par rapport à une architecture reposant sur une *mainframe*, elle n'effaçait pas pour autant l'asymétrie entre le serveur – gérant typiquement la base de données et ses droits d'accès – et ses clients.

Ont ensuite été mis en œuvre les premiers de réseau distribué, tel que les réseaux pair-à-pair, où chaque nœud du réseau peut être à la fois un client et un serveur et où il existe une symétrie potentielle entre tous les nœuds du réseau[9].

Il faut bien comprendre l'importance de la distinction entre l'architecture physique d'un réseau informatique et son modèle d'organisation ou protocole de fonctionnement – en particulier pour la gestion des données. Il est ainsi possible, même sur un réseau physiquement distribué où tous les nœuds ont potentiellement les mêmes capacités, de mettre en œuvre un service centralisé, par exemple dans le cas d'un réseau où il n'y aurait qu'un serveur désigné pour tous les clients. De plus, toutes les fonctions d'un réseau pair-à-pair ne sont pas nécessairement parfaitement décentralisé : Napster, l'un des premiers réseaux pair-à-pair, utilisait ainsi initialement un dépositaire central pour l'échange des fichiers musicaux entre ses utilisateurs et n'avait donc pas une organisation fonctionnelle totalement distribuée.

Une question centrale pour la tenue d'un registre commun à une communauté d'utilisateurs est celle des droits d'écriture et de lecture sur la base de données et, plus précisément, de savoir par qui et comment ils sont attribués et/ou gérés. Traditionnellement, la gestion d'une base de données est centralisée avec une entité responsable de la distribution des droits d'écriture et de

[8] Deux textes principaux existent à ce jour qui font explicitement référence à cette notion de « dispositif d'enregistrement électronique partagé » : l'ordonnance sur les minibons et la loi Sapin II.

[9] Nous ne rentrons pas ici dans la distinction précise entre réseau décentralisé et réseau distribué, notamment introduite par Paul Baran de la Rand Corporation dans les années 1960s, dont les idées amenèrent à la mise en place d'un des premiers réseaux distribués en 1969 financé par l'ARPANET, et qui devint Internet. On pourra par exemple consulter sur le sujet : https://www.rand.org/about/history/baran.html

lecture qui contrôlera donc les accès. Supposons que la base de données rende compte justement des différents soldes des comptes des clients d'une banque : cette dernière pourra par exemple s'assurer que chaque client aura son propre numéro de compte et qu'un même client ne pourra pas effectuer deux virements consécutifs si leur somme excède son solde disponible. Implicitement et explicitement par des documents contractuels, les clients de cette banque s'en remettront à cette dernière pour la bonne gestion de l'intégrité du système et de l'ensemble de ses opérations. La banque, en tant qu'entité centralisatrice responsable de la gestion des données bancaires du réseau financier, sera dépositaire de leurs avoirs tout autant que de leur confiance.

C. LA CONFIANCE DANS UN RESEAU DISTRIBUE

Le problème de la confiance dans la tenue d'un registre commun à tout un réseau peut donc être aisément résolu par la désignation d'une entité centralisatrice de confiance. Cette entité sera l'autorité de dernier ressort pour les membres du réseau en cas de problème. Pour reprendre un exemple bancaire, si un client prétend avoir réalisé un virement au bénéfice d'un autre client qui affirme ne pas l'avoir reçu, ils pourront tous les deux consulter leur banque à qui il reviendra de trancher. Si l'entité centralisatrice est effectivement irréprochable, les clients peuvent espérer une résolution simple de leur problème. Tout ce système s'effondrerait cependant si l'autorité centrale s'avérait corrompue ou arbitraire, par exemple en introduisant des mécanismes de censure visant certains types de client.

Dans le sillage de la crise financière de 2008 et de la crise de confiance institutionnelle qu'elle put provoquer chez certains acteurs, le paradigme de la première *blockchain* – celle du Bitcoin - est précisément d'éviter ce type de modèle de gestion centralisée et de proposer un protocole qui permette de se passer de tiers de confiance[10]. Dans l'article novateur et fondateur de Satoshi Nakamoto, créateur du Bitcoin, la volonté de désintermédiation des institutions bancaires est claire et assumée[11].

Dans un réseau ouvert et accessible à tous, les règles de fonctionnement du réseau doivent cependant venir se substituer au dépositaire de confiance. Les utilisateurs "honnêtes" n'utiliseront une telle blockchain publique que s'ils ont l'assurance que d'éventuels utilisateurs "malhonnêtes" seront dans l'incapacité de nuire à l'intégrité du réseau – par exemple en falsifiant les transactions, etc. La force du protocole Bitcoin est précisément d'avoir proposé, pour la première fois, un ensemble de règles qui permettait de substituer à la confiance d'une autorité institutionnelle celle d'un protocole. Il a fallu à cette fin résoudre simultanément des

[10] Le courant qui a porté le Bitcoin a mis en avant différents avantages estimés d'un modèle distribué par rapport à un modèle centralisé basé sur un tiers de confiance selon différentes dimensions : politique (pas d'abus de pouvoir potentiels du tiers de confiance liés à sa capacité de censurer ou d'exclure certains acteurs), économique (plus d'efficacité transactionnelle à moindres coûts), sécuritaire (beaucoup moins facile, voire impossible d' «attaquer » une base de données distribuée »), etc.

[11] *Bitcoin: A Peer-to-Peer Electronic Cash System*, Satoshi Nakamoto, 31 octobre 2008, accessible à l'adresse suivante : https://bitcoin.org/bitcoin.pdf

problèmes connus tels que le "problème des généraux byzantins" évoqué plus en détail ci-dessous ou encore celui de la "double dépense".

D. LE CONSENSUS ET SA REMUNERATION

Face à un réseau pair-à-pair distribué utilisé par des milliers – voire millions – d'utilisateurs, la question de savoir comment cette vaste communauté va pouvoir s'entendre sur la mise à jour du registre se pose naturellement. Il serait ici possible de passer d'un extrême à l'autre, à savoir du monopole d'une entité centralisatrice se prononçant unilatéralement sur la validité des transactions à une situation où toute transaction devrait être validée par tous les utilisateurs.

L'évolution dynamique du consensus du réseau, c'est-à-dire la mise à jour du registre distribué doit se faire de manière ordonnée et fiable. Tout changement d'état du registre partagé doit être consensuel (tous les acteurs honnêtes doivent être d'accord sur la validité des transactions), fiable (seules les transactions honnêtes doivent être validées) et efficace (le mode de gouvernance ne doit pas s'avérer trop coûteux au vu des objectifs fixés).

Si de multiples protocoles de consensus existent, ne seront ici mentionnés que les mécanismes de "preuve de travail" (*proof-of-work* – **PoW**) et de "preuve d'enjeu" ou "preuve de participation" (*proof-of-stake* – **PoS**).

L'approche "preuve de travail" exige d'un nœud du réseau qui voudrait mettre à jour la blockchain qu'il ait effectué un travail de résolution d'un problème cryptographique avant de pouvoir modifier la base de données en y ajoutant un bloc. En somme, ce mécanisme s'assure que quiconque voudra écrire sur la base de données devra payer un prix pour le faire. La somme de tous ces prix payés se retrouvera dans la complexité calculatoire du chaînage cryptographique des blocs d'informations, et donc *in fine* dans la sécurité du registre distribué.

L'approche "preuve d'enjeu" procède d'une autre philosophie : un membre devra, pour modifier l'état du réseau, montrer qu'il est déjà impliqué dans le système. Sans mécanisme d'ajustement et de pondération des différentes participations à un instant *t*, ce type de mécanisme risque de créer une concentration des pouvoirs en permettant à des acteurs du réseau ayant déjà de fortes participations de les renforcer dynamiquement, avec le risque de léser – voire de faire disparaître – les participations minoritaires[12].

Etablir un consensus sera d'autant plus difficile – et donc coûteux – qu'il faudra interroger et coordonner de multiples acteurs qui ne se connaissent pas et ne se font a priori pas confiance. C'est ici qu'intervient une distinction fondamentale entre blockchain publique et privée. La première doit être ouverte à tous, sans permission nécessaire de la part des autres membres du

[12] Une problématique « classique » qu'on retrouve dans les relations entre actionnariat et gouvernance d'entreprise.

réseau, et permettre à quiconque le souhaite de devenir un nœud de ce dernier. La seconde fonctionnera quant à elle comme un club où une permission sera nécessaire pour entrer. Cette distinction est essentielle et explique le schisme parfois observé entre les soutiens de chaque paradigme d'organisation. Pour les partisans des blockchains publiques, évoquer une blockchain privée est un contresens : devoir obtenir la permission pour devenir membre du réseau renvoie précisément à la censure institutionnelle que Satoshi Nakamoto voulait absolument éviter – à un modèle centralisé où le monopole serait devenu oligarchie. Pour les partisans des blockchains privées, le prix du consensus entre une multitude d'acteurs anonymes est souvent considéré comme exorbitant et inutile : ils auront souvent une logique de consortium et seront principalement intéressés par la tenue d'un registre commun à un ensemble d'acteurs, certes, mais qui se connaissent déjà plus ou moins entre eux. On comprend bien d'ailleurs pour ces derniers la tentation d'avoir à terme un protocole de consensus de preuve de participation plutôt que de preuve de travail : un club a déjà fourni un travail de sélection de ses membres et ces derniers se font *a priori* confiance entre eux – revenir à un système de gouvernance anonyme où chacun se défie de tous serait d'une certaine manière revenir en arrière.

On peut imaginer entre ces deux extrêmes – registre complètement public et ouvert à tous et registre privé accessible à quelques membres – un continuum de confiance entre les acteurs auquel correspondrait un "juste prix" pour établir le consensus et sécuriser le réseau.

E. LA CRYPTOGRAPHIE ET LA RESILIENCE DES ALGORITHMES

La sécurité des blockchains, sujet essentiel, est principalement fondée sur de la cryptographie, et cela à différents niveaux[13]. Le premier concept essentiel est celui de fonction de hachage (*hash function*). La caractéristique déterminante d'une fonction de hachage est que s'il est facile de calculer la sortie correspondante y = H(x) (l'*output*) pour une entrée x donnée (l'*input*), il est cependant quasiment impossible pour un y donné de trouver x tel que H(x) = y. Tout comme ouvrir un coffre sans en connaître le code d'accès nécessite d'essayer une à une toutes les combinaisons possibles, inverser une fonction de hachage, i.e. trouver un x produisant un y donné, forcera celui qui veut résoudre ce problème à tester aléatoirement une série d'entrées jusqu'à trouver une solution. Or, contrairement à beaucoup de codes de la vie courante ne dépassant pas quelques chiffres, les fonctions de hachage s'avèrent autrement plus complexes. Par exemple, pour la fonction SHA-256, la sortie (le y) sera une série de 256 bits, ce qui donne $2^{256} \approx 10^{77}$ combinaisons potentielles avant de tomber sur la bonne – soit presque autant que les estimations actuelles du nombre d'atomes dans l'univers visible[14]! Ce dernier aspect est essentiel : du nombre littéralement astronomique d'entrées à essayer pour trouver une

[13] La cryptographie ne constitue cependant pas la panacée. Ainsi, dans le protocole Bitcoin, le fait que le registre soit partagé, dupliqué et consultable par tous apporte un élément de fiabilité important en marge de toute sécurisation cryptographique. Le regard de tous sur l'ensemble des transactions du registre doit permettre de détecter très rapidement toute tentative d'altération de ce dernier.

[14] Estimé de l'ordre de 10^{80}.

sortie donnée découle la quasi-impossibilité d'inverser ce type de fonction avec les moyens de calcul actuels[15].

Les fonctions de hachage auront de nombreux usages comme par exemple de prouver l'intégrité d'un message. Il suffira par exemple à un utilisateur U1 d'envoyer à un utilisateur U2 un message M avec son empreinte numérique y =H(M). En faisant l'hypothèse que l'empreinte y' reçue par U2 n'a pas été altérée (i.e. y'=y), U2 pourra vérifier que le message reçu d'U1 n'a pas été corrompu en chemin en calculant son empreinte numérique et en la comparant à y. Une autre utilisation de ces fonctions de hachage dans les blockchains est précisément de pouvoir permettre de chaîner les blocs d'information les uns après les autres et de pouvoir détecter facilement toute modification de cette chaîne de blocs. Imaginons par exemple un livre où l'on inscrirait en bas de chaque page N son empreinte numérique qui serait calculée à partir du propre texte de la page N, T_N, et de l'empreinte numérique de la page précédente y_{N-1} ; pour la première page, on calculerait seulement $y_1 = H(T_1)$. Toute modification – même une simple permutation de deux caractères – d'une page intermédiaire I se répercuterait alors de proche en proche jusqu'à l'empreinte numérique inscrite en bas de la page finale qui représenterait une empreinte numérique, calculée de manière récursive, du livre. On pourrait ainsi immédiatement chercher l'altération du texte dans la première page dont l'empreinte numérique aurait été modifiée.

Un autre développement essentiel du chiffrement fut l'apparition de la cryptographie asymétrique avec les travaux de Diffie et Hellman en 1976[16] et la mise en pratique des principes évoqués par Rivest, Shamir et Adleman en 1978[17], aujourd'hui mondialement connus pour l'algorithme de chiffrement asymétrique "RSA". Cette avancée historique[18] aura permis pour la première fois à deux individus de communiquer de manière secrète sans avoir établi de secret préalable entre eux – à la différence d'anciennes techniques de chiffrement dite symétriques où l'émetteur et le récepteur devaient s'être préalablement entendus sur la manière dont les messages seraient chiffrés et donc déchiffrés[19]. Avec la cryptographie asymétrique, U1 peut envoyer à U2 un message qu'il chiffrera avec sa clé privée, et que U2 pourra déchiffrer avec la clé publique car connue de tous de U1. La puissance de cette approche est de permettre à U1 d'authentifier de manière certaine auprès de tous les membres du réseau tout message qu'elle enverrait : ainsi tout message déchiffré avec sa clé publique mais qu'elle n'aurait pas chiffré n'aurait aucun sens. Inversement, n'importe quel membre du réseau, par exemple U2, peut communiquer de manière secrète avec U1 en chiffrant le message qu'il lui envoie avec la clé

[15] Nous ne rentrons pas ici dans des considérations liées aux risques posés par l'émergence des ordinateurs quantiques (ou aux contre-mesures *quantum-proof* déjà envisagées par certains protocoles).

[16] *New Directions in Cryptography*, Whitfield Diffie et Martin E. Hellman, 6 novembre 1976

[17] *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, R.L. Rivest, A. Shamir, and L. Adleman, février 1978

[18] Le cryptologue français Jacques Stern écrit dans *La science du secret* (Odile Jacob, 1998) que cette avancée de Diffie et Hellman est tellement fondamentale pour la cryptographie que l'on peut dire qu'il y a un avant et un après.

[19] Le code, dit de César, qui consiste à transformer les caractères par un décalage connu à l'avance en est l'un des exemples les plus simples ; avec un décalage d'une lettre dans l'alphabet « *Bonjour* » devient « *Cpokpvs* ».

publique de U1. Ce dernier sera le seul à pouvoir déchiffrer un tel message puisque, pour devenir lisible, il nécessite d'être transformé avec sa clé privée que seul U1 connaît.

Ces concepts de cryptographie asymétriques ont permis la floraison des signatures électroniques. Il est essentiel de comprendre que la combinaison de signatures électroniques et de registre distribué permet à n'importe quels membres d'un réseau de se transférer la propriété de jetons digitaux ouvrant toutes sortes d'applications possibles. Ces jetons peuvent être considérés comme des unités de valeur propres au registre distribué – on parlera alors de crypto-monnaies ou de monnaies virtuelles – ou comme des identifiants virtuels d'autres actifs – titres de propriété par exemple. Cela ouvre formellement la possibilité de représenter sur un même registre des titres et des unités de compte pour les régler, c'est-à-dire d'avoir sur un même registre des comptes titres et des comptes espèces et donc de disposer d'un système de règlement-livraison intégré.

F. *CODE IS LAW*

L'idée derrière l'expression *« code is law »* du juriste américain Lawrence Lessig[20], devenue depuis fameuse, est de souligner comment, subrepticement, les différentes pratiques du cyberespace sont régies par les possibilités et les limites du code informatique, et comment ces pratiques risquaient à terme de s'affranchir, voire de supplanter, les principes juridiques et constitutionnels antérieurs. En définissant les contours de nos usages du cyberspace et d'une partie croissante de nos vies, le code informatique risque de devenir d'une certaine manière force de loi – au moins par les pratiques qu'il imposerait de manière implicite.

Replacé dans le contexte de la DLT, le principe est le même. Dans une blockchain ouverte à tous, la confiance qu'il est possible d'avoir en l'intégrité du réseau vient justement de l'attente que les règles de fonctionnement imposées par le code informatique ne pourront être transgressées. Du point de vue d'un utilisateur "honnête", peu importe de savoir si les autres participants du réseau sont honnêtes ou malhonnêtes, bien intentionnés ou à la recherche de failles à exploiter. Si l'on sait que le code ne pourra être corrompu ou détourné, la question des intentions des autres utilisateurs ne se pose plus. C'est pour cela que certains se réfèreront souvent à des blockchains comme à des *trustless systems*, c'est-à-dire à des systèmes où la question de la confiance dans les contreparties à une transaction ne se pose plus. La confiance se déplace d'un dépositaire de confiance à un protocole chargé de mettre en œuvre de manière infaillible et incontournable un système de règles et leur exécution. Cette omnipotence de principe du code n'est pas sans risques et peut sembler peu réaliste pour qui a déjà écrit des lignes de code, comme le souligne le problème de *The DAO* évoqué plus en détail ci-dessous.

[20] *Code is Law*, Lawrence Lessig, Harvard Magazine, janvier 2016, accessible à l'adresse suivante : http://harvardmagazine.com/2000/01/code-is-law-html

Le questionnement inverse est également digne d'intérêt : la loi peut-elle être codée ? Son esprit est-il réductible à un ensemble de lignes de code qui pourrait couvrir de manière exhaustive tous les scénarios et les contextes de son application ? Face à la faillibilité des anticipations humaines, la réponse semble clairement négative. S'il est parfaitement compréhensible d'espérer mettre en place un système aussi fiable que possible, il paraît également essentiel d'envisager, pour toute plateforme de traitement automatisé des transactions, des procédures de résolution – comme elles existent déjà aujourd'hui dans différents domaines du secteur financier ou des assurances.

G. LE DEBIT DU RESEAU

Le débit constitue une question importante pour tout réseau, qu'il se focalise par exemple sur les paiements ou sur les activités post-marché. Cette question, essentielle, a fortement divisé la communauté Bitcoin par le passé, à la fois sur les objectifs et sur les moyens.

Une première source de divergence concernait l'impératif et l'urgence d'augmenter le débit du réseau. Alors qu'il était pour certains essentiel pour le développement du réseau qu'il soit capable de traiter davantage de transactions – notamment pour avoir un débit comparable à celui des réseaux de cartes de crédit, d'autres avançaient que le réseau Bitcoin n'était pas fait pour tous les usages de paiement. On faisait ainsi valoir qu'il était aussi inadéquat d'inscrire directement des micro-transactions dans la blockchain du Bitcoin que de vouloir utiliser un coffre-fort hyper-sécurisé pour stocker une pièce de monnaie. Différents paradigmes d'usage où le réseau Bitcoin serait utilisé comme dépositaire d'empreintes numériques du bilan quotidien des activités de réseaux secondaires et périphériques (*sidechains*) étaient par exemple avancées. Une autre source de divergence concernait les moyens techniques nécessaires à une augmentation du débit, avec notamment un vif débat au sein de la communauté Bitcoin sur la nécessité d'augmenter la taille maximale des blocs encore aujourd'hui fixée à 1 mégaoctet (**Mo**).

Ces discussions constituent des défis de gouvernance pour la cohésion de cette communauté ouverte et peuvent donner lieu à certains schismes ou fourches (*forks*), suivant les choix des acteurs les plus actifs pour le fonctionnement opérationnel du réseau (les *mineurs*). Un consensus semble avoir été trouvé pour l'évolution du protocole *Bitcoin Core* appelé *segwit*, lequel a d'abord conduit en août dernier à l'adoption de la proposition *segregated witness*[21] et qui pourrait donner lieu courant novembre[22] au doublement de la taille d'un bloc à 2 Mo (*segwit2x*).

[21] *Segwit,* qui a fait l'objet du *bitcoin improvement proposal* (BIP141), permet, en structurant différemment les données propres aux transactions et leurs signatures électroniques, de récupérer de l'espace de stockage à nombre de transactions constant et donc de traiter plus de transactions en moyenne par bloc et d'augmenter le débit du réseau.

[22] Au bloc 494 784.

Pour les applications financières évoquées dans ce rapport, et suivant la plateforme de registre distribué envisagée, son caractère public ou privé et son protocole de validation des transactions, les questions techniques liées au débit du réseau peuvent changer de manière significative. Ainsi, sur la plateforme Corda proposée par le consortium R3, la validation de transactions se fait directement entre les contreparties via une connexion *point-to-point* sans diffusion des transactions à l'ensemble du réseau et sans mécanisme *stricto sensu* de preuve de travail ou de preuve de participation. Si Corda utilise des concepts blockchain standards comme le recours à des *oracles*, i.e. des paramètres extérieurs fournis par le cadre de la plateforme et dont les valeurs ne peuvent a priori être contestées par les participants, cette plateforme de consortium est donc très éloignée du protocole Bitcoin[23].

De manière générale, moins le protocole de validation de nouvelles transactions est contraignant en termes de calcul, plus il est facile d'augmenter la vitesse de leur traitement. Il y a un compromis à trouver entre sécurité et débit, et le caractère public ou privé du registre partagé est déterminant sur cette question, chaque approche ayant ses partisans et détracteurs.

H. LES SMART CONTRACTS

Si le réseau Bitcoin peut être utilisé pour bien d'autres applications que le simple transfert de bitcoins, son dessein initial, tel qu'indiqué clairement dans l'article de Satoshi Nakamoto[24], était de fournir un système pair-à-pair de cash électronique. Procédant souvent d'une volonté de généralisation des fonctions réalisées par une blockchain au-delà du simple paiement, différents écosystèmes sont apparus dans le sillage du Bitcoin, comme Ethereum où cette volonté de généralisation était explicite. De manière schématique, dans le cas d'Ethereum, les données du registre ne sont pas uniquement destinées à garder la trace d'un numéraire électronique mais peuvent également être utilisées pour exécuter un programme distribué sur l'ensemble du réseau (un *smart contract*) et avec lequel tous les membres de ce dernier pourront potentiellement interagir.

Le terme *smart contract* peut être mal compris s'il est, dans une interprétation littérale de l'adjectif qui le compose, défini par opposition à des contrats traditionnels supposés "idiots". L'intelligence à laquelle ce terme, mis en avant par Nick Szabo dès les années 1990, fait allusion est surtout celle de la facilité de gestion et d'exécution des termes du contrat (son *enforceability*). On s'assure dans le design d'un *smart contract* que l'exécution de ce programme, i.e. cet ensemble de lignes de code, soit la plus fluide et intelligente possible. Un bon *smart contract* peut donc être défini comme un contrat qui permet une exécution automatisée et dénuée d'ambiguïté de ses termes et qui réduit ainsi les risques de contentieux.

[23] Par exemple, Corda dispose également d'une entité charger de contrôler les accès des différents utilisateurs appelée *doorman*.

[24] *Bitcoin: A Peer-to-Peer Electronic Cash System*, Satoshi Nakamoto, 31 octobre 2008, accessible à l'adresse suivante : https://bitcoin.org/bitcoin.pdf

En distribuant des *smart contracts* sur un réseau, on cherchera à automatiser le mieux possible les différents processus de gestion des transactions, en particulier les activités de post-marché. Cela ouvre sur le plan théorique tout un ensemble de possibilités et de problématiques transverses.

I. FOCUS : LE PROBLEME DES GENERAUX BYZANTINS

Toute personne s'intéressant à la blockchain se souvient de la première fois où on lui a parlé des généraux byzantins, qui semblent rattacher la blockchain à une filiation quasi templière.

C'est l'étude fondatrice de Leslie Lamport, Robert Shostak et Marshall Pease, publiée en 1982[25], qui fait usage de cette parabole pour donner chair à son étude en recherche logique financée en partie par la NASA. Cette étude sur la fiabilité des transmissions et sa vérification au moyen de raisonnements logiques avait besoin d'un traître, et même de plusieurs traîtres. Or, quel autre environnement que Byzance pour réunir dans un même espace-temps une organisation extrême – byzantine – et les éléments de la duplicité la plus noire ? On pourrait bien sûr questionner la pertinence de ce choix de référence et les préjugés historiques et orientalistes qu'elle peut comporter – tel n'est cependant pas l'objet du présent rapport. Quoiqu'il en soit, ces généraux se battant pour attaquer ou sauver chacun la porte d'une ville (de la ville des villes ?) de manière coordonnée mais sans certitude sur le fait de savoir si les ordres qui leur sont transmis sont les bons, ont connu la postérité. Ces généraux ont en particulier permis de vulgariser durablement le mécanisme essentiel du raisonnement logique étudié par Leslie Lamport, Robert Shostak et Marshall Pease portant sur la vérification des informations transmises au sein d'une organisation donnée.

Il n'était bien évidemment pas question de blockchain à la date de publication de cet article mais de transmission d'information via des composants informatiques. Comme l'écrivent les auteurs :

> *« un système informatique fiable doit être en mesure de gérer la défaillance d'un ou plusieurs de de ses composants.*
>
> *Un composant défaillant peut produire un type d'action qui peut ne pas être identifiée- en particulier adresser une information contradictoire à plusieurs endroits du système.*
>
> *La majeure partie de notre étude est consacrée à ce problème abstrait et nous indiquerons comment des solutions peuvent être mises en place pour mettre en œuvre un système informatique fiable ».*

[25] *The Byzantine Generals Problem*, Leslie Lamport, Robert Shostak et Marshall Pease, 5 juillet 1982

La suite de l'étude passe en revue différentes hypothèses pratiques qui permettent à chaque fois de dégager une règle logique. La première règle conclut ainsi que, s'agissant de transmission orale simple, seules les situations dans lesquelles les traîtres représentent moins du tiers des généraux peuvent être identifiés. Dans le cas contraire, les ordres transmis par le ou les généraux félons se mêleront aux ordres fiables et confondront les généraux loyaux, de sorte que leurs actions seront décoordonnées.

Le reste de l'étude aborde peu à peu des situations plus complexes pour parvenir à la conclusion qu'en présence de messages écrits rendus infalsifiables, le problème logique peut être résolu par les généraux fidèles quel que soit le nombre de traîtres au sein de l'armée. Par "message infalsifiable", les auteurs n'entendent ni un message juste – puisqu'il peut avoir été adressé par un traître ou par un général fidèle qui aura été abusé par un traître, ni un message crypté.

Une des portées essentielles de cette étude est de démontrer qu'au sein d'une chaîne d'ordres, en assortissant le message d'un algorithme qui effectue des calculs annexes, par exemple dans un délai incompressible avant que le message ne soit envoyé au destinataire suivant, le destinataire saura avec certitude si ce message s'inscrit dans une chaîne de messages fidèles ou si la chaîne a été en partie interrompue ou falsifiée et pourra adapter son raisonnement et ses vérifications en conséquence.

La portée de l'analyse et sa pertinence pour les recherches qui ont suivi est aisément perceptible. La blockchain doit notamment beaucoup à cette analyse qui conjugue transmission de l'information en réseau et algorithme de vérification utilisé par les opérateurs au sein du réseau. De fait, le développement de la blockchain s'inscrit dans cette filiation. Son apparition a donné un nouvel élan aux premières études des années 1980 en décentrant la réflexion pour faire de la chaîne elle-même non plus seulement un moyen de transmission plus ou moins fiable mais un moyen d'archivage et de preuve.

Les solutions dégagées par le problème des généraux byzantins mettent également en lumière un principe qui constitue également une limite ontologique au fonctionnement de la blockchain : la chaîne doit en effet être continuellement vérifiée par les membres du réseau pour conserver sa validité. Comme le concluent d'ailleurs les auteurs, les solutions qu'ils proposent sont nécessairement coûteuses puisqu'elles *« sont consommatrices en temps et en nombre de messages »*. C'est un des défis que la blockchain doit aujourd'hui relever.

II. L'UTILISATION DE LA BLOCKCHAIN DANS LES MARCHES FINANCIERS

La DLT semble trouver dans les activités financières et particulièrement dans les marchés financiers un potentiel important. Les raisons principales tiennent à la baisse du coût de transactions attendue du fait de la diminution du nombre d'intermédiaires. Selon une étude d'Oliver Wyman citée par le professeur Michael Mainelli[26], le coût annuel mondial lié à la compensation et au processus de livraison dans les marchés financiers est estimé à plus de 40 milliards de dollars, essentiellement du fait de la nécessité de réconcilier les transactions. D'autres éléments sont cependant avancés, comme la sécurisation des transactions ou la plus grande rapidité dans le dénouement du cycle des transactions.

A. ACTIVITES DU MARCHE PRIMAIRE

Au-delà de la technologie comme mode opératoire d'un système d'échange, la blockchain a aussi trouvé à travers les crypto-monnaies une utilisation comme moyen de levée de fonds, en lieu et place tant des bourses traditionnelles que du marché du capital investissement.

Depuis déjà plusieurs mois, fleurissent aux Etats Unis ou ailleurs des offres publiques d'une nature nouvelle[27], non pas tant parce qu'elles portent sur des *start-up* mais parce qu'elles s'effectuent sous forme de crypto-monnaies, comme le Bitcoin (**BTC**) ou l'Ether (**ETH**). D'où leur nom : *Initial Coin Offering* (**ICO**), en référence aux *Initial Public Offering* (**IPO**). Ces opérations sont un mode de financement rapide – il faut de quelques jours à quelques heures pour lever les fonds – pour des entrepreneurs dans le monde de la DLT leur permettant de tester leur projet ou idées auprès de la communauté d'experts. Compte tenu du potentiel de cette technologie, ces levées attirent aussi de plus en plus des investisseurs en recherche de plus-values, sans que ceux-ci ne comprennent toujours les spécificités technologiques du projet.

Une ICO requiert un formalisme réduit : la levée s'effectue dans le cadre d'un projet sous forme d'un document (*whitepaper*) où sont présentés les fondateurs, le projet, le besoin de financement, son affectation future, le processus d'ICO et les conditions de paiement en crypto-monnaies. Les levées de fonds sont faites en ligne sur des sites spécialisés. Dans la plupart des cas, l'organisation communique autour de son projet en présentant l'équipe qui développe le

[26] *The impact and potential of blockchain on securities transaction lifecycle*, M. Mainelli et A. Milne, 9 mai 2016, accessible à l'adresse suivante : http://www.swiftinstitute.org/wp-content/uploads/2016/05/The-Impact-and-Potential-of-Blockchain-on-the-Securities-Transaction-Lifecycle_Mainelli-and-Milne-FINAL.pdf

[27] L'une des premières utilisations documentées des ICO pour un projet de crypto-monnaies était Mastercoin, qui a été complété par des forums Bitcointalk. Mastercoin est un méta-protocole sur la chaîne de bloc Bitcoin qui fournit des fonctionnalités supplémentaires que la couche Bitcoin de base ne propose pas. L'ICO a eu lieu en 2013 : Mastercoin (MSC) a levé plus de 5000 Bitcoin (BTC) au taux de 100 MSC par BTC.

token (jeton émis lors de l'ICO), son code source, les conditions d'émission, etc. Les sommes levées au titre de l'ICO le sont généralement sous forme de BTC ou d'ETH. Les "investisseurs" intéressés reçoivent alors des tokens en échange de leur paiement. Ces tokens représentent une sorte d'"intérêt économique" dans l'entreprise : ils ouvrent la possibilité, en fonction du projet, d'être affectés à différentes utilisations et permettent éventuellement aux détenteurs de recevoir les fruits de développement du projet, d'autant plus lorsque la levée sert à financer la phase de recherche et de développement et celle de test. En aucun cas ils ne donnent accès au capital de la société. Une fois la levée terminée, il est possible d'échanger les jetons reçus sur le marché secondaire sur des plateformes spécialisées.

Parmi les caractéristiques des ICO et les différences avec les levées de fonds traditionnelles, on peut noter les éléments suivants :

- Faible identification des parties : les investisseurs n'ont souvent pas besoin de s'identifier sur la plateforme. De même, l'émetteur n'effectuera pas ou peu de vérification d'identité des investisseurs ou de leurs sources de financement ;

- Le montant levé est transparent mais peut être manipulé : les paiements BTC et ETH sont enregistrés sur les chaînes de blocs publiques, ce qui permet à quiconque de voir la quantité et les montants aller vers une adresse de l'ICO. Cependant, bien que les montants investis soient transparents, il est difficile de savoir qui a envoyé les fonds. Cela signifie qu'il est presque impossible de savoir si le projet fait l'objet d'un vrai succès ou si la levée de fonds est artificielle du fait de la présence de l'émetteur lui-même dans la levée ;

- Prime aux premiers arrivants : souvent, la *crowdsale* est offerte avec des niveaux, où les premiers investisseurs se voient offrir un meilleur prix que les investisseurs ultérieurs ;

- Rétention et découverte de prix : habituellement, le projet ne propose pas à l'offre la totalité des jetons mais en retient un certain nombre, pour le management notamment – par exemple, 60% des jetons seront vendus dans l'ICO et le projet en conservera 40% ;

- Plafond et plancher : il y a parfois des montants de levée totaux minimum et maximum. Si le minimum n'est pas atteint, les investisseurs sont remboursés et le projet ne se poursuit pas. Lorsque le maximum est atteint, plus aucun jeton n'est distribué.

Les ICO empruntent à la fois à la notion de don et à celle d'investissement.

Tentative de définition du *token*

Il existe de nombreux types différents de jetons, chacun avec des caractéristiques et des utilisations variables. Certains jetons, comme BTC, fonctionnent comme une crypto-monnaie quand d'autres peuvent représenter un droit sur des biens corporels ou incorporels. Les jetons dans une blockchain peuvent également être utilisés dans de nouveaux protocoles et réseaux pour créer des applications distribuées. En règle générale, les tokens émis peuvent conférer des droits sur les profits à venir générés par la startup et/ou des droits de vote sur le projet financé. Ces jetons, parfois appelés *pièces d'application* ou *jetons de protocole*, représentent la prochaine phase d'innovation dans la DLT et le potentiel de nouveaux types de modèles décentralisés : par exemple, le *cloud computing* sans Amazon, les réseaux sociaux sans Facebook ou les marchés en ligne sans eBay.

Devant ce flou, les principaux acteurs mondiaux de crypto-monnaies se sont associés pour créer le *Blockchain Token Securities Law Framework*[28] en tant que forme d'autorégulation. Le partenariat comprend les entreprises comme Coinbase, ConsenSys, Union Square Ventures et Coin Center.

Régime des Offres publiques et des ICO

Ces nouveaux modes de financement conduisent à s'interroger sur la réglementation qui leur est applicable. Plusieurs régimes légaux sont potentiellement possibles (contrat de franchise, licence informatique), mais c'est surtout l'analogie avec le régime de l'offre de valeurs mobilières qui pose le plus de questions. Certains jetons, selon leurs caractéristiques, peuvent ainsi tomber sous le coup des lois fédérales ou d'État des Etats Unis sur les valeurs mobilières. Cela signifie, entre autres choses, qu'il serait illégal de les offrir à la vente aux résidents des États-Unis s'ils n'étaient pas soit enregistrés auprès de la *Securities and Exchange Commission* (**SEC**) conformément au Securities Act de 1933, soit valablement exemptés d'enregistrement. Tel est d'ailleurs le sens de la position exprimée récemment par la SEC, qui a publié une note insistant sur le fait que les jetons pouvaient, selon leurs caractéristiques, être considérés comme des titres financiers[29] avant de considérer que l'offre de jetons réalisée par The DAO constituait une offre au public de titres financiers au sens du Securities Act[30], notamment parce que les jetons en question donnaient accès aux profits potentiels de l'émetteur. La SEC a pu à cette occasion préciser que la qualification des jetons serait examinée au cas par cas et dépendrait de la réalité économique de la transaction et donc des caractéristiques des jetons. Bien que suivie le mois suivant par Singapour[31], cette approche n'en reste pas moins

[28] *Major Players Unite to Define Blockchain Token Securities Law,*Dom Galeon et Patrick Caughill, 7 décembre 2016, accessible à l'adresse suivante : https://futurism.com/major-players-unite-to-define-blockchain-token-securities-law

[29] *"Depending on the facts and circumstances of each individual ICO, the virtual coins or tokens that are offered or sold may be securities". Investor Bulletin: Initial Coin Offerings*, SEC, 25 juillet 2017

[30] *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, SEC, 25 juillet 2017

[31] http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx

minoritaire à ce jour et d'importantes incertitudes restent ouvertes quant au futur régime juridique des ICO et tokens.

Dans la mesure où les ICO peuvent s'apparenter à des levées de fonds, la règlementation applicable au sein de l'Union Européenne est la Directive sur l'offre au public de titres (la **Directive Prospectus**)[32]. Si les conditions énumérées par la Directive Prospectus sont remplies, l'émetteur doit alors rédiger et publier un prospectus. Parmi les éléments constitutifs du champ d'application, le plus important pour notre propos est celui relatif à la présence de *valeurs mobilières*, cette expression ayant été remplacée par celle de *titres financiers* lors de la transposition en droit français. Dans quelle mesure les jetons émis d'une chaine de blocs peuvent-ils être qualifiés comme tel ? C'est là l'essentiel de l'enjeu et du débat. Alors qu'aux Etats Unis le test *Howey*, utilisé pour déterminer si un instrument financier doit être qualifié de *securities,* se focalise notamment sur la notion de monnaie c'est celle de titre financier ou de valeurs mobilières qui est au centre des discussions dans l'Union Européenne. Dans les chaines de blocs comme celle du BTC ou de l'ETH, les jetons représentent une valeur, ce qui ne veut pas dire grand-chose. Ces jetons peuvent revêtir aussi bien les fonctions d'une valeur d'échange, d'un actif non financier, voire même d'un actif financier, selon les cas d'usage. C'est donc à une analyse au cas par cas qu'il convient de se livrer.

Si ces jetons ne rentrent pas dans la définition des titres financiers, les ICO ne sont alors pas soumises à la réglementation relative à l'offre au public de titres. Les ICO échappe-t-il pour autant à toute réglementation ? Les régulateurs ne se sont pas encore prononcés clairement, tout au moins dans l'Union Européenne, sur la question. En France, on notera les pouvoirs de l'Autorité des Marchés Financiers (**AMF**) en matière de *biens atypiques* ou *biens divers*, c'est-à-dire les investissements en rentes viagères, pierres précieuses, wagons, diamants, manuscrits, vins panneaux photovoltaïques, etc. Dès lors qu'il s'agit, par voie de communication à caractère promotionnel ou de démarchage, de souscrire à des droits sur des biens mobiliers ou immobiliers (biens divers 1) ou d'acquérir des droits sur un ou plusieurs biens en mettant en avant la possibilité d'un rendement financier direct ou indirect ou ayant un effet économique similaire (biens divers 2), l'AMF est compétente à tout le moins pour examiner la documentation proposée au public[33].

D'autres pays se sont prononcées sur la légalité des ICO ou ont alerté le public sur les risques de ces opérations :

- Le régulateur financier au Royaume-Uni (*United Kingdom Financial Conduct Authority* – **FCA**) a, dans une publication en date du 12 septembre 2017, mis en garde les investisseurs potentiels quant aux risques associés aux ICO. La publication qualifie les ICO d'investissements spéculatifs très risqués et incite les investisseurs à la plus

[32] Directive 2003/71/CE du Parlement européen et du Conseil du 4 novembre 2003. La Directive Prospectus a vocation à être remplacée par le Règlement (UE) 2017/1129 du 14 juin 2017 (le **Règlement Prospectus**) qui entrera en application le 21 juillet 2019.

[33] Article L. 550-1- du Code Monétaire et Financier

grande prudence. La FCA a également précisé que seuls certaines ICO seraient probablement susceptibles de relever de sa compétence ;

- Le régulateur financier canadien (*Canadian Securities Administrators* – **CSA**) a publié une note en date du 24 août 2017 dans laquelle il affirme que les ICO pourraient être soumises au droit des titres financiers canadien mais précise que les jetons ne constitueraient pas nécessairement des *securities* au sens du droit canadien. Le régulateur précise que les jetons pourraient également être soumis au droit des produits dérivés s'ils pouvaient être qualifiés de la sorte ;

- Le régulateur financier israélien (*Israel Securities Authority* – **ISA**) a annoncé le 30 août 2017 qu'il organiserait un comité qui se prononcera sur l'application du droit des titres financiers aux ICO ;

- Un comité de régulateurs mené par la Banque Populaire de Chine a publié une déclaration le 4 septembre 2017 interdisant toute ICO future et imposant aux émettrices de rembourser les jetons déjà émis[34] ;

- Le régulateur financier singapourien (*Monetary Authority of Singapore* – **MAS**) a publié une déclaration en date du 1er août 2017 dans laquelle il affirme que certains jetons pourront être qualifiés de *securities* au sens du *Securities and Futures Act* singapourien, auquel cas les émetteurs devraient alors déposer un prospectus auprès de la MAS préalablement à l'offre de jetons sauf en cas d'exemption applicable. De plus, les émetteurs ou intermédiaires de ces jetons qualifiés de *securities* devraient disposer des agréments nécessaires conformément au *Securities and Futures Act* ;

- Le régulateur hongkongais (*Securities and Futures Commission* – **SFC**) a, dans une declaration du 5 septembre 2017, affirmé que les jetons pourraient, selon les circonstances de chaque ICO, être qualifiés de *securities* au sens de la *Securities and Futures Ordinance*, ce qui déclencherait diverses obligations d'agrément et d'enregistrement auprès de la SFC ;

- Le régulateur sud-coréen (*Financial Services Commission* – **FSC**) a annoncé le 3 septembre 2017 la création d'un groupe de travail avec d'autres régulateurs sur les crypto-monnaies et leur cadre réglementaire. La FSC a notamment insisté sur son souhait de renforcer les exigences en termes de connaissance des clients et de lutte contre le financement du terrorisme. Le 29 septembre, elle a finalement interdit toute levée de fonds sous forme de crypto-monnaie, justifiant cette mesure par la protection des investisseurs face à l'augmentation des ICO frauduleuses ;

- Le régulateur financier suisse (Financial Market Supervisory Authority– **FINMA**) a, dans un communiqué de presse du 29 septembre 2017, annoncé enquêter sur plusieurs

[34] http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html

ICOs. La FINMA précise, dans le Guide 04/2017 publié à la même date, que les ICOs sont susceptibles, selon leur structuration, d'être gouvernées par (i) la réglementation relative à la lutte contre le blanchiment et le financement du terrorisme, (ii) la réglementation bancaire relative à la réception de dépôts du public, (iii) les règles applicables aux titres financiers et aux produits dérivés, et enfin (iv) celles applicables aux organismes placements collectifs. Comme l'indique la FINMA, *"due to the close proximity in some areas of ICOs and token-generating events with transactions in conventional financial markets, the likelihood arises that the scope of application of at least one of the financial market laws may encompass certain types of ICO model"*;

- La Banque Centrale Russe, en plus de ses alertes concernant le caractère risqué des ICO, a annoncé vouloir restreindre les ICO à des investisseurs autorisés, via la bourse de Moscou, avant la fin de l'année[35].

B. ACTIVITES DU MARCHE SECONDAIRE ET TRADING

Si la DLT est porteuses d'innovations sur le marché primaire avec l'apparition des ICO, elle pourrait également influencer en profondeur les activités du marché secondaire et de *trading*.

S'agissant de la phase négociation, l'aspect distinctif de ce processus repose principalement sur la façon de concevoir un processus efficace d'appariement des ordres et de formation de prix. Fondamentalement, la possibilité d'utiliser, avec une valeur ajoutée, la blockchain au niveau des activités de négociation dépend de deux facteurs : (i) de la nature des instruments financiers échangés et (ii) de la nature de l'activité de négociation visée.

Les modalités de formation du prix dépendent intrinsèquement de la nature de l'instrument financier. Pour certains instruments, le prix est uniquement formé par la rencontre des intérêts à l'achat et à la vente. C'est le cas typiquement des produits de type actions. La formation du prix de ces produits nécessite donc la centralisation de l'offre et de la demande à chaque instant. Cette centralisation peut être 'réelle', c'est-à-dire qu'une seule et même plateforme rassemble l'ensemble de l'offre et de la demande sur l'instrument concerné. Elle peut également être 'virtuelle', et c'est d'ailleurs la norme sur la plupart des marchés où les intérêts à la vente et à l'achat sur un même instrument sont dispersés sur de multiples plateformes opérant parallèlement. Dans ce cas la cohérence des prix est assurée par des arbitrageurs qui, avec la latence la plus faible possible, font le lien entre ces plateformes à tout instant. Ces instruments impliquent donc non seulement un certain degré de centralisation des intérêts mais également (et c'est une conséquence) des capacités d'absorption et de traitement de volumes considérables et une latence très faible.

[35] https://www.cbr.ru/press/PR/?file=04092017_183512if2017-09-04T18_31_05.htm

Sur ces instruments, la blockchain, de par son caractère par essence décentralisé et ses limites en termes de capacité de traitement, ne peut donc être utilisée pour héberger un carnet d'ordres, sans (i) mettre en danger la formation du prix et (ii) revenir plusieurs décennies en arrière en termes de capacité de traitement de volumes d'ordres et de latence, même en mettant de côté l'impossibilité par la construction même de la blockchain de contribuer à former un prix résultant de la rencontre de l'offre et de la demande.. Il est à ce titre intéressant de noter que les carnets d'ordres des bourses de cryptomonnaies sont aujourd'hui opérés en dehors de toute blockchain36.

En revanche, une fois que les ordres sont appariés en carnet, et donc que la question de la centralisation n'est plus pertinente et celle de la latence moins aigue, la transaction en résultant peut être créée sur la blockchain, en amont même de son dénouement, règlement et livraison. C'est même la condition sine qua non de l'utilisation de la blockchain pour l'optimisation des processus de post-marchés dont nous parlerons plus loin. Pour une question de performance (à savoir la combinaison de la taille et des algorithmes de chiffrement), cette possibilité semble aujourd'hui ouverte à un nombre restreint d'instruments, ceux dont la liquidité est limitée. Il est fort probable qu'elle s'étende à des instruments dont la liquidité est plus importante à mesure que les performances de la blockchain s'accroissent.

A titre d'exemple, en se concentrant sur la question de la capacité et en excluant les sujets de centralisation et de latence, Opimas37 estime que la blockchain devrait atteindre 1.5 terabytes pour héberger l'ensemble des transactions sur titres effectuées sur les carnets des plateformes européennes en 2015 (sans même prendre en compte le nombre d'ordres en amont), capacité qui devrait s'accroitre au rythme de l'augmentation des volumes des marchés concernés. Or aujourd'hui la taille de la blockchain Bitcoin est d'environ 130 000 megabytes. Cette augmentation de taille est envisageable, néanmoins elle demanderait un accroissement considérable des capacités computationnelles, de bande passante et de stockage de données au niveau des nœuds et des mineurs, impliquant donc en retour une certaine forme de concentration, seules quelques institutions ayant les moyens d'atteindre de telles capacités. Une alternative consiste à optimiser les performances de la blockchain en externalisant une partie des vérifications en dehors de la blockchain en tant que telle, pour les confier à des acteurs désignés pour les effectuer. Dans ce cas, la blockchain ne peut être que privée, contrôlée par des acteurs identifiés, ce qui aboutit là encore à un certain degré de concentration.

En revanche, l'utilisation de la blockchain au niveau des activités de négociation est envisageable même en amont de la création de la transaction pour d'autres instruments. C'est le cas typiquement des instruments dont le prix de la négociation purement bilatérale entre deux contreparties (notamment pour les produits dérivés non-standards).

[36] Bank of America Merrill Lynch, Exchange Views – How will blockchain change European market structure, 01 Feb 2016; SWIFT Institute, Working Paper n°2015-007, The impact and potential of blockchain on the securities transaction lifecycle, 09 May 2016; UBS, Global Exchange – The potential impact of blockchain / DLTs on the global equity exchanges

[37] Opimas, Blockchain for capital markets - A pipe dream, May 2016

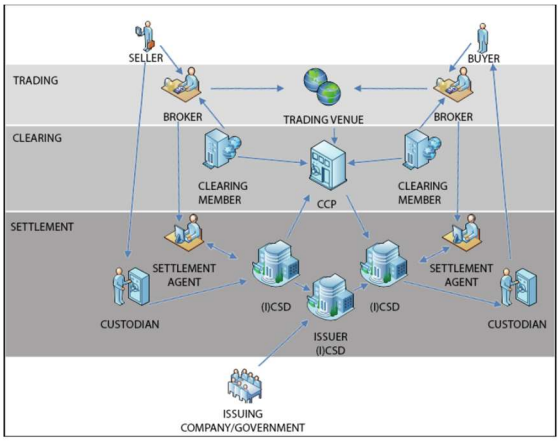
La possibilité d'utiliser la blockchain pour les activités de négociation dépend donc de multiples facteurs. Néanmoins, on peut s'attendre à ce que la mise en œuvre des apports de cette technologie sur d'autres segments de la chaîne de valeur ait un impact majeur sur les activités de négociation. Notamment, en réduisant les frictions au niveau de la post-négociation, la blockchain devrait avoir un impact tant sur la demande que sur l'offre de capitaux, en incitant un nombre croissant d'émissions de capital sur les marchés et en augmentant l'investissement et les échanges sur les instruments en circulation et donc les volumes négociés.

C. ACTIVITES DE POST-MARCHE

La DLT peut également simplifier le schéma traditionnel d'organisation et de fonctionnement des activités de post-marché.

De manière classique, le cycle d'une transaction en bourse nécessite la présence d'un intermédiaire de marché, d'une bourse et d'infrastructures et intermédiaires relevant du post-marché, à savoir d'une chambre de compensation, d'un organisme de règlement-livraison, d'un dépositaire/teneur de compte et un dépositaire central. Tous ces acteurs jouent un rôle propre et spécifique dont l'historique remonte à la création des bourses modernes au 19ème siècle. Depuis cette date, certains pans de cette chaine de valeur se sont transformés de manière radicale tant du point de vue technologique (avec le passage par exemple de la cotation à la criée en bourse à une cotation totalement électronique), que concurrentiel (aujourd'hui à un moment T il est possible de traiter la même action sur une multitudes de plateformes de négociation en Europe). On peut également noter que les agents de change ont été remplacés par les banques ou courtiers, les bourses à l'origine nationales se sont regroupées dans des ensemble régionaux, les chambres de compensation et les dépositaires centraux ont suivi la même évolution, etc. Ces derniers, dorénavant appelés *infrastructures de marchés*, sont de plus passés d'une structure actionnariale de forme coopérative à un actionnariat capitalistique – ce que l'on a appelé dans les années 1990 la *démutualisation*.

Dans ce modèle, l'instruction d'achat ou de vente d'un titre financier sur un marché boursier suit un cycle complexe, tant d'un point de vue technique que juridique, du fait de la présence de ces multiples acteurs. Il est même parfois difficile de "tracer" un ordre de son passage par l'investisseur jusqu'à la livraison ou le paiement : la présence de la chambre de compensation rend en effet impossible toute traçabilité individuelle d'une instruction du fait de la technique de compensation multilatérale.

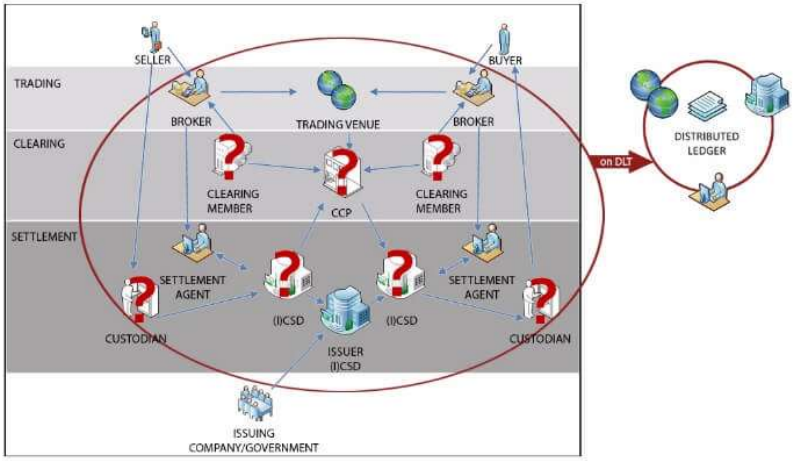


Par ailleurs, depuis de nombreuses années, les exigences de fonds propres pour les infrastructures de marché mais aussi pour les intermédiaires financiers se sont significativement accrues afin de mieux encadrer le risque de défaut d'une contrepartie sur l'ensemble du processus du cycle boursier.

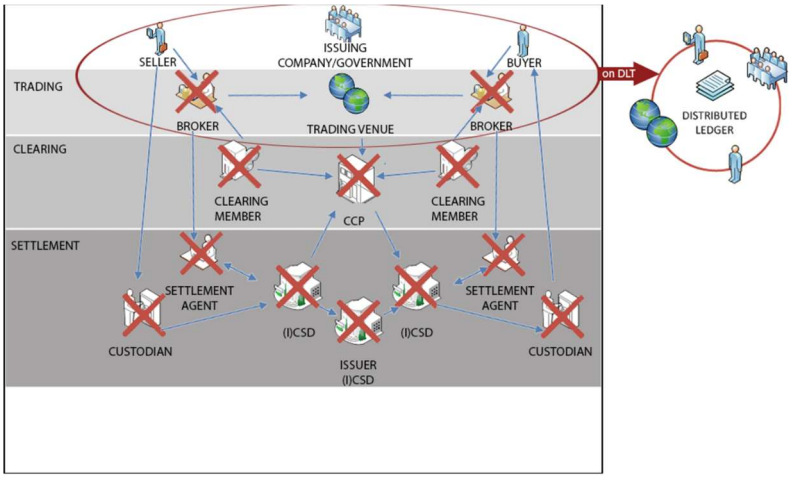
Dans les marchés financiers, la disparition progressive des titres papiers et leur remplacement par des actifs dématérialisés conduit au remplacement des livraisons physiques d'actifs contre somme d'argent fiduciaire par des jeux d'écritures numériques. Tel est aussi le cas avec la monnaie fiduciaire qui tend à être remplacée par la monnaie scripturale. Reste cependant inchangée la nécessité d'un "*golden record*" par les infrastructures de marché et les intermédiaires afin de mettre à jour leurs bases de données individuelles en communiquant avec les autres institutions impliquées aux différents niveaux de post-négociation, et ce afin de pouvoir refléter chaque transaction dans les enregistrements au niveau de chaque intermédiaire/infrastructure. Le coût très élevé de ce type de processus conduit à examiner les potentialités offertes par les registres distribués comme une alternative aux systèmes actuels centralisés.

Une architecture en format DLT pourrait en effet résoudre ces lourdeurs et surtout diminuer drastiquement les coûts pour les investisseurs, mais aussi les besoins de fonds propres pour les intermédiaires de marché. Peu d'études précises ont été réalisées sur ces économies de fonds propres, lesquelles ne seraient pas identiques selon les classes d'actifs en fonction de leur régime réglementaire. Mais, comme le souligne la BCE, *"DLTs have the potential to address many of the shortcomings identified in the post-trade market"*[38]. Comment ? En simplifiant le processus de transaction et en reconsidérant le rôle de certaines des infrastructures de marché. En effet, une DLT pourrait tout à la fois tenir le rôle d'une bourse, d'une chambre de compensation et d'un dépositaire central, voire même d'un système de règlement-livraison, l'ensemble des transactions étant alors enregistrés dans un registre décentralisé. La question du paiement dans un système de blockchain publique étant toutefois délicate compte tenu du recours à une crypto-monnaie.

[38] ECB, *Distributed Ledger Technolgies in securities post trading, revolution or evolution*, Occasional paper series, n° 172, April 2016.



Au-delà même des infrastructures de marché, ce sont les courtiers et intermédiaires eux-mêmes qui pourraient voir leur rôle profondément affecté par la DLT. En effet, rien n'empêcherait technologiquement chaque investisseur d'avoir directement accès à la DLT pour négocier son ordre, même si une telle offre n'existe pas encore sur le marché.



Tous ces éléments militent en faveur d'une réflexion intégrant à la fois la dimension opérationnelle mais aussi technique et juridique du recours à la DLT comme substitut au fonctionnement actuel des activités de post-marché.

Certaines infrastructures de marché ont initié des travaux sur les bénéfices que pourraient leur apporter cette technologie. Ainsi, selon Euroclear[39], l'application de DLT en matière de règlement-livraison des titres pourrait générer les avantages suivants :

- réduction de la latence du règlement ;

[39] Euroclear & Slaughther and May

- réduction du risque de conservation ;
- transparence accrue pour les émetteurs, les investisseurs finaux et les régulateurs ;
- réduction de l'intermédiation de la tenue des registres ; et
- augmentation de la sécurité des données.

La difficulté majeure en la matière est le peu d'expérimentation mais aussi le faible nombre d'analyses pratiques sur les impacts de la DLT dans les activités de post-marché. La plus récente et la plus complète réside sans doute dans le travail accompli par la bourse de Tokyo en 2016 qui a testé le recours au DLT pour ses activités de compensation et de livraison[40]. Dans son rapport, la Bourse japonaise reprend le cycle d'une transaction boursière et examine en quoi la DLT pourrait modifier le processus actuel.

Compensation et règlement

Contrairement au processus de négociation, il n'est pas ici nécessaire, même si cela serait souhaitable, d'agréger les ordres, de sorte que le processus décentralisé de DLT pourrait apporter des avantages comme notamment son taux de disponibilité. C'est d'ailleurs sur cet aspect de compensation que la bourse de Tokyo estime les impacts les plus importants. En effet, dans la mesure où les transactions sont inscrites les unes à la suite des autres, il n'est plus utile de recourir à un mécanisme de compensation : ce sont les mêmes transactions qui sont négociées sur le marché puis réglées et livrées. On revient ainsi à un système non pas en net, mais en brut, sans qu'il ne soit besoin de compenser. C'est ainsi l'existence même de la chambre de compensation qui est remise en cause par la DLT.

Propriété des titres financiers

L'identification des propriétaires des titres et immédiate et surtout complète. Bien sûr, il convient de s'assurer de la confidentialité de certaines informations, mais le principe d'une traçabilité de la détention de chaque titre constitue une avancée majeure.

Evènements sur les titres financiers

[40] Atsushi Santo & ali. "*Applicability of the Ditributed Ledger Technology to Capital Market Infrastructure*", Japan Exchange Group, Working Paper, 3O August 2016, vol. 15

Une liste des actionnaires à une date déterminée peut être récupérée rétroactivement, et il est dès lors possible de mettre en œuvre des évènements tels que le paiement de dividendes ou l'attribution de droits à certaines catégories d'actions en utilisant la liste des actionnaires.

Pour toutes ces raisons, l'étude effectuée par la bourse de Tokyo considère que l'application de DLT au processus post-marché pourrait rendre le travail existant plus efficace à l'avenir. Cependant, l'étude a identifié plusieurs préoccupations qui pourraient empêcher le déploiement à court et moyen terme de la DLT. Il s'agit notamment de la question de la synchronisation des horloges entre les nœuds qui peut empêcher d'effectuer les transactions en même temps. Une autre difficulté tient dans la vitesse des transactions : la capacité de débit en DLT, qui détermine si de nombreuses transactions peuvent être traitées par unité de temps, est généralement affectée par la manière dont fonctionne l'algorithme de consensus. Comme il a déjà été précisé ci-dessus, augmenter la capacité de débit nécessite d'augmenter le nombre maximum de transactions par bloc ou d'adopter un algorithme de consensus plus rapide. Le premier pourrait être atteint en augmentant la taille des blocs, mais cela entraînerait une plus grande bande passante réseau pendant le processus de consensus. Tout dépend en réalité du type de technologie utilisé par la DLT.

Même s'il est trop tôt pour tirer des conclusions définitives, il ressort de ces différentes études qu'il existe un potentiel dans la technologie du grand livre distribué. En outre, l'innovation est en général bienvenue dans le marché européen de l'après-commerce pour les valeurs mobilières, où elle peut renforcer tant la sécurité que l'efficacité. Un certain nombre de facteurs pourraient cependant poser des obstacles potentiels à l'adoption généralisée et à l'utilisation des DLT.

De nombreux chantiers restent à régler avant que la DLT ne vienne remplacer les outils informatiques existants dans les activités de post-marché. Qu'il s'agisse des questions juridiques, opérationnelles ou de gouvernance, tous ces sujets doivent être examinés sereinement. Tout ceci va prendre du temps : pour la BCE, la révolution du post-marché n'est envisageable à court terme et le processus d'utilisation de la DLT sera sans doute graduel et fonctionnera parallèlement avec les outils existants.

Dépositaire central

Le Règlement (UE) 909/2014 du Parlement et du Conseil du 23 juillet 2014 concernant l'amélioration du règlement de titres dans l'Union européenne et les dépositaires centraux de titres (**CSDR**), dispose à son article 3 que « *tout émetteur établi dans l'Union qui émet ou a émis des valeurs mobilières admises à la négociation ou négociées sur des plates-formes de négociation veille à ce que ces valeurs mobilières soient inscrites en compte en tant qu'immobilisation ou après l'émission directe sous forme dématérialisée. Lorsqu'une transaction sur valeurs mobilières a lieu sur une plate-forme de négociation, les titres concernés sont inscrits en compte auprès d'un DCT à la date de règlement convenue ou avant cette date, s'ils ne l'étaient pas déjà*. ».

Plate-forme de négociation au sens de CSDR signifie un marché réglementé, un système multilatéral de négociation ou un système organisé de négociation. Ainsi l'article 3 de CSDR impose aux émetteurs dont les titres sont côtés d'émettre ces titres auprès d'un dépositaire central de titres.

Dans la mesure où CSDR est d'application directe, l'utilisation de DLT pour les activités de post-marché et de tenue de compte sur titres cotés requiert donc pour l'opérateur de la DLT, dans l'état actuel de la réglementation, l'obtention d'une licence de *Central Securities Depository* (**CSD**).

D. ACTIVITES DE GESTION D'ACTIFS

1. Les enjeux de la blockchain pour la gestion d'actifs

La blockchain est une technologie potentiellement porteuse d'innovation pour l'industrie de la gestion d'actifs, tant en termes d'efficacité opérationnelle et de réduction des coûts que d'exploitation de l'information. Ces différents usages pourront s'apprécier aussi bien au niveau de la gestion de l'actif – soit les investissements faits par les organismes de placement collectifs (**OPC**) – que de la gestion du passif – soit les porteurs de parts des OPC. Son impact portera essentiellement d'une part sur le circuit de l'information avec les parties prenantes – dépositaires, teneurs de compte, *asset servicer*, distributeurs, fournisseurs de données, émetteurs, etc., et, d'autre part, en interne entre les différents services. De plus, combiné aux possibilités offertes par la Directive (UE) No 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (**DSP2**), les sociétés de gestion pourront développer des activités de commercialisation directe des OPC aux investisseurs.

A l'actif (liste non exhaustive) :	***Au passif (liste non exhaustive) :***

Post-trade : projet en cours sur les transactions sur les petites capitalisations françaises	Règlement-livraison d'un fonds d'investissement
Processus de vote aux assemblés	Vente directe de fonds à l'investisseur grâce à DSP2
Gestion des Opérations Sur Titres	Le cycle de vie des fonds comprenant la gestion des événements des OPC de la création à la dissolution
Gestion du collatéral	Le suivi et le paiement des rétrocessions
Registre d'actionnaires	L'information des porteurs, l'harmonisation de l'actualisation des documents (*Fact sheet*, *Key Investor Information Document*)
Reporting de transaction MIF, EMIR, SFTR	Connaissance clients : KYC
Reporting régulateur AIFM	Le marquage des ordres

De nombreux projets sont en cours avec une mise en production prévue pour fin 2017 ou début 2018. Il est donc trop tôt pour quantifier les retours sur investissement et identifier les difficultés éventuelles lors de leur déploiement à grande échelle. La "blockchainisation" dans la gestion pour compte de tiers peut s'envisager par cercles concentriques de plus en plus éloignés de la société de gestion filiale d'un groupe :

- Autoconsommation OPC « maison », amélioration du partage et de la traçabilité de l'information au sein des différents services d'une même entité : gestion des *reportings*, contrats, consolidation des outils et des données, etc. ;

- Distribution intra-groupe et diffusion de l'information (KYC) ;

- Distribution hors groupe mais dans le même pays de domiciliation ; et

- Distribution internationale.

Concrètement, et au-delà de l'aspect technologique « pur », un des usages déterminant de la blockchain pour l'industrie de la gestion d'actifs est la tenue de passif des fonds via la réduction du nombre d'intermédiaire et l'amélioration et la récupération de la connaissance client.

Après avoir introduit la chaîne de valeur des sociétés de gestion de portefeuille (**SGP**) et leur écosystème, nous concentrerons l'analyse sur l'impact de cette nouvelle technologie dans les systèmes de règlement-livraison des parts d'OPC, selon les modèles *Clearing and Settlement Depositary* (**CSD**) et *Transfert Agent* (**TA**).

2. La chaîne de valeur des sociétés de gestion de portefeuilles

Les sociétés de gestion de portefeuilles sont les institutions chargées de la gestion financière, administrative et comptable des produits gérés pour compte de tiers : OPC et mandats discrétionnaires. Agréées à cet effet par l'AMF, elles s'engagent à gérer de manière indépendante et dans l'intérêt exclusif de l'investisseur les sommes qui leur sont confiées, les actifs gérés restant déposés chez le dépositaire/teneur de comptes.

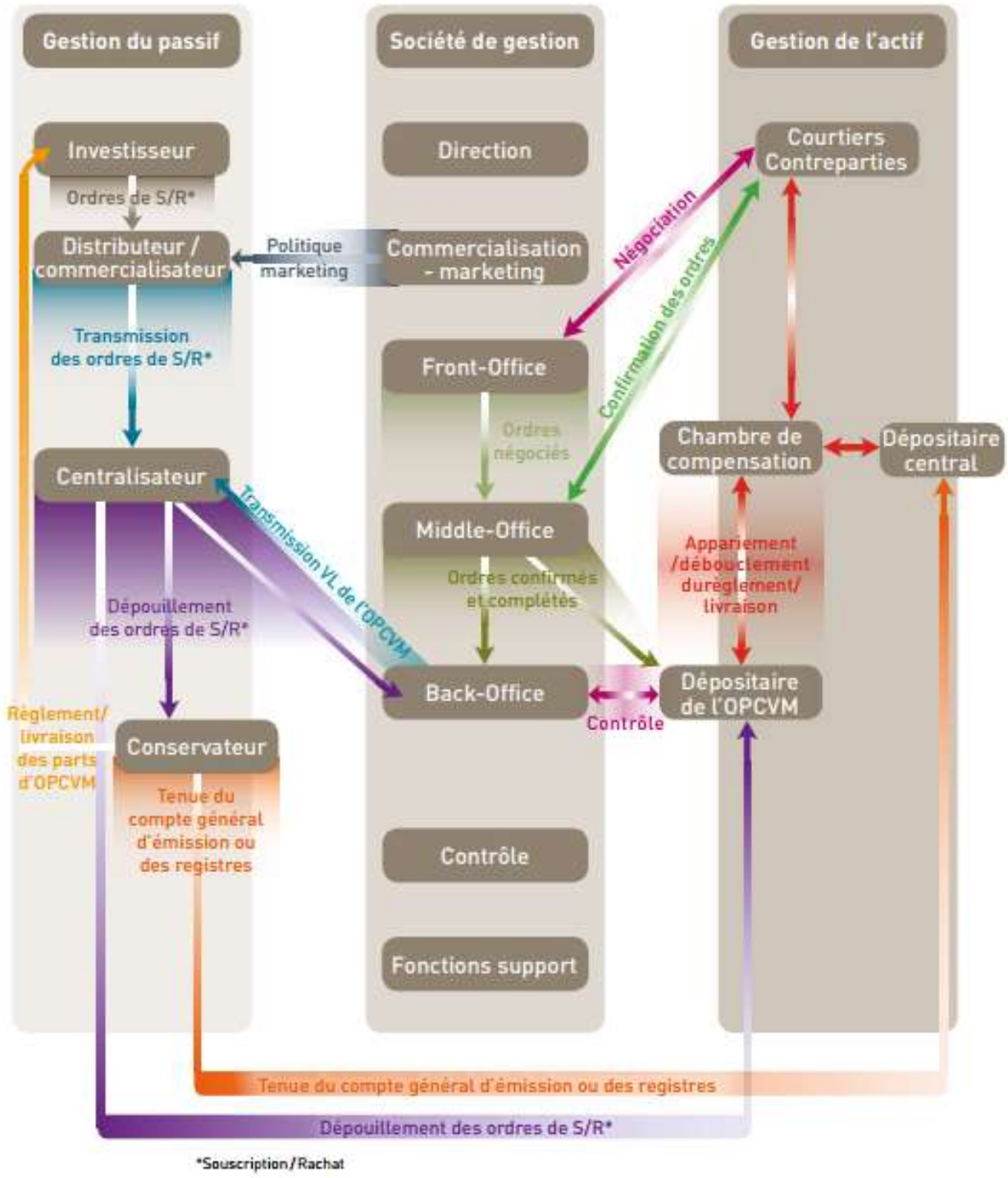
Aujourd'hui, il n'y a pas un schéma organisationnel unique de la société de gestion mais une multitude de schémas organisationnels ou de modèles de gestion, que les sociétés adaptent en fonction de différents paramètres tels que leur spécialisation, leur expertise d'investissement, leur taille, la structure de leur actionnariat, leur stratégie commerciale, leurs partenariats, leurs modes de distribution, etc.

Source : AFG.

3. L'écosystème des sociétés de gestion de portefeuilles

L'écosystème le plus proche d'une société de gestion est composé de dépositaires, de conservateurs, de teneurs de comptes, de commissaires aux comptes, d'auditeurs, de courtiers et de centralisateurs logés dans la plupart des cas chez le teneur de compte ou le dépositaire du fonds.

La société de gestion dans son écosystème



Source : AFG.

Deux grands axes se distinguent dans l'activité de la société de gestion :

- La gestion de l'actif qui englobe l'ensemble des activités liées à la gestion financière et constitue le cœur de métier des sociétés de gestion. Les principales activités sont les activités de marché liées à l'allocation, la sélection de titres et la réalisation des investissements : achat et vente de titres détenus en portefeuille, passation d'ordres, négociation, confirmation et contrôle de ces ordres, etc. ; et

- La gestion du passif qui regroupe les activités liées à la centralisation des ordres de souscriptions ou de rachats des porteurs, aux opérations de règlement-livraison, ainsi que pour la gestion collective à la tenue de compte émetteurs de l'OPC avec la mise à jour du nombre de parts en circulation de l'OPC.

La gestion du passif concerne ainsi en amont le processus de distribution et en aval la tenue de comptes/du registre des porteurs et la conservation[41]. Elle est exploitable par toutes les fonctions de la SGP : commerciales, marketing, contrôle de risques, fonctions financières, gestion, direction générale. Elle constitue à la fois une obligation réglementaire de plus en plus encadrée et un élément clé de la relation client et de la connaissance de ce dernier.

La gestion du passif : outil pour la connaissance client

Les différents acteurs impliqués dans la gestion du passif sont :

Le Centralisateur : réceptionne l'ensemble des ordres de souscription et de rachat sur les parts d'OPC venant des distributeurs et contrôle leur conformité aux conditions explicitées dans le prospectus ou dans la convention de commercialisation. Une fois la valeur liquidative connue, le centralisateur se charge de convertir en montant les ordres libellés en part, et inversement. Il communique les diverses informations collectées à la société de gestion, au teneur de compte émetteur (création ou radiation des parts) et au dépositaire de l'OPC (mouvements de fonds).

Le dépositaire/Conservateur : les sociétés de gestion ne peuvent détenir ni titres ni espèces en provenance de leurs clients. Les instruments financiers constituant le portefeuille de leurs véhicules d'investissement (OPC et mandats en titres vifs) sont alors, de par la réglementation, confiés à une entité distincte, le dépositaire pour les OPC et le teneur de compte-conservateur (**TCC**) pour les mandats. Les principales fonctions du dépositaire sont :

- La conservation des actifs des fonds ou mandats. Il s'agit d'assurer la tenue à jour des comptes titres et espèces, de conserver les titres de propriété des instruments financiers, de recevoir les ordres de règlement-livraison et de les exécuter en relation avec le dépositaire central ou les dépositaires locaux ou étrangers, et enfin d'informer le fonds et de traiter les opérations sur titres intervenant sur les portefeuilles ;

[41] *Gestion du passif des OPC et enjeux réglementaires*, Kramer Levin, juillet 2014

- Le contrôle de la régularité des décisions prises pour le compte du véhicule d'investissement. Il s'agit de la vérification de la conformité des décisions d'investissement effectuées par l'OPC aux dispositions législatives et règlementaires et au prospectus (règles de composition de l'actif, de répartition des risques, etc.). Le dépositaire est aussi en charge du calcul périodique de la valeur liquidative, vérifie les documents produits par la SGP (rapports annuels, comptes, états périodiques, etc.) et doit être en mesure d'évaluer les procédures et systèmes informatiques utilisés par la société de gestion ;

- La surveillance des flux de liquidité. Le dépositaire doit garantir un suivi efficace des flux de liquidités de l'OPC, qu'il soit un Organisme de Placement Collectif en Valeurs Mobilières (**OPCVM**) ou un Fonds d'Investissement Alternatif (**FIA**), dans le but de prévenir les fraudes ainsi que de garantir la lutte contre le blanchiment et la prévention du terrorisme

Le dépositaire central offre des services tels que l'enregistrement des titres lors de l'émission, leur conservation centralisée et leur livraison contre espèces en cas d'opération sur les marchés financiers. En France, le dépositaire central est Euroclear.

L'Agent de Transfert : Dans le cadre de la commercialisation à l'étranger de leurs OPCVM, les sociétés de gestion ont recours à un agent de transfert (*transfer agent*), intermédiaire incontournable de la distribution transfrontière. Outre son rôle de collecteur des ordres de souscription et de rachat sur l'ensemble du pays de commercialisation, il tient également les positions de chaque commercialisateur, calcule les commissions de distribution attendues et diffuse les éléments de *reporting* associés. L'agent de transfert est donc pour l'étranger ce que le teneur de compte émetteur, le teneur de registre et le centralisateur sont en France.

Le suivi du passif regroupe :

- Deux fonctions réglementées et définies par le règlement général de l'AMF :

    - La fonction de centralisateur peut-être exercée par l'OPC lui-même, la société de gestion, un Prestataire de Services d'Investissement (**PSI**) ou, cas le plus fréquent, par le dépositaire ;

    - La fonction de teneur de compte-émetteur. Cette fonction est assurée par l'OPC lui-même, sous sa responsabilité : il ne peut déléguer cette activité qu'à un PSI et uniquement dans les conditions indiquées dans le Règlement Général de l'AMF. Il conserve néanmoins pleine responsabilité vis-à-vis des investisseurs.

- Une pratique développée initialement pour suivre les encours sur lesquels la société de gestion s'engage à rémunérer un distributeur : la tenue de position des souscripteurs.

Le suivi du passif permet généralement d'identifier les souscripteurs – investisseurs institutionnels au sens large – et les établissements teneurs de compte des souscripteurs de détail. Il permet de connaitre la clientèle ou type de clientèle des fonds. Le suivi du passif est ainsi un levier important pour le développement commercial et l'amélioration de la rentabilité des sociétés de gestion.

Un outil de suivi du passif constitue le lien entre les fonctions finance, risque, marketing et commerciales. Il représente la base nécessaire à toute mise en place de processus visant à améliorer et à contrôler l'efficacité et la rentabilité commerciale de la société de gestion :

- Connaissance du client et donc meilleure efficacité commerciale ;

- Gestion du risque de liquidité des fonds, ce qui devient une obligation règlementaire, surtout pour les fonds à effet de levier ;

- Perspective d'efficience de gestion en adaptant la gestion de l'actif aux justes contraintes du passif, jetant les bases d'une gestion actif/passif pour des fonds.

4. Les modèles CSD et Transfert Agent

Selon le modèle Transfert Agent, les ordres relatifs aux fonds et le système règlement-livraison sont traités de manière bilatérale entre les institutionnels ou les distributeurs et les agents de transfert. Ce modèle est répandu au Luxembourg, en Irlande, au Royaume-Uni et en Espagne. Au contraire, sous le modèle CSD, adopté en France, Allemagne, Norvège, Autriche et Portugal, l'infrastructure relative aux ordres sur fonds et au règlement-livraison est fournie principalement par les dépositaires centraux.

Il s'agira ici d'analyser les effets potentiels de la DLT sur ces deux systèmes, sans pour autant porter un quelconque jugement de valeur sur le mérite de ces deux systèmes ou établir une hiérarchie entre eux.

A titre préliminaire, il doit être souligné que le développement des registres distribués est naturellement susceptible d'inciter les émetteurs à substituer au système des titres au porteur, largement plébiscité en France jusqu'à aujourd'hui, celui des titres au nominatif naturellement plus compatible avec les DLT.

4.1. Le modèle CSD

En France, l'administration des fonds est chargée de la comptabilité et de la valorisation des actifs des OPC mais non de la collecte des souscriptions et rachats des parts de l'OPC ou de la tenue du passif. Un centralisateur, indépendant de l'administrateur de fonds, collecte les ordres de souscriptions et de rachats sur les parts de l'OPC et donc les flux sur le passif de celui-ci. Son rôle se limite à la gestion des flux : il ne reconstitue pas les stocks, i.e. la tenue de position du passif.

En vertu du Règlement général de l'AMF[42], les tâches essentielles relatives à la centralisation des ordres sur les parts d'OPC sont les suivantes :

- Assurer la réception centralisée des ordres et procéder à l'enregistrement correspondant ;

- Contrôler le respect de la date et de l'heure limite de centralisation des ordres mentionnées dans le prospectus ;

- Communiquer en montant et, le cas échéant, en nombre global de parts/actions souscrites et rachetées le résultat de la réception centralisée des ordres à l'OPC ;

- Valoriser les ordres après avoir reçu de l'OPC l'information relative à la valeur liquidative de l'action/part concernée ;

- Communiquer les informations nécessaires à la création et à l'annulation des parts/actions au teneur de compte émetteur ; et

- Communiquer les informations relatives au résultat du traitement des ordres à l'entité qui a transmis l'ordre au centralisateur et à l'OPC.

La tenue de position du passif des OPC en France, qui est à distinguer de la tenue de compte émission[43], est donc toujours déduite de l'ensemble des flux et n'est ni normée ni règlementée. Elle est assurée soit par la SGP elle-même, le centralisateur ou une tierce partie.

La tenue de position du passif des OPC est la ventilation du nombre de parts ne revêtant pas la forme nominative par investisseur ou par intermédiaire en relation avec l'investisseur – distributeur ou teneur de compte conservateur.

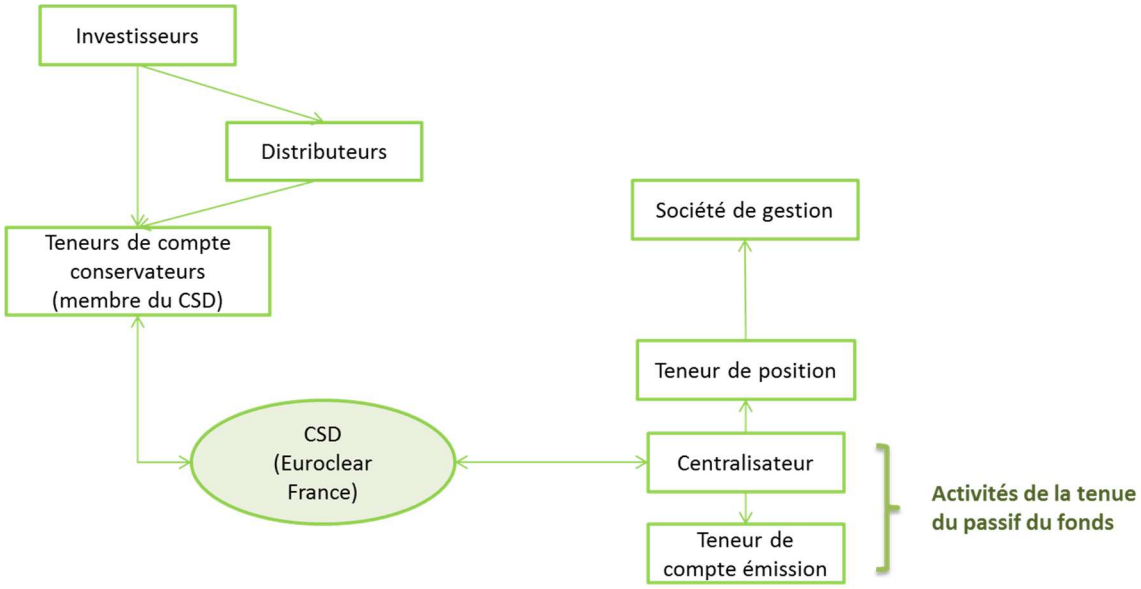
En France, le système de marquage des ordres de souscription et de rachat sur les parts d'OPC permettant de ventiler les flux n'est pas obligatoire, mais a fait l'objet de recommandations de la part de l'Association Française de la Gestion Financière (**AFG**) et de l'Association française

[42] Articles 411-65 et 422-43 du Règlement général de l'AMF

[43] La tenue de compte émission est définie aux articles 411-70 et 422-48 du Règlement général de l'AMF

des Professionnels des Titres (**AFTI**) depuis près de 10 ans. Ce marquage, gratuit, est normé via une codification SWIFT.

Le modèle CSD simplifié peut être présenté comme suit :



Ce modèle implique la désignation d'un centralisateur chargé de collecter les ordres de souscription et de rachat et de les exécuter au nom de l'OPC[44]. Les parts d'OPC en Euroclear France étant des titres au porteur, l'identité de l'investisseur final n'est pas connue du centralisateur.

Il n'existe pas de registre des actionnaires d'un OPC[45] mais seulement un compte émetteur géré par le teneur de compte émetteur et détenu en Euroclear France. Ce compte émetteur reflète le nombre total de parts sur le marché.

Dans le circuit français des souscriptions/rachats, 3 organisations sont courantes pour un même processus :

- La SGP est aussi centralisateur, teneur de positions, teneur de compte ;
- La SGP est uniquement teneur de position ; ou
- Le centralisateur est aussi teneur de position et teneur de compte émission

[44] *Gestion du passif des OPC et enjeux réglementaires*, Kramer Levin, juillet 2014

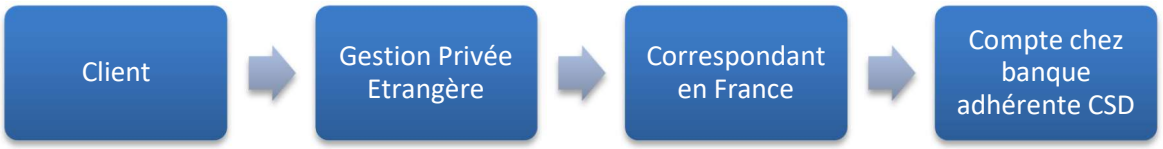
[45] Dans le cas d'inscription en nominatif pur, il est possible de tenir un registre actionnaires pour un OPC.

POUR LA SOCIETE DE GESTION	
Avantages du modèle CSD	**Inconvénients du modèle CSD**
- Probabilité d'erreur faible avec la livraison contre paiement - Faible coût car le modèle n'est pas spécifique au fonds mais à l'ensemble des transactions financières, d'où des économies d'échelle importantes - Possibilité d'utiliser les fonds dans la gestion du collatéral - Utilisation des codes internationaux (BIC, BIC1) - Souplesse du marquage permettant d'identifier l'entité recherchée par la SGP	- La connaissance du passif des OPC est approximative - Il n'a pas toujours de cohérence entre les attestations de position et le marquage des ordres - Difficulté à identifier les transferts de position d'un investisseur entre deux TCC, dû à l'absence de marquage des ordres ou connaissance des investisseurs
POUR L'INVESTISSEUR INTERNATIONAL	
Avantages du modèle CSD	**Inconvénients du modèle CSD**
- Probabilité d'erreur faible avec la livraison contre paiement - Souplesse du modèle avec possibilité d'accepter les ordres directs - Un investisseur ayant un compte-titres en France peut y rassembler tous ses actifs moyennant des droits de garde.	- Obligation de disposer d'un compte-titres et cash dans une banque affiliée chez le dépositaire central Euroclear France - Système ouvert aux banques non françaises qui peuvent devenir membres d'Euroclear France mais en pratique banques plutôt domestique.

Le modèle français est donc principalement bancaire : système des règlements-livraison des parts ou actions de fonds et tenue de compte à la fois de l'actif et du passif des fonds. En effet, il s'appuie sur le système CSD dont seules les banques sont adhérentes ainsi l'ensemble des flux financiers passe par ces dernières.

De même, la tenue de comptes est assurée par des établissements bancaires, contrairement au système luxembourgeois. Le modèle français impose dans la pratique que les souscripteurs de fonds possèdent un compte-titres dans une banque qui elle-même a directement ou indirectement un compte auprès du CSD. Ce modèle ne permet pas d'identifier facilement les distributeurs et investisseurs, ce qui complexifie pour les SGP le suivi des distributeurs et la gestion du partage des commissions sur encours.

Sur les règlements-livraisons et la tenue de compte au passif des fonds, il existe une considérable hétérogénéité des processus. Chaque souscription peut passer par plusieurs règlements livraisons successifs et plusieurs inscriptions en comptes.



Les inscriptions en compte des flux de souscriptions rachats ne prévoient pas toujours d'identifier le bénéficiaire final. Les intermédiaires parfois agrègent les flux ce qui dénature la qualité du marquage de l'identité du bénéficiaire.

Le marquage des ordres de souscriptions rachats oblige à dévoiler aux intermédiaires quels sont les clients de la SGP, puisque le marquage via le BIC/BIC1 identifie formellement la personne morale à l'origine de la souscription rachat.

En résumé, le modèle CSD repose sur un système identique à l'actif et au passif des fonds, alors que les besoins sont très différents : des informations supplémentaires sont nécessaires au passif (identité de la contrepartie) qui sont perdues par les systèmes de compensation.

4.2. Le modèle Agent de Transfert

Au Luxembourg par exemple, l'administration des fonds comprend la fonction d'agent de transfert, dont la fonction principale est la tenue du registre des parts des fonds (OPC). Cette tenue de registre est règlementée mais les codifications ne sont ni normées ni homogènes pour un même investisseur.

Aucun centralisateur n'intervient ainsi, ce rôle étant assuré par l'agent de transfert. Ce dernier dispose d'un un périmètre d'activité élargi incluant :

- le traitement des souscriptions et rachats et de la conversion des parts du fonds ;

- le contrôle de l'identité des porteurs et de l'origine des fonds investis par ceux-ci ;

- la surveillance de l'entrée des liquidités ;

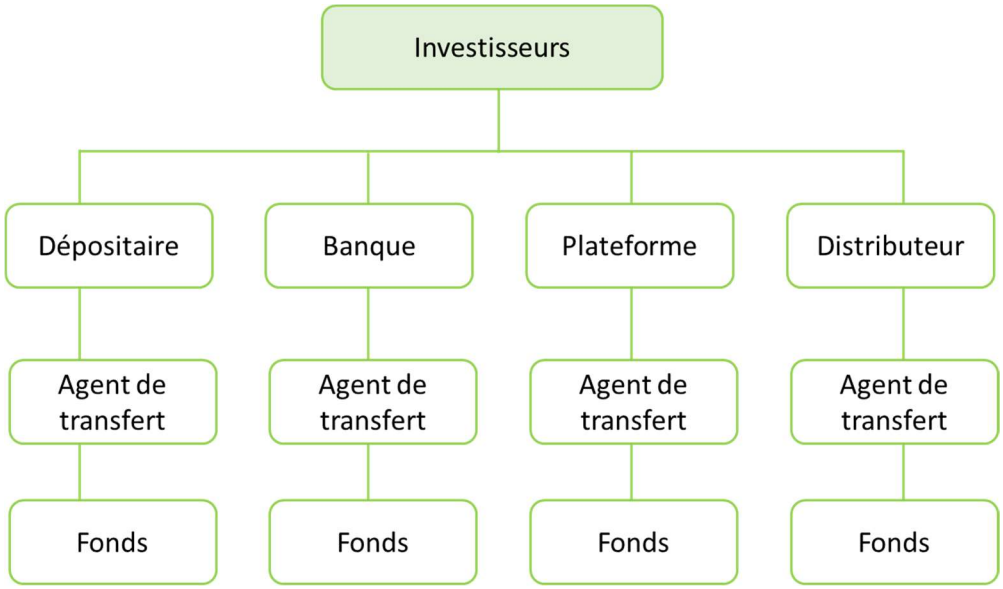
- la tenue d'un registre nominatif de certains porteurs de parts du fonds et de tout transfert de propriété des parts du fonds. Il est à noter que certains porteurs ne sont pas identifiés dans le registre qui utilise alors des comptes *omnibus*, notamment pour les porteurs dont les parts sont livrées via les CSD comme Euroclear ou Clearstream ;

- la surveillance des transactions et l'identifier des transactions douteuses ou criminelles ;

- le contrôle de l'envoi des relevés, rapports, avis et autres documents destinés aux porteurs de parts du fonds ;

- la gestion de tous les événements sur les parts émises par le fonds : distribution ou réinvestissement des dividendes, fusion de fonds ou de compartiments, etc. ; et

- le calcul et le paiement des rétrocessions aux distributeurs (*trailer fees*).



Source : Kramer Levin

L'agent de transfert tient le registre officiel de l'OPC et est la seule entité mandatée pour réaliser la collecte, le traitement et la confirmation des ordres[46]. Après confirmation de l'ordre de la part du TA, le client ou son entité répresentante donne l'instruction à sa banque pour créditer le compte du fonds. Par ailleurs ce compte est tenu généralement par le dépositaire de l'OPC, dans certains cas l'agent de transfert peut tenir des comptes dédiés auprès d'une banque intermédiare. Dans tous les cas, le TA est le seul à réconcilier les flux espèces avec les transcations qu'il a exécutées.

POUR LA SOCIETE DE GESTION	
Avantages du modèle TA	**Inconvénients du modèle TA**
- Connaissance du passif des OPC pour les investisseurs en compte chez le TA - Information de l'identification des flux et confirmés par des attestations de position	- Connaissance incomplète du passif lorsque les investisseurs sont intermédiés - Pas d'harmonisation des procédures - Coûts plus élevés - Autant d'enregistrement que de TA - Lien très difficile pour la gestion du collatéral - Rigidité du registre
POUR L'INVESTISSEUR INTERNATIONAL	
Avantages du modèle TA	**Inconvénients du modèle TA**
- Ouverture compte-titres simple et rapide - Responsabilité de la tenue de position chez le TA - Constitue un Benchmark historique - Pas d'intermédiation bancaire	- Autant de comptes titres que de TA - Pas ou peu d'harmonisation des procédures - Coûts plus élevés - Procédure KYC plus lourde en cas de TA multiples

[46] *Gestion du passif des OPC et enjeux réglementaires*, Kramer Levin, juillet 2014

5. Blockchain, règlement-livraison et tenue des comptes

De façon générale, la DLT pourrait remplacer la plupart des "*tiers de confiance*" centralisés – banques, compensateurs, notaires, cadastre, etc. – par des systèmes informatiques distribués.

A titre d'illustration, pour effectuer des transactions financières, les banques passent aujourd'hui par des chambres de compensation et de *clearing* (**CCP**). Ces dernières sont des tiers de confiance qui vérifient la licéité d'une transaction. Elles vérifient également que l'acheteur reçoit bien son titre de propriété et le vendeur les sommes dues à ce titre.

Si leur rôle de garantie est capital dans une transaction, les CPP restent des systèmes complexes et centralisés. À titre d'exemple, une opération complexe portant sur des marchés à terme peut prendre jusqu'à deux jours pour assurer un *clearing* complet. Avec une blockchain, ce délai est considérablement réduit, jusqu'à une dizaine de minutes. Le système étant automatisé, la blockchain pourrait par ailleurs permettre de se passer totalement de certains intermédiaires financiers comme les CPP.

Source : Fundsquare

L'avantage est donc double pour les SGP :

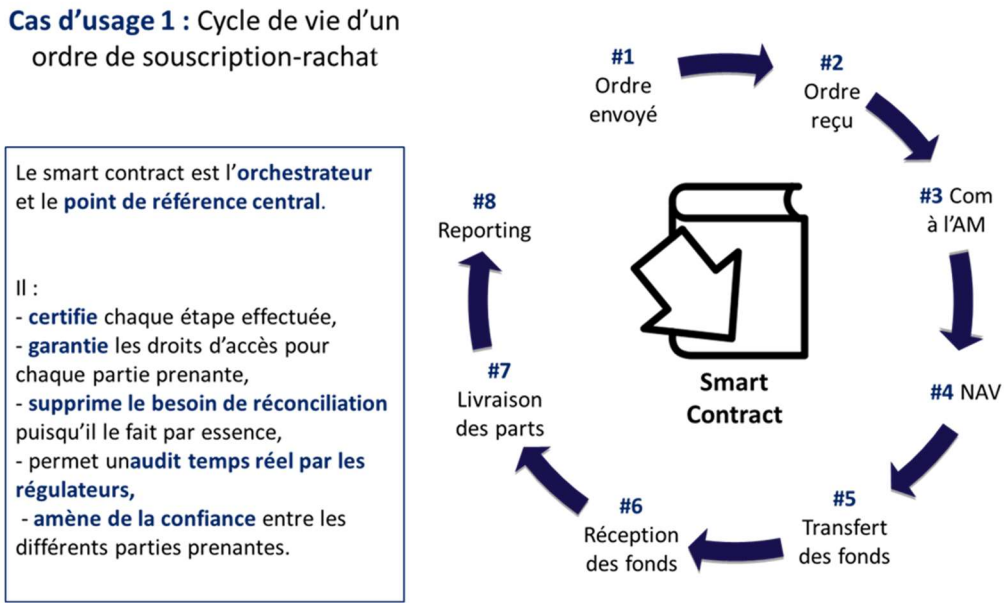
- Les transactions effectuées via une blockchain sont plus fiables, puisque sécurisées mathématiquement grâce à un algorithme infalsifiable. On évite donc le risque d'erreur imputable au tiers de confiance qui disparaît ; et

- La disparition du tiers de confiance réduit mécaniquement les coûts, en l'occurrence les commissions perçues par ce dernier.

Quel que soit le modèle d'infrastructure (blockchain privée ou publique) gardant ou non les intermédiaires en place, il faut envisager le registre distribué comme un registre commun à l'ensemble des banques, générant des économies d'échelles massives et réduisant d'autant plus les coûts unitaires par transaction.

La blockchain pourrait apporter de la sécurité, la confidentialité et l'identification du client à un coût compétitif. La DLT permettrait de se passer d'intermédiation pour établir une information sécurisée entre deux parties.

Ce système identifie la validité des flux et la Balance Comptable Décentralisée (*Decentralised Ledger Platform* – **DLP**) et historise le détail des transactions bloc par bloc.



Source : UTOCAT

A ce stade, un registre distribué publique de gestion des souscriptions/ rachats permettrait un accès à de nombreux acteurs. Les SGP et les investisseurs pourraient adhérer directement à ce système sans nécessairement être tenus de passer par un établissement bancaire teneur de compte titres.

Ce système permettrait de dépasser l'opposition actuelle entre modèle CSD et modèle TA et d'avoir une organisation transverse et homogène quel que soit la juridiction du fonds de la SGP ou de l'investisseur.

Certains points doivent cependant nécessairement être adressés avant toute utilisation de la DLT :

- Comme les informations de la blockchain sont anonymisées, il faudra prévoir des clés d'identification permettant de réattribuer l'historique des évènements aux entités juridiques concernées ;

- Les informations échangées dans la blockchain doivent être standardisées voire normalisées pour être exploitables, y compris sur longue période – une multitude de standards empêcheraient les économies d'échelle – et ce quelle que soit la DLT utilisée ; et

- Pour que la tenue de comptes-titres via une blockchain présente un niveau de sécurité satisfaisant, il faudrait que le droit reconnaisse les modalités d'enregistrement et de conservation.

Une fois ces points adressés, les avantages pour une SGP sont les suivants :

- La SGP pourrait disposer d'une information détaillée et homogène sur l'ensemble du passif de ses fonds sans avoir recours au centralisateur ou au teneur de compte- titres ;

- Ce qui permettrait d'imaginer une multitude de services au profit des investisseurs des fonds puisqu'ils sont connus et tracés.

Les points technologiques et réglementaires restant à traiter seront alors les suivants :

- Compatibilité de l'utilisation de DLT avec la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 et le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (*General Data Protection Regulation* – **GDPR**) applicable à partir du 25 mai 2018. Cette question est plus amplement abordée ci-dessous ;

- Reconnaissance ou non des crypto-monnaies par les banques centrales ou reconnaissance du *token* comme un mode de paiement ;

- Qui serait le tiers de confiance dans une blockchain publique ?

- Quel critère permettrait de détermine la propriété d'un titre traité au sein d'un registre distribué ?

E. ACTIVITES DE TENUE DE REGISTRE

1. Contexte général de la tenue de registre

Contrairement aux activités de post-marché, les titres non admis aux opérations d'un dépositaire central et non émis par une société par offre au public ne font pas l'objet d'une tenue de compte conservation auprès d'un intermédiaire habilité à cet effet. Ces titres font alors l'objet d'une tenue d'un registre de titulaires de titres nominatifs par la société émettrice[47]. Lorsqu'ils sont émis par un OPC, ces titres font l'objet d'une tenue de "compte émission" de parts ou actions[48].

Bien qu'il ne s'agisse pas de tenue de compte conservation, les inscriptions des titres au nom de leurs titulaires dans les registres tenus par les émetteurs, les OPC ou leurs mandataires sont réalisées sur des "comptes titres"[49].

Les titres concernés n'ont pas vocation à quitter la forme nominative : seuls les titres admis aux opérations d'un dépositaire central peuvent circuler sous la forme porteur sous réserve de la latitude laissée par l'article L. 211-7 du Code monétaire et financier pour les parts et actions d'OPC.

Un propriétaire de titres financiers nominatifs peut charger un intermédiaire habilité en tant que teneur de compte conservateur d'administrer son compte de titres ouvert chez un émetteur. Les titres prennent alors la forme nominative administrée[50]. Dans ce dernier cas, lorsque les parts ou actions d'OPC circulent à la fois sous la forme nominative et au porteur, une réconciliation des titres est nécessaire.

2. Règles professionnelles de la tenue de registre

Pour permettre aux émetteurs, ou à leurs mandataires, le cas échéant, et aux teneurs de compte-conservateurs de faire face à leurs obligations respectives, et à ces derniers de traiter les opérations initiées par les émetteurs ou les détenteurs d'instruments financiers dans des conditions optimales, un cahier des charges a été établi sous l'égide du Comité Français d'Organisation et de Normalisation Bancaires (**CFONB**).

[47] Articles R. 228-7 à R. 228-9 du Code de commerce

[48] Articles 411-70 RGAMF (OPCVM) et 422-48 RGAMF (FIA)

[49] Article L. 211-3 du Code monétaire et financier

[50] Article R. 211-4 du Code monétaire et financier

Ce cahier des charges, dont la version la plus récente date de 2013[51], décrit l'ordre de mouvement normalisé, seul support des mouvements d'instruments financiers entres les sociétés émettrices ou leurs mandataires et les teneurs de compte-conservateurs en charge de l'administration des comptes de titres nominatifs administrés. Ce cahier des charges a valeur de règles professionnelles au sens de l'article 322-54 du Règlement général de l'AMF lorsque les titres ont été émis par offre au public.

3. Difficultés pratiques de la tenue de registre

Le virement est le fait, pour le teneur de compte, de débiter un compte d'un certain nombre d'instruments financiers pour en créditer un ou plusieurs autre(s) du même nombre. Le virement en registre nominatif s'effectue aujourd'hui et de façon pratique au moyen d'un ordre de mouvement signé par le cédant à l'appui duquel la société émettrice constate l'opération intervenue et procède dans le registre nominatif au virement des titres requis.

La cause du mouvement de titres peut être :

- soit une cession sous quelque forme que ce soit : vente, échange, donation ou apport de titres ;

- soit une opération sur titres : attribution, souscription, etc. ;

- soit un virement sans changement de propriété ou toute autre opération impliquant un virement de titres : conversion du nominatif pur vers le nominatif administré, et inversement.

Les lourdeurs administratives pour réaliser le virement des titres inscrits en registre sont nombreuses dans la mesure où ce virement repose sur un document dont les originaux doivent être échangés en plusieurs exemplaires entre les différents intervenants. Or, tant que l'inscription en compte n'est pas matériellement intervenue, le transfert de propriété ne s'est pas réalisé au bénéfice du cessionnaire et l'opération n'est pas opposable aux tiers.

Ces difficultés sont d'autant plus importantes lorsque les titres bénéficient ou sont soumis à un régime fiscal spécifique : PEA, titres issus d'options de souscription ou d'acquisition de titres, actions gratuites, BSCPE, etc. Or, l'ordre de mouvement n'a pas vocation à véhiculer des informations d'ordre fiscal.

Il existe également ici un potentiel dans le recours à une technologie DLT, où elle peut apporter sécurité et efficacité aux émetteurs ou à leurs mandataires, aux intermédiaires financiers teneurs

[51] *Cahier des Charges applicable aux teneurs de comptes d'instruments financiers français non admis aux opérations d'un dépositaire central,* Communication CFONB n° 2013-0041

de compte et, bien entendu, investisseurs. Et ce d'autant plus que le Règlement européen CSDR du 23 juillet 2014 relatif aux dépositaires centraux prévoit clairement le cas d'une pluralité de dépositaire, émetteur et teneur de registre pour mettre en place des « *mesures adéquates de coopération et d'échange d'informations afin de maintenir l'intégrité de l'émission* »[52]

Focus sur les produits dérivés

La présente section vise à contribuer à élargir la réflexion sur l'utilisation de la DLT sur les produits dérivés, désignés en droit français sous le terme de *contrats financiers* ou d'*instruments financiers à terme*.

La DLT, un enjeu important pour les produits dérivés

Comparativement aux activités post-marché, l'utilisation de la DLT dans l'industrie des produits dérivés n'a donné lieu qu'à assez peu de cas d'usage et n'a pas été au cœur des différents rapports des régulateurs européens ou d'institutions internationales mentionnés ci-après.

La DLT représente cependant un enjeu très important pour les produits dérivés pour deux raisons principales.

Tout d'abord, de manière structurelle, les produits dérivés demandent un important travail de réconciliation des données entre les deux parties au contrat, dans la mesure où notamment la valeur du contrat varie en fonction de la valeur d'un actif sous-jacent.

Ensuite, suite à la crise financière de 2008, des engagements ont été pris au niveau international (G20 de Pittsburgh en 2009) afin de mieux encadrer réglementairement les dérivés, se traduisant par une déclaration des transactions à des référentiels centraux, une obligation de compensation pour certains dérivés standardisés et des exigences de collatéralisation renforcées pour les dérivés non compensés (Règlementation EMIR[53] dans l'UE), obligeant notamment les parties à un travail de réconciliation plus fréquent.

[52] Règlement 909/2014 du parlement européen et du Conseil du 23 juillet 2014 relatif aux dépositaires centraux de titres, Article 37.1 et 37.2 : « *Le DCT prend les mesures de rapprochement comptable appropriées afin de vérifier que le nombre de titres qui composent une émission ou une partie d'émission qui lui est confiée est égal à la somme des titres enregistrés sur les comptes de titres des participants au système de règlement de titres qu'il exploite et, le cas échéant, sur les comptes de titulaires qu'il tient. Ces mesures de rapprochement comptable sont effectuées au moins quotidiennement.*
2. Le cas échéant, et si d'autres entités, par exemple, l'émetteur, un teneur de registre, un agent d'émission, un agent de transfert, un dépositaire commun, un autre DCT ou une autre entité, participent au processus de rapprochement comptable pour une émission donnée, le DCT et toute autre entité concernée conviennent de mesures adéquates de coopération et d'échange d'informations afin de maintenir l'intégrité de l'émission ».

[53] Règlement (UE) 648/2012 du Parlement européen et du Conseil du 4 juillet 2012 sur les produits dérivés de gré à gré, les contreparties centrales et les référentiels centraux.

La DLT, en ce qu'elle permet aux utilisateurs de stocker et d'accéder à des informations relatives à un ensemble donné d'actifs et de pouvoir effectuer des transactions enregistrées dans un réseau, devrait donc permettre une plus grande efficacité dans la gestion par les parties de leurs transactions dérivées.

Les projets récents d'application de la DLT aux produits dérivés

Différents projets ont été lancés ou sont en cours, même si l'information publique disponible relativement à ces projets reste pour l'instant parcellaire.

Le point commun de ces différents projets réside dans la volonté *:*

- d'intégrer dans un système d'information partagé entre différentes parties des éléments qui étaient traditionnellement conservés dans les systèmes d'information propres de chacune des parties à une transaction sur produits dérivés ; et

- d'intégrer au maximum les aspects juridiques directement dans les systèmes d'information.

Sur l'exécution des transactions sur une blockchain, le projet[54] a consisté à intégrer au départ dans un *smart contract* des informations essentielles sur une opération de produit dérivé simple, puis à exécuter cette transaction sur une blockchain. L'opération a impliqué des flux lors de sa mise en place, en cours de vie et lors de son dénouement. Le projet a été réalisé sur la plateforme Corda du consortium R3.

Gestion des événements affectant les sous-jacents au cours de la vie de la transaction : la *Depositary Trust and Clearing Corporation* (**DTCC**) a lancé début 2017 un projet de refonte de la base *Trade Information Warehouse*, un registre servant à la fois à la collecte des informations sur les opérations de produits dérivés et à la gestion des événements *post-trade* affectant les sous-jacents de dérivés de crédit, sur le principe d'une blockchain. La gouvernance serait assurée par DTCC, les entreprises participantes disposant chez elles d'une copie du registre distribué. Le projet s'appliquerait à tous les *credit default swaps*, qu'ils fassent l'objet d'une compensation centrale ou non.

Les principales difficultés lors de la mise en place de projets blockchain appliqués aux produits dérivés semblent consister en *:*

- la nécessité de pouvoir réunir un nombre important de contreparties afin que le réseau puisse acquérir une masse critique ;

- le degré de maturité des plateformes actuelles blockchain ; et

[54] Projet mené notamment par Barclays en avril 2016.

- l'intégration de ces blockchains avec les systèmes informatiques existants des institutions financières.

L'ISDA et le développement des *smart contracts*

L'usage de la blockchain permettrait de poursuivre l'effort de standardisation de la documentation publiée par l'International Swap and Derivatives Association (**ISDA**).

Rappelons que l'ISDA a été créée en vue de standardiser au maximum les opérations de produits dérivées OTC afin de faciliter le processus de négociation des transactions entre les parties et la gestion de ces transactions. Cet objectif historique a été récemment rappelé au cours d'une publication de septembre 2016[55] dans laquelle l'ISDA réaffirme sa volonté d'intégrer au maximum les évolutions technologiques aux produits dérivés en tenant compte tout particulièrement de l'accroissement du poids de la réglementation.

La récente publication en août 2017[56] d'un livre blanc questionnant l'apport de la DLT et des *smart contracts* aux produits dérivés s'inscrit donc dans cette tendance de fond visant à standardiser au maximum la documentation de ces produits et à intégrer les apports de la technologie.

Une blockchain appliquée aux produits dérivés fonctionnerait de la manière suivante : la blockchain, privée, ne serait ouverte qu'aux seuls membres participants et les transactions seraient enregistrées dans ce registre distribué. Un *smart contract* déployé sur le réseau effectuerait de manière automatique certaines actions relativement à certaines transactions.

Cela permettrait de résoudre le problème pour les parties d'avoir plusieurs versions d'un même document stockées dans différents endroits et d'obtenir à intervalles réguliers un consensus sur la valeur d'un contrat dérivé et du *collateral* remis au titre de la transaction.

Contrats juridiques et code informatique

Ce récent livre blanc met en lumière des problématiques intéressantes, tournant principalement autour de la question de savoir jusqu'où un contrat peut être intégré à un code informatique. La conclusion serait qu'il n'est pas possible pour un contrat juridique d'être intégralement reflété dans un code informatique qui s'exécuterait automatiquement sur une blockchain. Ce qui justifie la distinction proposée par certains entre le *smart legal contract*,

[55] *The Future of Derivatives Processing and Market Infrastructure*. ISDA Whitepaper, septembre 2016

[56] *Smart Contracts and Distributed Ledger – A Legal Perspective,* ISDA / Linklaters Whitepaper, août 2017

accord juridique entre les parties pouvant intégrer du code informatique, et le *smart contract code*, le code informatique exécutable directement sur la blockchain.

Il ressort qu'au mieux le *smart contract code* pourrait remplacer certaines clauses opérationnelles du contrat de la transaction dérivée ou, à défaut, n'être qu'une manière d'automatiser des clauses déjà existantes du contrat. Parmi les clauses opérationnelles qui seraient aisément transposables en *smart contract code*, on trouverait par exemple les clauses précisant qu'un paiement doit être effectué à une date donnée en fonction de certains paramètres déterminables – tel par exemple le *pay-off* d'une option. Parmi les clauses non opérationnelles qu'il ne serait pas possible de réduire en *smart contract code*, on trouverait par exemple celles précisant la loi applicable au contrat entre les parties, le choix de la juridiction applicable en cas de litige, ou encore des déclarations faites par les parties.

Encourager le développement du *smart contract code* nécessiterait un important travail de reformalisation des définitions ISDA. En outre, la difficulté à tout automatiser tient notamment au fait qu'il est possible pour les parties d'effectuer certains choix en cours de vie de la transaction – par exemple, si un cas de résiliation survient, l'une des parties peut décider d'exercer ou non ce droit pendant un certain laps de temps, ce qui ne semble pas programmable *a priori*.

En revanche, lorsque des informations extérieures au contrat sont nécessaires pour l'exécution du code informatique, elles pourraient être remplacées par des déterminations d'oracles tiers –par exemple pour un CDS, une détermination du *Credit Derivatives Determinations Committee*) afin de permettre la poursuite de l'exécution du programme informatique.

Focus sur la Caisse des Dépôts

En tant que tiers de confiance public historique, la Caisse des Dépôts s'est intéressée très tôt à la DLT, initiant ses programmes blockchain et lançant dès 2015 LaBChain, le premier consortium européen dédié à l'exploration collective de la DLT et de ses usages dans les métiers de la banque finance assurance, qui compte aujourd'hui 29 membres financiers, technologiques et institutionnels.

Par cette démarche d'innovation, techno-agnostique puisqu'elle ne se limite à aucun protocole, la Caisse des Dépôts ambitionne d'utiliser la blockchain comme une infrastructure numérique publique pour améliorer la résilience, la transparence et l'efficacité des systèmes

financiers existants tout en créant de nouveaux services en support de l'écosystème français et au service des citoyens.

En collaboration avec la Place financière et avec le vivier français de startups blockchain, la Caisse des Dépôts est engagée dans la réalisation de nombreuses expérimentations relatives à différents cas d'usage de la blockchain, nourrissant une démarche de recherche et développement, d'acculturation aux fonctionnalités, avantages et limites de la blockchain ainsi que son dialogue, en tant qu'interlocuteur privilégié, avec le régulateur et le législateur sur les enjeux et l'avenir juridiques des technologies de registre distribué.

Au-delà de la dizaine de projets stratégiques pour l'Établissement Public et ses filiales en cours sur divers secteurs d'activités, la Caisse des Dépôts expérimente la blockchain dans les métiers financiers dans le cadre de LaBChain notamment pour la gestion du collatéral-titre, l'identité numérique et les KYC. Elle le fait également dans le cadre d'un Partenariat de recherche avec l'institut de recherche IRT SystemX sur une plateforme dédiée au Fintech-Regtech.

La Caisse des Dépôts a par ailleurs lancé, avec BNP Paribas, CACEIS, Euroclear, Euronext, S2iEM et Société Générale et avec le soutien de Paris Europlace, la création de la start-up LiquidShare, nouvelle Fintech européenne exploitant la DLT pour simplifier et accélérer les opérations de post-marché pour les PME non-cotées tout en réduisant les coûts de transaction. Enfin, dans le cadre de l'ordonnance de réforme du statut juridique des bons de caisse du 28 avril 2016, la Caisse des Dépôts développe, main dans la main avec l'association Finance Participative France et plusieurs de ses membres, une plateforme blockchain pour émettre, enregistrer et échanger des minibons, avec l'objectif de tester un prototype avant la fin de l'année 2017.

III. L'ENVIRONNEMENT REGLEMENTAIRE INTERNATIONAL DE LA BLOCKCHAIN

Le succès de la blockchain et le développement des crypto-monnaies n'a pas laissé indifférent régulateurs et institutions européens ou internationaux, qui ont chacun contribué à la réflexion générale en publiant de nombreuses études, voire même en proposant une réflexion pour un cadre réglementaire adéquat pour son épanouissement.

Si les régulateurs se montraient réservés voire hostiles au Bitcoin, ils portent un regard tout à fait différent sur la DLT. Les régulateurs accueillent en effet positivement cette nouvelle technologie, perçue comme un moyen d'améliorer la sécurité et l'efficience des marchés financiers.

A. POSITIONS DES INSTITUTIONS ET DES REGULATEURS EUROPEENS

1. European Securities and Markets Authority (ESMA)

L'*European Securities and Markets Authority* (**ESMA**) a déjà publié trois documents relatifs à la DLT : un appel à contribution[57], un document de consultation[58] et un rapport sur l'application de la DLT aux marchés financiers[59].

Ces trois documents dévoilent le vif intérêt de l'ESMA dans le développement de la blockchain. Consciente des enjeux et de la technicité du sujet, l'autorité a souhaité mener une réflexion en incitant dans sa démarche la participation active du public. L'appel à contribution du 22 avril 2015 témoigne du besoin des régulateurs d'apprendre davantage d'une technologie qu'ils ne connaissent que très peu. C'est pourquoi l'objectif affiché par l'autorité de régulation européenne était avant tout de collecter le maximum d'information pour comprendre les risques et les bénéfices de la technologie afin de déterminer, le cas échéant, le besoin ou non de légiférer sur cette matière.

L'ESMA voit avant tout dans la DLT le moyen de réduire sensiblement les coûts structurels des transactions sur les marchés et de développer les échanges financiers dans le secteur des titres.

---

[57] Appel à contribution du 22 avril 2015 disponible à l'adresse suivante : https://www.esma.europa.eu/sites/default/files/library/2015/11/2015532_call_for_evidence_on_virtual_currency_investment.pdf

[58] Document de consultation du 2 juin 2016 disponible à l'adresse suivante : https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf

[59] Rapport du 7 février 2017 disponible à l'adresse suivante : https://www.esma.europa.eu/sites/default/files/library/dlt_report_-_esma50-1121423017-285.pdf

Toutefois, pour l'ESMA, la DLT apparaît davantage comme un outil destiné à réduire les coûts des transactions qu'un instrument révolutionnaire pour refonder l'architecture de marché.

C'est dans le post-marché que l'ESMA reconnaît le plus fort potentiel de la DLT. Soucieuse de mettre en exergue les difficultés de la mise en place des registres distribués, notamment auprès des nouveaux entrants, l'autorité relève les principaux enjeux à résoudre avant d'envisager l'essor à grande échelle de la technologie :

- Le besoin d'interopérabilité avec les infrastructures existantes ;
- L'accès à la monnaie banque centrale ;
- La gouvernance des systèmes ;
- La protection des données inscrites sur les registres partagés ; et
- A droit constant, les risques de l'application de la législation européenne aux systèmes blockchain.

Il est également important de préciser que l'ESMA ne considère pas que le droit actuel empêche le développement de la technologie. Tout au plus, certaines dispositions mériteraient d'être clarifiées pour faciliter son fonctionnement, tant en droit financier qu'en droit des sociétés, des contrats, de l'insolvabilité ou encore de la concurrence.

2. Banque Centrale Européenne (BCE)

La Banque centrale européenne a diffusé dans le courant du mois d'avril 2016 une publication occasionnelle relative au mécanisme de la blockchain appliqué dans le secteur du post-marché[60]. L'institution précise toutefois que son contenu ne pourra refléter sa position en matière de DLT. Toutefois, ce document demeure un bon indicateur pour déterminer comment la BCE perçoit l'arrivée de cette nouvelle technologie.

A l'instar de l'ESMA, les auteurs voient en la technologie un moyen décisif pour améliorer le fonctionnement et l'attrait des marchés financiers : réduction des coûts de réconciliation, amélioration de la chaîne de valeurs dans le post-marché ou encore utilisation plus efficiente des garanties octroyées.

Le rapport partage également la circonspection de l'ESMA quant à sa capacité à pouvoir proposer une nouvelle architecture de marché. En particulier, les auteurs estiment que la

[60] Disponible à l'adresse suivante : https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf

blockchain ne semblerait pas en mesure de remplacer les actuelles chambres de compensation, notamment dans le cadre de compensation des opérations à terme.

La publication se montre également réservée sur la capacité de la DLT à surmonter à court terme les difficultés liées à sa mise en application sur les marchés.

Un rapport de l'*Advisory Group on Market Infrastructures for Securities and Collateral* (**AMI-SeCo**) de la BCE publié en septembre 2017[61] évoque plus en détail les différentes applications pratiques potentielles de la DTL en matière d'activités de marché, tout en soulignant le stade précoce de développement de cette technologie et donc la difficulté à se prononcer non seulement sur son adoption à large échelle sur les marchés financiers, mais aussi sur le type de DLT qui pourrait être adoptée le cas échéant.

3. Parlement européen

Les institutions européennes montrent un intérêt croissant pour la blockchain. Le comité *Sciences and Technology Option Assessment* (**STOA**) du Parlement européen a ainsi récemment décidé, en lien avec la Commission européenne, de mettre en place un groupe de travail autour de la DLT destiné à surveiller l'évolution et le fonctionnement de cette nouvelle technologie et déterminer le besoin ou non de légiférer.

En parallèle, la Commission européenne a publié un document de consultation portant sur les Fintechs et, entre autres, l'utilisation de la DLT, dans le courant du mois de mars 2017[62].

Une récente publication du Parlement européen de février 2017 intitulée *« How blockchain could change our lives »*[63] et rédigée par son comité STOA a été diffusé avec l'objectif de sensibiliser les parlementaires européens aux vertus de cette technologie. Le document expose de manière large les enjeux de l'adoption d'un cadre législatif pour la blockchain, sans se limiter pour autant au monde financier. Cette publication a donc une place importante dans la conception de la future réglementation européenne, puisqu'elle constituera l'une des bases de travail pour guider les travaux des députés. Si le rapport se montre enthousiaste au développement à grande échelle de la blockchain, il demeure prudent sur son aspect révolutionnaire.

B. INSTITUTIONS INTERNATIONALES

[61] The potential impact of DLTs on securities post-trading harmonisation and on the wider EU financial market integration, BCE, Advisory Group on Market Infrastructures for Securities and Collateral, septembre 2017

[62] Disponible à l'adresse suivante : https://ec.europa.eu/info/sites/info/files/2017-fintech-consultation-document_en_0.pdf

[63] Disponible à l'adresse suivante : http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf

1. Financial Stability Board (FSB)

Dans un discours prononcé le 3 novembre 2016 au cours d'une conférence[64], le secrétaire général du FSB, M. Svein Andresen, a précisé que l'organisation avait initié une réflexion sur la réglementation de la DLT afin de proposer aux régulateurs une série de recommandation en la matière.

Ces travaux sont menés en parallèle avec le comité des paiements et des infrastructures de marchés pour identifier les points clefs qui seront l'objet de son intervention auprès des pays membres.

2. Banque des Règlements Internationaux (BRI)

Le comité des paiements et des infrastructures de marchés de la Banque des règlements internationaux a publié, dans le courant du mois de février 2017, un rapport analytique sur la DLT dans les services de paiement, de compensation et de règlement livraison[65].

Ce rapport propose aux régulateurs nationaux ainsi qu'aux banques centrales une grille d'analyse et de compréhension de la technologie, afin de saisir les risques et les opportunités de sa mise en place. Rappelant les règles et les utilisations possibles du registre blockchain, le rapport souligne à nouveau le caractère immature de la technologie et l'absence de réel potentiel révolutionnaire sur l'infrastructure de marché actuelle.

La BRI a également publié en septembre 2017 une longue étude sur le crypto-monnaies dans son rapport trimestriel[66]. L'étude se penche notamment sur les *central bank cryptocurrencies* (**CBCC**), crypto-monnaies émises par les banques centrales et échangées sur un réseau pair-à-pair décentralisé. La BRI effectue une distinction entre deux formes potentielles de CBCB, la première étant un instrument de paiement largement accessible aux consommateurs (*retail CBCC*) et la seconde un token d'accès restreint pour les paiements de gros (*wholesale CBCC)*. Alors que la première garantirait aux consommateurs l'anonymat de leurs paiements comme le fait déjà la monnaie fiduciaire, la seconde permettrait quant à elle une réduction des coûts de transfert. L'étude met également en évidence certains risques potentiels associés au développement de CBCC, incluant notamment l'incitation aux *bank runs* si la monnaie scripturale est aisément échangeable contre une CBCC sans risque et l'atteinte portée au business model des établissements de crédit.

---

[64] Disponible à l'adresse suivante : http://www.fsb.org/wp-content/uploads/Chatham-House-The-Banking-Revolution-Conference.pdf

[65] Disponible à l'adresse suivante : http://www.bis.org/cpmi/publ/d157.pdf

[66] BRI, Central bank cryptocurrencies, septembre 2017 : https://www.bis.org/publ/qtrpdf/r_qt1709f.htm

3. Organisation Internationale des Commissions de Valeurs (OICV-IOSCO)

Dans un rapport sur les Fintechs[67], l'OICV développe sa vision de l'utilisation de la DLT ainsi que les solutions d'encadrement réglementaires envisageables.

Il convient de noter que l'OICV reste prudente dans l'utilisation qui peut en être faite. A ce titre, l'organisation rappelle dans son rapport les circonstances de l'attaque de The DAO et souligne les risques associés à la tenue d'un registre décentralisé unique. Si la DLT permet globalement de réduire la part de l'erreur humain dans le fonctionnement d'une infrastructure de marché, elle aggrave également les conséquences d'une erreur de codage.

L'OICV appelle avant tout à un renforcement de la coopération entre les régulateurs, d'autant plus importante que la DLT est par essence un phénomène international, sujet à entraîner le cumul des réglementations applicables et des organes de supervision.

4. Fonds Monétaire International (FMI)

Le FMI a publié deux rapports relatifs à la DLT :

- Un rapport sur les crypto-monnaies publié en janvier 2016[68] ; et
- Un rapport sur les Fintechs et les services financiers publié en juin 2017[69].

Le premier rapport détaille l'émergence des crypto-monnaies et de la DLT, en insistant sur les défis réglementaire soulevés par ces innovations technologiques. Le FMI souligne notamment les difficultés posées par l'anonymat en matière de lutte anti-blanchiment, lutte contre le financement du terrorisme, de politique fiscale et de contrôle des changes. Il met de plus en avant la protection des intérêts des consommateurs face aux transactions frauduleuses prenant appui sur la DLT et les crypto-monnaies.

Le second rapport explore les innovations potentielles des Fintechs en matière de sécurité des transactions, de confiance sur les marchés financiers, de protection de l'anonymat et de

[67] Disponible à l'adresse suivante : https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf

[68] *Virtual Currencies and Beyond: Initial Considerations*, IMF Staff Discussion Note, janvier 2016

[69] *Fintech and Financial Services:Initial Considerations*, IMF Staff Discussion Note, juin 2017, accessible à l'adresse suivante : http://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2017/06/16/Fintech-and-Financial-Services-Initial-Considerations-44985

l'amélioration des services financiers. Le FMI conclu à la difficulté d'anticiper l'ampleur des évolutions provoquées par les Fintechs au cours des années à venir. Il incite à ce titre les régulateurs nationaux à faire preuve de prudence afin de maintenir l'intégrité et la stabilité des marchés financiers, notamment en matière de lutte anti blanchiment et contre le financement du terrorisme, de cybersécurité et de l'intégrité des données, algorithmes et plateformes.

IV. LES QUESTIONS JURIDIQUES POSEES PAR LA BLOCKCHAIN EN MATIERE D'INSTRUMENTS FINANCIERS

La DLT peut impacter directement le régime juridique des instruments financiers en remettant en cause le mode de détention, le régime de transfert de propriété, mais aussi plus fondamentalement le mode de représentation des titres, avec le concept de "*e-securities*". Or, les études juridiques en Europe sur l'impact de cette technologie sont rares.

Les impacts de la DLT ne s'arrêtent cependant pas au droit des titres. Au-delà du régime juridique propre aux instruments financiers, cette technologie interroge le juriste sur bien d'autres aspects : droit de la preuve, droit de la propriété intellectuelle, protection des données personnelles, cybersécurité, etc. Toutes ces questions ne sont pas propres au droit des titres mais il convient de les examiner pour vérifier si et comment elles peuvent avoir un impact dans l'utilisation de la blockchain dans les activités de post-marché.

L'enjeu juridique posé par la DLT est d'évaluer en quoi celle-ci bouleverse ou non les concepts juridiques traditionnels et, selon le cas, la nécessité ou non de réformer en profondeur certaines branches du droit afin de l'adapter à cette technologie. La question doit être examinée tant sur les domaines transversaux du droit comme la propriété intellectuelle, la protection des données, la signature électronique ou encore la cybersécurité, que dans le droit plus spécifique qui régit les activités de post-marché.

Au présent stade de réflexion, la DLT ne s'avère pas à ce point incompatible avec le cadre juridique existant qu'il serait nécessaire de créer une nouvelle branche du droit spécifique à cette technologie. Au contraire, le droit commun permet d'embrasser de manière convaincante la plupart des questions posées par cette technologie. Si des adaptations seront sans doute nécessaires à la marge, en particulier pour la prise en compte du régime de propriété des titres enregistrés dans une blockchain, il s'agit là plus de précision que de modifications substantielles.

Les lignes qui suivent sont de simples indications et ne constituent pas une analyse juridique détaillée des impacts de cette technologie dans l'ensemble des règles de droit qui régit tel ou tel domaine du droit.

A. BLOCKCHAIN ET DROIT DES TITRES

Si, comme évoqué au sein de la section ci-dessus relative aux tokens, la DLT est susceptible de modifier le concept juridique de titre financier en lui-même, elle pourrait également influencer le régime juridique de la représentation des titres financiers.

Les développements qui suivent concernent plus spécifiquement les titres non cotés, et non les parts et action d'OPC qui obéissent par ailleurs à un régime spécifique, comme cela a été examiné plus haut.

La pratique de la conservation / tenue de compte de titres distingue schématiquement les systèmes de détention directe et les systèmes de détention indirecte ou multi-intermédiés de titres. De la même manière, le principe de l'inscription en compte des titres constitue le mode de fonctionnement usuel dans les marchés financier, que ce soit dans les systèmes de détention directe ou indirecte, même si dans certains pays les titres sont toujours matérialisés ou représentés sous forme d'un certificat global. Ainsi, en matière de circulation de titres comme en matière de preuve de la détention du droit sur les titres, l'inscription en compte au nom du titulaire (qu'il s'agisse du propriétaire ou d'un intermédiaire dans le cas d'une chaine de détention) joue un rôle central dans les droits du titulaire. Toute la difficulté lors du recours à un DLT vient du fait que les notions de registre central ou de comptes ne sont plus pertinentes. Comment alors assurer l'opposabilité des droits dans une DLT ? En fait, tout dépend du rôle de la DLT. Si celle-ci ne constitue que le reflet des inscriptions en compte, il ne s'agit alors que d'une technologie sans influence sur le régime juridique des titres ; si au contraire l'ensemble des titres émis par un émetteur est versé dans une DLT et que les achats et les ventes de ces titres ne peuvent plus s'effectuer que via cette DLT, celle-ci prend alors une autre dimension.

C'est en ce sens qu'il convient d'abord d'examiner dans quelle condition des titres peuvent circuler dans une DLT au regard du droit européen, et notamment le Règlement relatif aux dépositaires centraux de titres (« **CSDR** »)[70].

DLT et Dépositaires centraux de titres :

L'admission d'un titre financier aux opérations d'un DCT, ou sa livraison dans un système de règlement et de livraison d'instruments financiers, résulte soit d'une contrainte réglementaire, soit du choix de l'émetteur ou du propriétaire du titre financier.

Tout d'abord, certains titres financiers sont obligatoirement admis aux opérations d'un DCT en vertu du droit européen. L'article 3(2) du Règlement CSDR prévoit que :

« *Lorsqu'une transaction sur* ***valeurs mobilières*** *a lieu sur une plate-forme de négociation, les titres concernés sont inscrits en compte auprès d'un DCT à la date de règlement convenue ou avant cette date, s'ils ne l'étaient pas déjà.*

« Lorsque des valeurs mobilières sont transférées à la suite d'un contrat de garantie financière au sens de l'article 2, paragraphe 1, point a), de la directive 2002/47/CE, elles sont inscrites en compte auprès d'un DCT à la date de règlement convenue ou avant cette date, si elles ne l'étaient pas déjà. »

[70] Règlement 909/2014 du Parlement européen et du Conseil du 23 juillet 2014 relatif aux dépositaires centraux de titres.

Le règlement CSDR se fonde sur la définition de « *valeurs mobilières* » utilisée dans la directive MIF2[71], qui couvre « *les catégories de titres négociables sur le marché des capitaux* » dont une liste non limitative est donnée par la directive, incluant notamment les actions de sociétés, les obligations et autres titres de créance. Cependant, la section C de l'annexe I de la directive MIF2 distingue clairement, parmi les catégories d'instruments financiers, les valeurs mobilières des instruments du marché monétaire et des parts ou actions d'organismes de placement collectif.

Ensuite, certains titres financiers sont obligatoirement admis aux opérations d'un DCT. La loi française ne restreint pas ce périmètre. En effet, l'article L.211-7 du code monétaire et financier n'oblige pas l'inscription en compte auprès d'un DCT et laisse le choix à l'émetteur de réaliser la tenue de compte conservation.

En droit français, les instruments financiers sont définis comme des titres et des contrats :

> « *II. - Les titres financiers sont :*
>
> *1. Les titres de capital émis par les sociétés par actions ;*
>
> *2. Les titres de créance ;*
>
> *3. Les parts ou actions d'organismes de placement collectif.*
>
> *III. - Les contrats financiers, également dénommés "instruments financiers à terme", sont les contrats à terme qui figurent sur une liste fixée par décret.*
>
> *IV. - Les effets de commerce et les bons de caisse ne sont pas des instruments financiers »*[72].

Dans cette définition, il convient donc de distinguer les instruments financiers sous forme de titres – les actions et titres de capital mais aussi les obligations et les titres de créances – de ceux sous forme de contrats financiers – les swaps, options et autres contrats à terme. Seule la catégorie des titres a été étudiée dans le cadre du présent Rapport.

Dématérialisés depuis 1984, les instruments financiers sous forme de titre ne sont plus représentés que par une inscription en compte. Ce concept d'inscription en compte a fait depuis lors florès puisqu'il est considéré au niveau international comme la *summa divisio* en matière de titres, pour les différencier avec les instruments financiers qui restent représenter sous forme papier ou de certificats.

[71] Directive n° 2014/65 /UE du Parlement et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE.
[72] Article L. 211-1 du Code monétaire et financier

Le droit français distingue les titres nominatifs et les titres aux porteurs, les premiers étant inscrits en compte chez l'émetteur alors que les seconds sont inscrits en compte chez un intermédiaire financier habilité.

Comme on le voit, la notion de compte et celle de tenue de compte sont centrales dans la conception française du droit des titres. Au point d'ailleurs de lier le transfert de propriété à l'inscription en compte : selon l'article L. 211-17 du Code monétaire et financier, « *Le transfert de propriété de titres financiers résulte de l'inscription de ces titres au compte-titres de l'acquéreur* ».

Cette notion de propriété comme droit absolu de l'investisseur vis-à-vis de l'émetteur de l'instrument financier est une pierre angulaire de la conception française du droit des titres. Celle-ci peut être résumée autour de trois principes :

- Droit de propriété sur les titres inscrits en compte : la personne inscrite en compte est le seul propriétaire des titres et en tout état de cause, elle dispose d'un droit exclusif sur les titres inscrits dans le compte ouvert à son nom. Aucune revendication concurrente ne peut intervenir. Bien que ces titres soient fongibles, le teneur de compte n'est à aucun niveau de la chaine de détention le propriétaire de ces titres. En cas de clôture du compte, il doit restituer les mêmes titres pour la même quantité ;

- Unicité du compte-titres du propriétaire : il n'y a qu'un seul compte qui fait foi, c'est-à-dire qui atteste de la propriété des titres exclusivement en faveur de la personne titulaire du compte, que ce soit chez l'intermédiaire teneur de compte, ou chez l'émetteur. Les autres comptes sont des comptes miroirs, que ce soit dans la chaîne d'intermédiation ou chez le dépositaire central ;

- Comptabilité titres tenue par débit-crédit : tout transfert de propriété des titres doit se traduire par un débit et un crédit sur deux comptes différents.

Le problème avec la DLT consiste en ce que celle-ci ne connait pas de *compte* : suite d'écritures dans un registre décentralisé, cette technologie ne fonctionne pas par un débit d'un compte et crédit d'un autre compte, mais comme une suite de transactions.

C'est en ce sens que cette technologie vient potentiellement modifier le monde du droit des titres, non seulement en France mais dans tous les pays qui utilisent le concept ou la notion de *book entry securities*. Au point d'ailleurs que deux conventions internationales relatives au droit des titres mettent au cœur de leur objectif ce concept :

- la convention de La Haye du 5 juillet 2006 relative à la loi applicable à certains droits sur des titres détenus auprès d'un intermédiaire ; et

- la convention de Genève du 9 octobre 20009 d'Unidroit sur règles matérielles relatives aux titres intermédiés.

En droit positif français, la représentation des titres financiers s'effectue au moyen de leur inscription en compte au nom de leur propriétaire.

Ainsi que le prévoit l'article L.211-3 du code monétaire et financier, « *les titres financiers, émis en territoire français et soumis à la législation française, sont inscrits dans un compte-titres tenu soit par l'émetteur, soit par l'un des intermédiaires mentionnés aux 2° à 7° de l'article L.542-1* ».

L'article L.211-4 dispose quant à lui que cette inscription est effectuée « *au nom d'un ou plusieurs titulaires, propriétaires des titres financiers qui y sont inscrits* », sous réserves de dérogations (intermédiaires inscrits notamment).

L'article L.211-8 du code monétaire et financier permet au teneur de compte-conservateur de titres financiers de déléguer ses tâches à un tiers.

Régime actuel de représentation et de transmission de titres non cotés :

Le système de représentation et de transmission de titres financiers non cotés (*i.e.*, non admis aux opérations d'un dépositaire central ou livrés dans un système de règlement et de livraison d'instruments financiers) fonctionne en pratique selon le schéma suivant.

Premièrement, une société non cotée dispose d'un livre intitulé « Registre de Mouvement de Titres » dans lequel sont retranscrites toutes les opérations relatives aux titres de la société concernée (émissions, augmentations de capital, cessions, nantissements etc.). Il s'agit d'une sorte de « livre journal », traditionnellement coté et paraphé par le greffe du Tribunal de commerce auprès duquel la société est immatriculée, sans que cela constitue une condition formelle de validité[73]. Deuxièmement, une société non cotée tient un compte « émission » qui retrace l'ensemble des émissions de titres de la société et le volume des titres émis par celle-ci ; ce compte, structurellement débiteur, n'est mouvementé qu'à l'occasion d'opérations sur le capital et représente toujours le total des titres émis. Enfin, en parallèle, conformément aux articles L. 211-3 et suivants du Code monétaire et financier, la société ou son mandataire désigné (dont la dénomination et l'adresse doivent être publiés au Bulletin des annonces légales obligatoires conformément à l'article R. 211-3 du Code monétaire et financier) doit tenir des « comptes d'inscription » ou « comptes de titulaires » au nom de chacun des actionnaires dans lesquels sont inscrits des titres financiers dont ils sont propriétaires[74].

[73] Cf. Question écrite n° 01986 de M. Lucien Neuwirth (Loire - RPR) publiée dans le JO Sénat du 10/07/1986 - page 951

[74] Conformément à l'article L. 212-3 I du Code monétaire et financier, les actions émises sur le territoire national et soumises à la législation française qui ne sont pas admises aux négociations sur un marché réglementé doivent en principe revêtir la forme nominative (sauf exception applicables à certains véhicules d'investissement).

Sur le plan juridique, les comptes de titulaires sont les « comptes-titres » visés à l'article L. 211-3 du Code monétaire et financier. Ces comptes-titres sont fondamentaux en matière d'enregistrement des titres, de vérification des droits de propriété et de constatation des opérations de transfert de propriété. En effet, l'article R. 211-1 du Code monétaire et financier précise que « *les titres financiers ne sont matérialisés que par une inscription au compte de leur propriétaire* ». C'est donc l'inscription en compte qui matérialise le titre et établit le droit de propriété de l'actionnaire sur celui-ci. En outre, l'article L. 211-17 alinéa 1er du Code monétaire et financier précise que le transfert de propriété de titres financiers résulte de l'inscription de ces titres dans le compte-titres de leur acquéreur, ces transferts étant opérés par virement d'un compte d'actionnaire à un autre (article L. 211-15 du Code monétaire et financier). S'agissant des titres financiers non cotés[75], le Code de commerce précise également que l'inscription en compte de l'acheteur est faite à la date fixée par l'accord des parties et notifiée à la société émettrice[76].
En conséquence, l'inscription en compte constitue également l'élément clé pour constater l'existence et la propriété des titres financiers non cotés et les opérations de transfert de propriété portant sur ces titres (ces dernières pouvant également être attestées par le registre de mouvement de titres).

En pratique, les transferts de propriété de titres non cotés sont aujourd'hui réalisés au moyen d'ordres de mouvements de titres (« **ODM** ») signés par le cédant[77] au vu desquels la société émettrice constate l'opération intervenue[78], l'enregistre dans son registre de mouvement de titres[79] puis procède enfin au virement des titres du compte-titre du cédant vers celui du cessionnaire[80].

Les ODM ne sont soumis à aucun formalisme particulier pour les transferts de titres financiers non cotés. Néanmoins en pratique, les ODM sont établis sur le modèle d'ordre annexé à la norme Afnor NF K 12-500. Ils précisent notamment la nature des titres objet de la cession (actions de capital, actions de jouissance, obligations convertibles etc.), le montant nominal des titres[81], les modalités de l'opération (inscription en compte, transfert, remboursement, mutation, donation attribution, souscription, affectation en nantissement etc.)

Toujours sur le plan pratique, les comptes-titres des actionnaires sont généralement établis sous forme de feuillets individuels (établis en général sur une seule face) réservés à un titulaire de titres à raison de sa propriété ou à plusieurs titulaires à raison de leur copropriété, de leur bail, de leur nue-propriété ou de leur usufruit sur ces titres.

---

[75] L'article L. 228-1 du Code de commerce précise que les valeurs mobilières sont des titres financiers au sens de l'article L. 211-1 du code monétaire et financier, qui confèrent des droits identiques par catégorie.
[76] Article R. 228-10 du Code de commerce.
[77] L'obligation de signature incombe au seul cédant qui exécute par cette signature son obligation de délivrer les actions cédées. Cette obligation a été confirmée par un arrêt de la Chambre commerciale de la Cour de cassation le 24 mai 2011 (Cass. com., 24 mai 2011, n° 10-12163).
[78] Article R. 228-8 du Code de commerce s'agissant des valeurs mobilières.
[79] Quant aux indications à porter sur le registre, cf. article R. 228-10 du Code de commerce et article 4.2 du cahier des charges CFONB précité.
[80] Quant aux indications à porter sur les comptes de titulaires, cf. article 4.3 du cahier des charges CFONB précité.
[81] Pour les obligations sont également ajoutées les informations suivantes : l'année d'émission et le taux d'intérêt applicable.

Pour chacune des opérations de transfert de titres financiers, sur la base des ODM qui lui sont transmis[82], la société émettrice inscrit dans le registre de mouvement de titres par ordre chronologique : (i) la date de l'opération de transfert de propriété, (ii) les noms, prénoms et domicile de l'ancien et du nouveau titulaire des titres (ou la dénomination sociale, le numéro d'identification et le siège social pour les personnes morales), étant précisé que le nom de l'ancien titulaire des titres peut être remplacé par un numéro d'ordre permettant de retrouver ce nom dans les registres, (iii) la valeur nominale et le nombre de titres transférés (toutefois, lorsque ces titres sont des actions, le capital social et le nombre de titres représentés par l'ensemble des actions de la même catégorie peuvent être indiqués en lieu et place de leur valeur nominale), (iv) le cas échéant, si la société a émis des actions de différentes catégories et qu'il n'est tenu qu'un seul compte d'actions nominatives par actionnaire, la catégorie et les caractéristiques des actions transférées et (v) le numéro d'ordre affecté à l'opération[83].

Des particularités s'appliquent également concernant les nantissements de titres non cotés. En effet, pour les opérations de nantissement, il convient d'indiquer le nom du titulaire des actions avec la mention « *Titres nantis au profit de* (identité de la personne concernée) ».

Le défaut de tenue du registre des mouvements de titres d'une société non cotée et des comptes d'actionnaires n'est pas sanctionné par les textes. Néanmoins, au regard des textes susmentionnés, le défaut d'inscription en compte des titres financiers et d'inscription des virements de compte à des comptes matérialisant les opérations de transfert de ces mêmes titres poseraient des problèmes majeurs pour constater les droits des actionnaires, et le cas échéant, serait source de responsabilité civile de l'émetteur, notamment vis-à-vis de l'acquéreur.

Au regard de ces éléments, s'il existe bien trois niveaux d'enregistrement des titres et/ou des opérations sur les titres émis par une société non cotée, ce sont en réalité uniquement les comptes-titres dans lesquels figurent les inscriptions qui « représentent » les titres financiers et qui permettent de constater les droits de propriété des titulaires des comptes.

Fonctions d'une DLT :

Dans ce contexte, trois fonctions peuvent être dévolues au DLT.

- Technologie alternative à la tenue des compte-titres : les titres financiers continueraient d'être inscrits dans un compte-titre ouvert au nom du propriétaire des titres, et le DLT serait utilisé ou bien comme substitut aux technologies traditionnelles de tenue des compte-titres (c'est-à-dire qu'opérationnellement, les compte-titres seraient inclus dans le DLT) ou bien comme complément aux technologies de tenue des comptes-titres (c'est-à-dire

[82] Il est considéré que par sa signature de l'ordre de mouvement, le cédant donne pour instruction à la société émettrice de débiter son compte d'actionnaire et corrélativement de créditer celui du cessionnaire pour le nombre de de titres inscrits dans cet ordre de mouvement.

[83] Article R. 228-9 du Code de commerce s'agissant des valeurs mobilières et article 4.2 du cahier des charges CFONB précité.

qu'opérationnellement, le DLT et les compte-titres seraient distincts, le DLT servant essentiellement aux réconciliations entre compte-titres et à la transmission des titres – cf. partie suivante). Le cas échéant, les enregistrements dans le DLT pourraient être utilisés en cas de défaillance du teneur de compte pour déterminer combien de titres financiers doivent être restitués aux titulaires de comptes, à l'instar des comptes tenus par un DCT en vertu de l'article L.211-10 du code monétaire et financier.

- Preuve de la propriété des titres : les titres financiers continueraient d'être inscrits dans un compte-titre ouvert au nom du propriétaire des titres, mais l'inscription dans le DLT pourrait avoir force de preuve.

- les titres financiers seraient représentés par une inscription dans le DLT, soit parce que les inscriptions dans le DLT seraient considérées comme des inscriptions dans un compte-titre, soit parce que la loi le prévoirait explicitement.

Les réponses à la consultation de Place lancée par le Trésor au cours du Printemps 2017 ont semblé indiquer que les praticiens souhaitaient voir l'utilisation des DLT dans cette troisième option. Dans un tel cas, il faudra donc s'assurer que les inscriptions dans la DLT auront les mêmes effets que celles d'une inscription en compte auprès d'un intermédiaire ou de l'émetteur.

L'une des solutions consisterait alors à assimiler juridiquement les inscriptions dans une DLT à des inscriptions en compte.

B. BLOCKCHAIN ET DROIT DE LA PROPRIETE INTELLECTUELLE ET BREVET

Quels sont les différents éléments composant la blockchain, et qui en sont les auteurs ? Ces auteurs peuvent-ils revendiquer des droits sur leurs créations ? Comment ces droits se matérialisent-ils en pratique ? L'objet du présent paragraphe est de déterminer si le droit de la propriété intellectuelle français est adapté pour répondre à ces questions portant sur cette technologie nouvelle.

1. Les composants et les auteurs de la blockchain

Afin d'apprécier la DLT sous l'angle de la propriété intellectuelle, il est nécessaire d'en déterminer les différentes composantes, et de tenter d'en identifier les auteurs.

1.1. Les éléments composant la blockchain

Les codes sources du logiciel

La DLT n'est autre qu'une série de logiciels rendant possible les applications les plus diverses. L'exemple le plus parlant est celui des *smart contracts*, ces programmes autonomes qui, une fois démarrés, exécutent automatiquement des conditions définies au préalable et inscrites dans la blockchain. Les logiciels composant la blockchain sont constitués à l'aide de codes, appelés "*codes sources*". Le code source d'un logiciel est la forme utilisée par le programmeur pour écrire et modifier son programme. Il s'agit du programme exprimé dans un langage évolué qui permet au professionnel de l'informatique de le comprendre, de le reproduire ou de le modifier. Ce code source, appelé aussi "*prose*" est ensuite traduit en langage informatique, lisible et exécutable par un ordinateur : c'est le *code objet*. Ces codes – représentant les éléments centraux de la DLT – sont parfaitement identifiables et matérialisables, et peuvent ainsi faire l'objet d'une protection au titre du droit d'auteur octroyé à leur(s) concepteur(s), sous réserve du respect de certaines conditions que nous verrons, supra.

L'historique de la blockchain, ou « datas »

Les *datas* de la blockchain représente l'historique de tous les mouvements, toutes les transactions intervenues sur ce réseau global. L'ensemble de ces données est automatiquement et définitivement conservé dans la chaine de blocs sous forme de lignes de codes. Nous remarquerons que la législation actuelle relative à la propriété des bases de données devrait être appliquée à ces *datas*, composant essentiel de la blockchain.

Les actifs numériques, ou « tokens »

Les « tokens » sont des actifs numériques détenus par les utilisateurs de la blockchain dont le fonctionnement et les caractéristiques sont détaillés plus amplement ci-dessus.

L'interface graphique des logiciels et sites blockchain

Comme tout site ou logiciel disponible sur internet ou plus généralement sur un support numérique, l'apparence visuelle (ou *interface graphique*) de l'ensemble des sites matérialisant la DLT font partie intégrante de cette dernière. A ce titre, nous verrons que l'effort créatif des concepteurs de ces interfaces numériques peut faire l'objet d'une protection au titre du droit d'auteur.

1.2. Les auteurs de la blockchain

Blockchain publique, blockchain privée : développeurs web, codeurs, graphistes, mineurs

Qu'elles soient publiques ou privées, les blockchains restent des logiciels, des programmes informatiques dont les concepteurs, personnes physiques ou morales, sont identifiables. Ainsi, il semble que le caractère public ou privé d'une blockchain ne doive pas influer sur la propriété des codes sources, des codes objets, des interfaces graphiques etc. composant les différentes blockchains. Celles-ci sont, en tout état de cause, conçues par des développeurs web, codeurs et autres graphistes. En même temps, les gouvernances de l'une ou de l'autre rencontrant différentes tendances, on verra se dessiner des propriétés différentes, fruit non pas de l'application de la règlementation mais de la volonté des auteurs des blockchains privées versus des auteurs des blockchains publiques. Les mineurs, contributeurs rémunérés ou non pour gérer le réseau blockchain, ne sont pas générateurs de propriété intellectuelle si leur rôle se limite à exécuter et non à créer ou améliorer le code ou l'interface.

La blockchain, auteur de la blockchain : l'intelligence artificielle

Au sein de la technologie blockchain, des logiciels ainsi que des données peuvent être générées automatiquement par des logiciels existants, eux-mêmes conçus par des développeurs.

Me Benssoussan, avocat spécialiste du droit des technologies avancées, distingue deux situations : lorsque la réalisation d'une œuvre est rendue possible par une assistance robotique, alors le processus créatif est laissé à la personne physique, qui est considérée comme l'auteur de l'œuvre originale. En revanche, Me Benssoussan souligne qu'« *en l'état actuel du droit positif, seule une personne physique peut être auteur* », excluant ainsi les « *œuvres autonomes réalisées par un robot seul* »[84].

Ainsi, selon Me Benssoussan, les œuvres autonomes créées par des logiciels blockchain eux-mêmes ne sont pas susceptibles de protection. Ce constat est à rapprocher d'un cas célèbre aux Etats-Unis, à l'occasion duquel les juges d'un tribunal californien avaient refusé de reconnaitre des droits d'auteur à un singe ayant lui-même pris des autoportraits[85].

2. La blockchain, une propriété « commune » envisageable en cas de blockchain publique

2.1. Blockchain publique et blockchain privée : une distinction inopérante

[84] « Le robot créateur peut-il être protégé par le droit d'auteur » – Alain Benssoussan – Planète Robot n°42 : https://www.alain-bensoussan.com/wp-content/uploads/2016/12/34125221.pdf

[85] Northern District of California, Naruto V. Slater, 28.01.2016

Qui est propriétaire de la blockchain ? Certains auteurs, tels que Primavera de Filipi, chercheuse au CERSA, et Benjamin Jean, spécialiste de l'Open Source et président de l'association *Open Law, le droit ouvert*, estiment par exemple que les smart contracts, en tant que développement logiciel, « *peuvent être qualifiés d'œuvres soumises aux droits d'auteur dès lors que la contribution de leur concepteur est suffisamment importante pour révéler un apport personnel* »[86]. Peu importerait donc de distinguer entre blockchain publique et blockchain privée pour déterminer si les logiciels sont, ou non, soumis au droit d'auteur.

D'autres auteurs considèrent que la réponse à la question de la propriété réside dans la distinction blockchain publique – blockchain privée. Selon Hubert de Vauplane, dans une blockchain privée, « *la technologie développée par l'organisme en charge de la gestion de la blockchain est protégée par des droits de propriété intellectuelle, même si celle-ci utilise, pour une large partie, les codes sources versés librement lors de la création de la blockchain* ».[87] Inversement, les codes sources à l'origine des blockchains publiques n'auraient pas de propriétaire, selon la théorie communautaire des biens communs[88].

L'étude de cette théorie, imaginée par Elinor Ostrom, Prix Nobel d'économie 2009 pour ses développements sur les "communs", permet d'établir que ces "communs" sont considérés comme des « *bassins de ressources communes* » et renverraient, selon Philippe Yolka, professeur de droit public, à « *un tiers secteur, entre l'Etat et le marché : à des biens (lato sensu, au sens économique), ni publics ni privés, relevant d'une exploitation et d'un usage collectif* »[89]. Dès lors, si l'on appliquait la théorie des biens communs au logiciel, l'on pourrait considérer que le créateur d'un logiciel qui décide de laisser la possibilité à toute personne d'utiliser le logiciel, de le copier, l'étudier et même le modifier avant de le redistribuer, renoncerait à l'intégralité des droits qu'il détient sur sa création. Or, les logiciels sous licence libre, ou logiciels libres, peuvent être définis comme des logiciels « *protégés par le droit d'auteur et (qui) peuvent, généralement à titre gratuit, mais parfois aussi à titre onéreux, être exécutés, étudiés, diffusés et modifiés selon les termes d'une licence* »[90].

Ainsi, les logiciels, même ceux mis à disposition par leurs auteurs sous licence libre, ne s'affranchissent pas des règles relatives au droit d'auteur. Il est nécessaire de distinguer les logiciels sous licence libre de ceux relevant du domaine public. Alors que les premiers disposent d'un droit d'auteur et accordent une licence accordant certains droits aux utilisateurs par le biais de la licence choisie et ce sans avoir à passer par un accord spécifique avec chaque utilisateur, un « *programme du domaine public est un programme sur lequel son auteur a délibérément*

[86] « *Les smarts contracts, les nouveaux contrats augmentés ?* » - La revue de l'ACE – septembre 2016, n°137 – Primavera de Filipi et Benjamin Jean

[87] « *La Blockchain et la loi* » - La finance décryptée par le Droit - Hubert de Vauplane – 14 février 2016

[88] Voir note 5

[89] *« Prendre les « communs » au sérieux* » – Philippe Yolka – AJDA 2016. 1

[90] *Ch. Caron, Les licences de logiciels dits "libres" à l'épreuve du droit d'auteur français : D. 2003, p. 1556*

choisi de ne pas faire valoir ses droits »[91]. Ainsi, selon Bruce Perens, co-fondateur de l'Open Source Initiative, « *on ne peut pas vraiment dire qu'* [un programme du domaine public] *est assorti d'une licence ; quiconque peut l'utiliser comme bon lui semble, car quiconque peut le traiter comme s'il lui appartenait. On peut même assujettir un programme du domaine public à une nouvelle licence, en ôtant cette version modifiée du domaine public, ou en ôter le nom de l'auteur et traiter le programme comme son propre travail* »[92].

2.2. Les « licences libres » sous l'angle de la propriété intellectuelle

Dans une blockchain publique, le principe est la mise à disposition du logiciel et de ses codes sources à tous, afin que l'ensemble de la communauté puisse les exploiter, les copier, les diffuser et même modifier, pour en améliorer les performances. Pour autant, cette logique libérale se heurte-elle aux principes du droit de la propriété intellectuelle, accordant des droits spécifiques aux créateurs de logiciels ? Cela n'est pas le cas, car le concept de logiciel libre permet aux concepteurs de toute œuvre de l'esprit de mettre à disposition de tous les codes sources, en en autorisant l'exploitation, la copie, la diffusion et la modification, tout en fixant un cadre légal.

Prenant l'exemple des smart contracts, Primavera de Filipi et Benjamin Jean envisagent leur mise à disposition par l'intermédiaire des licences Open Source, et en exposent les principes :

> *« On parle d'Open Source en matière de logiciel lorsqu'une licence Open Source (c'est à dire répondant un certain nombre de critères de non-exclusivité définis par l'Open Source Initiative) est apposée sur un code logiciel afin d'en permettre le développement collaboratif et ouvert. Par extension, cette logique a été portée sur tout type de création potentiellement soumise à un quelconque droit de propriété intellectuelle (droit d'auteur, brevet, droit sui generis des bases de données, etc.) et s'étend à tous les aspects collaboratifs du projet (et non plus seulement la dimension juridique). […] En tant que développement logiciel, les Smart Contracts peuvent être qualifiés d'œuvres soumises au droit d'auteur dès lors que la contribution de leur concepteur est suffisamment importante pour révéler un apport personnel. »*[93]

Ainsi, le protocole blockchain d'origine et toutes ses implémentations – dont Ethereum – sont eux-mêmes sous licence GNU General Public Licence v2, une licence Open Source « à réciprocité » qui fixe un cadre juridique à l'utilisation et la modification des logiciels concernés. A ce titre, le droit de modifier et redistribuer est garanti seulement si l'utilisateur fournit le code

---

[91] La définition de l'*Open Source* - Bruce Perens, trad : Sébastien Blondeel – Essai publié dans le livre « *Open Sources — Voices from the Open Source Revolution* » *édité par Chris DiBona, Sam Ockman, et Mark Stone chez O'Reilly & Associates*

[92] Voir note 9

[93] « *Les smarts contracts, les nouveaux contrats augmentés ?* » - La revue de l'ACE – septembre 2016, n°137 – Primavera de Filipi et Benjamin Jean

source de la version modifiée du logiciel. En outre, les copies distribuées, incluant les modifications, doivent être aussi sous les termes de la « GPL »[94]. Plus largement, les logiciels Open Source donnent une latitude très large à ses utilisateurs, et sont définis par le mouvement Open Source Initiative selon huit critères, tel que l'absence de redevance en échange de l'accès au logiciel – même si l'existence d'une telle redevance n'est pas interdite, la possibilité d'accès au code source et de modification et distribution des travaux dérivés en vertu des mêmes conditions que la licence initiale, le respect de la paternité de l'auteur etc[95].

Un autre type de licence libre, la licence « *Creative Commons* » permet à l'auteur d'un logiciel de mettre son œuvre à disposition des utilisateurs en fixant des limites à son utilisation. En choisissant l'une des sept licences possibles, les auteurs peuvent accorder plus ou moins de latitudes aux utilisateurs. Par exemple, la licence « BY » attribue un droit d'exploitation commerciale de l'œuvre ainsi que sa modification par les tiers, sous réserve de citer l'auteur. La licence « BY ND », elle, n'autorise que l'exploitation sans modification. La licence « BY NC », quant à elle, autorise l'utilisation de l'œuvre originale à des fins non commerciales seulement, mais interdit la création d'œuvres dérivés[96]. Ce panel de licences offre différents niveaux de liberté accordée aux utilisateurs, ce qui permet à l'auteur du logiciel de déterminer avec précision la façon dont il en entend contrôler l'exploitation.

Alors que l'utilisation de ces licences est courante dans la blockchain publique, elle l'est moins dans les blockchains privées, dans lesquelles toute utilisation, modification ou diffusion est obligatoirement soumise à l'autorisation de l'auteur.

3. L'applicabilité du droit français de la propriété intellectuelle aux composants de la blockchain

Les grands principes du droit de la propriété intellectuelle français s'appliquent aux composants de la blockchain, identifiés précédemment, et en particulier le régime du droit d'auteur. La question de la protection par le droit des brevets, ainsi que les incertitudes relatives à la protection de certains composants de la blockchain, doivent également être envisagées.

3.1. Logiciels et interfaces graphiques : une protection assurée par le régime du droit d'auteur

Le régime général du droit d'auteur applicable aux interfaces graphiques

[94] Voir Note 11

[95] Jcl Propriété Littéraire et Artistique - Fasc.1975 : « *L'œuvre libre* » III. B. 2° – Mélanie Claire-Fontaine – 22 juillet 2014

[96] http://creativecommons.fr/licences

La blockchain est composée en particulier de logiciels et d'interfaces graphiques. Aux termes de l'article L.111-1 du Code de la propriété intellectuelle, « *L'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous.* A ce titre, l'article L.112-2 du Code de la propriété intellectuelle liste de façon non exhaustive les œuvres susceptibles de protection par le droit d'auteur, permettant à tout « créateur » d'une œuvre originale d'empêcher toute exploitation de son œuvre par les tiers. Les « *œuvres graphiques et typographiques* » ainsi que « *les logiciels, y compris le matériel de conception préparatoire* » sont par exemple susceptibles de recevoir une telle protection. Toute œuvre, qu'elle soit musicale, graphique, photographique, architecturale etc. se doit d'être originale, c'est-à-dire qu'elle « *révèle de l'effort créateur et reflète la personnalité de l'auteur* »[97].

L'interface graphique de ces logiciels se voit expressément reconnaitre le statut d'œuvre de l'esprit par les juridictions françaises et européennes, sous réserve de respecter le critère d'originalité ci-avant exposé. En matière d'interface graphique, l'originalité sera par exemple reconnue à une interface dont les « *spécifications externes, l'expression télévisuelle et l'enchaînement des fonctionnalités des logiciels de chacun des jeux concernés témoignaient d'un effort créatif portant l'empreinte de la personnalité de leurs créateurs* »[98]. Les interfaces de logiciels blockchain ne présentent à priori aucune particularité permettant de penser qu'il en sera différent.

Les dispositions spécifiques aux logiciels

En matière de logiciel, les tribunaux français estiment qu'un logiciel ne sera considéré comme original (et donc créateur de droits pour son auteur) que s'il est établi que son auteur a « *fait preuve d'un effort personnalisé allant au-delà de la simple mise en œuvre d'une logique automatique et contraignante et que la matérialisation de cet effort résidait dans une structure individualisée* »[99]. En d'autres termes, un logiciel rédigé dans un langage informatique différent de logiciels précédemment créés doit être considéré comme une œuvre originale, dès lors que ce langage a permis de le faire fonctionner avec un certain type de processeur, amélioration qui caractérise « *l'existence d'un apport intellectuel propre et d'un effort personnalisé* »[100]. Ainsi, la blockchain, composée de logiciels, tels les smart contracts, fera l'objet d'une protection permettant à leurs auteurs, les codeurs, de contrôler voire interdire toute exploitation de leur programme informatique, sous réserve d'établir le fameux « *apport intellectuel propre et effort personnalisé* ».

Les droits accordés aux auteurs d'un logiciel font l'objet de dispositions spécifiques, compte tenu des spécificités techniques de cette œuvre de l'esprit. A titre d'exemple, l'auteur d'un

[97] Cass. Com. 25 mars 1991, n°89-11204
[98] Cass. Civ.1 27 avril 2004, n° 99-18464
[99] Cour de cassation, Assemblée Plénière, 7 mars 1986 n° 83-10477
[100] Cour de cassation, 1ère chambre civile, 22 septembre 2011, n° 09-71.337

logiciel a la possibilité d'interdire « *la reproduction permanente ou provisoire d'un logiciel en tout ou partie par tout moyen et sous toute forme ».* Il a également la faculté d'empêcher « *toute traduction, adaptation, arrangement ou toute autre modification de son œuvre, ainsi que la reproduction en résultant.* »[101] Le droit moral de l'auteur d'un logiciel est quant à lui limité, étant donné que le droit de retrait ou de repentir, permettant à l'auteur de toute œuvre de retirer son autorisation à l'exploitation, est exclu en matière de logiciel[102]. Le droit à l'intégrité de l'œuvre, autre composante du droit moral, est quant à lui limité. L'auteur d'un logiciel ne pourra s'opposer à la modification de « son » logiciel par le cessionnaire des droits patrimoniaux, sous réserve de la préservation de son honneur et sa réputation[103].

Enfin, les tokens ne sont autres que des logiciels composés d'un code source et d'un code objet. Ainsi, il conviendrait d'appliquer les dispositions ci-dessus exposées. Si la propriété matérielle de ces actifs resterait la propriété de leur porteur, leur code source ainsi que le code source des logiciels permettant de créer des tokens seraient, au même titre que n'importe quel logiciel, la propriété de son créateur, le programmateur à l'origine de la création du token.

L'application des dispositions relatives au partage des droits en cas de pluralité d'auteurs

Le droit français prévoit différents niveaux de protection en fonction du rôle de chaque participant à la conception du logiciel. L'œuvre collective accorde des droits au seul initiateur du logiciel. Est dite collective l'œuvre créée par plusieurs personnes à l'initiative d'une seule personne, physique ou morale, qui va coordonner la création et éditer l'œuvre sous son nom. Cette personne sera seule titulaire des droits moraux et patrimoniaux sur l'œuvre[104]. En pratique, une œuvre sera dite collective si les contributeurs collaborent à la réalisation du logiciel sans participer à la conception d'ensemble[105].

L'œuvre de collaboration, quant à elle, accorde des droits égaux à tous les concepteurs. En effet, une œuvre dite de collaboration est « *l'œuvre à la création de laquelle ont concouru plusieurs personnes physiques ».*[106] En pratique, un logiciel est dit de collaboration lorsque ses auteurs ont agi en se concertant, dans un dessein commun et ce, sur un pied suffisant d'égalité[107]. Le code de la propriété intellectuelle précise à l'article L.113-3 que « *l'œuvre de collaboration est la propriété commune des coauteurs. Les coauteurs doivent exercer leurs droits d'un commun accord*. » L'œuvre peut donc être bloquée dans son exploitation, si le nombre d'auteurs concerné est trop important, ce qui est courant dans le monde du logiciel.

---

[101] Article L.122-6 du code de la propriété intellectuelle

[102] Article L. 121-7 du Code de la propriété intellectuelle

[103] Voir note 19

[104] Articles L.113-2 et L.113-5 du Code de la propriété intellectuelle

[105] « *Droit d'auteur des chercheurs, Logiciels, Bases de Données et Archives Ouvertes* », 5.4, Martin DANTANT– CNRS, Direction des affaires juridiques, 7 juillet 2014

[106] Article L.113-2 du Code de la propriété intellectuelle

[107] CA Paris, pôle 5, 1re ch., 27 févr. 2013, n° 11/11785 : Propr. intell. 2013, n° 47, p. 188, obs. A. Lucas

L'œuvre composite ou dérivée, enfin, reconnait des droits aux concepteurs successifs d'un logiciel. L'œuvre dérivée est « *l'œuvre nouvelle dans laquelle est incorporée une œuvre préexistante sans la collaboration de l'auteur de cette dernière* ».[108] Il peut s'agir notamment des cas où un morceau de code source déjà existant est incorporé dans un nouveau logiciel. Le créateur des nouveaux apports originaux sera titulaire des droits mais devra respecter les droits de l'auteur de l'œuvre antérieure.

Dans une blockchain privée, toute personne souhaitant améliorer un logiciel préexistant et soumis strictement au droit d'auteur, devra donc obtenir l'autorisation de l'auteur de l'œuvre antérieure. Dans une blockchain publique, en revanche, la tendance à développer sous licence libre apporte moins de contraintes juridiques à de nouveaux développements, encore cela dépend-il de la licence qui a été choisie par l'auteur – celui-ci, en particulier, pourra autoriser ou non les nouveaux développements et/ou exploitations commerciales. Ainsi, tout dépend finalement des autorisations accordées par la licence sous laquelle est placé le logiciel.

La propriété des données

A qui appartiennent les données (*datas*), constituant l'historique de toutes les transactions effectuées sur la blockchain ? Les bases de données, définies par l'article L.112 dudit code comme « *un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen* », permettent à leurs auteurs d'interdire l'extraction ou la réutilisation de la base qu'il a créée. Les bases de données intégrées à une blockchain pourraient donc appartenir aux personnes à l'origine du stockage de données sous forme de blocs. Les données, quant à elles, appartiendraient aux personnes concernées par ces données. C'est le cas des données dites « personnelles », permettant d'identifier directement ou indirectement une personne physique. Ces données « *relèvent d'un droit fondamental, le droit à la vie privée, lequel ne peut être cédé* »[109].

3.2. Une possible protection des logiciels par l'intermédiaire du droit des brevets

En France, « *sont brevetables, dans tous les domaines technologiques, les inventions nouvelles impliquant une activité inventive et susceptibles d'application industrielle* ».[110] La protection accordée par le brevet est potentiellement beaucoup plus puissante que celle prévue par le droit d'auteur. Alors que l'existence de ce dernier ne résulte pas d'un dépôt "officiel", et

[108] Article L.113-2 du Code de la propriété intellectuelle
[109] *« A qui appartiennent nos données ? »* - 26 novembre 2014 : http://www.cil.cnrs.fr/CIL/spip.php?article2611
[110] Article L.611-10 al. 1 du Code de la propriété intellectuelle

est donc soumis de l'appréciation incertaine et imprévisible des juges du fonds, l'existence même d'un brevet entraine des droits surs et plus difficilement contestables auprès d'un juge. Si le droit français considère que les programmes d'ordinateur et logiciels, « *en tant que tels, ne sont pas considérés comme des inventions brevetables* »[111], ils peuvent tout de même faire l'objet d'un brevet « *si l'objet revendiqué présente un caractère technique* »[112]. Ainsi, l'Institut National de la Propriété Industrielle (**INPI**) précise que « *si un programme d'ordinateur est capable de produire, lorsqu'il est mis en œuvre sur un ordinateur, un effet technique supplémentaire allant au-delà de ces effets techniques normaux consistant à faire fonctionner l'ordinateur, il n'est pas exclu de la brevetabilité.* » A titre d'exemple, « *lorsqu'on s'intéresse à la question de la diminution de la consommation en énergie d'une voiture ou encore, à l'augmentation de la vitesse de transmission des informations sur un processeur électronique, on se trouve face à un problème d'ordre technique. Répondre concrètement à ces questions, c'est apporter une solution technique à des problèmes techniques* »[113].

Ainsi, les logiciels blockchain répondant aux critères précités pourraient faire l'objet, en France, d'une protection par le droit des brevets. Aux Etats-Unis l'USPTO, l'office américain des marques et des brevets, recensait à priori 71 demandes de brevets relatifs à la blockchain et aux crypto monnaies en 2012. Ce chiffre serait passé à 469 en 2016[114].

3.3. Les incertitudes relatives à la protection des algorithmes et la protection par le secret des affaires

Certains composants de la blockchain ne sont pas protégeables, ni par le droit d'auteur, ni par celui des brevets. A titre d'exemple, l'algorithme, dont la définition « Larousse » est reprise par l'INPI, se dit d'un « *ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations. Un algorithme peut être traduit, grâce à un langage de programmation, en un programme exécutable par un ordinateur* »[115].

Aussi, les algorithmes seuls, en tant de principes mathématiques, font partie du domaine des idées et sont donc, comme le veut l'adage, de "libre parcours"[116]. Ceci étant dit, les algorithmes intégrés à des logiciels originaux pourront faire l'objet d'une protection, en tant que partie intégrante d'une œuvre originale. Toutefois, dès lors qu'un tiers parviendra à extraire

---

[111] Article L.611-10 du Code de la propriété intellectuelle

[112] INPI – Procédure de délivrance – Directives brevets et certificats d'utilité – Mai 2016 : https://www.inpi.fr/sites/default/files/inpi_dir_brevets_delivrance_20160601.pdf

[113] Jcl Brevets - Fasc.4221: « *La protection des logiciels par brevet d'invention* » point 28 – Sébastien Drillon – 3 février 2017

[114] https://cointelegraph.com/news/blockchain-patent-applications-almost-double-in-q1-2017-uspto-data

[115] « *La propriété intellectuelle et la transformation numérique de l'économie* » - Marc Schuler et Benjamin Znaty - https://www.inpi.fr/sites/default/files/1_3_extrait_pi_et_transformation_economie_numerique_inpi.pdf

[116] Voir note 30

légalement l'algorithme d'un logiciel, et quand bien même ce logiciel serait protégé par le droit d'auteur, il sera libre de réutiliser cet algorithme qui, seul, ne serait pas protégeable[117].

Dans ces conditions, comment protéger ces algorithmes ? L'analyse d'Hubert de Vauplane à ce sujet mérite d'être soulignée : *« Cette question de la propriété ou du contrôle des codes sources résonne de manière particulière dans l'industrie financière : il s'agit de la question de la protection des algorithmes utilisés dans certaines transactions financières et développés par des experts (les « quants ») dans la mesure où la plupart de ces algorithmes ne peuvent être protégés par des brevets ou droits d'auteur ; dès lors, ces algorithmes sont gardés secrets. Ce qui n'est possible que dans une blockchain privée où les développements spécifiques apportés par l'éditeur ne sont pas toujours juridiquement protégés mais dans ce cas, ils ne sont pas ouverts, pas même aux participants de la chaine privée »*[118].

Ainsi, d'un point de vue pratique, la distinction entre blockchains publiques et blockchains privées pourrait avoir un impact sur les droits de propriété intellectuelle : seuls les concepteurs de blockchains privés pouvant utiliser la protection apportée par le secret, pour les éléments délaissés par le droit d'auteur.

En conclusion, l'étude des différentes composantes de la blockchain amène à considérer que le droit de la propriété intellectuelle en France est suffisamment développé pour réglementer les différentes composantes de la blockchain, à la fois dans ses éléments et ses auteurs.

C. BLOCKCHAIN ET PROTECTION DES DONNEES PERSONNELLES

La blockchain étant définie comme un registre d'opérations infalsifiable, distribué, vérifiable par tous et reposant sur un consensus, il en résulte que les opérations enregistrées dans une blockchain ont vocation à être inaltérables et donc ineffaçables. S'il est possible d'annuler une opération en passant une opération opposée, il n'est pas possible d'effacer une opération.

[117] Idem

[118] « *La Blockchain et la loi* » - La finance décryptée par le Droit - Hubert de Vauplane – 14 février 2016

Or, le GDPR[119] prévoit un droit à l'effacement[120]. Il est donc légitime de s'interroger sur la compatibilité de la définition de la blockchain avec cette réglementation.

1. Données personnelles, données anonymisées et données pseudonymisées

Le GDPR s'applique aux traitements de données personnelles, celles-ci étant définies largement comme toute information se rapportant à une personne physique identifiée ou identifiable, y compris par référence à un identifiant, ou à un ou plusieurs éléments spécifiques propres à son identité. A contrario, lorsque les données sont anonymes ou anonymisées, c'est-à-dire lorsque les données ne permettent pas de réidentifier directement ou indirectement la personne concernée, le GDPR ne s'applique pas.

Le GDPR mentionne une troisième catégorie de données, les données pseudonymes[121], qui sont des données non nominatives mais qui permettent cependant l'identification indirecte d'un individu et sont donc considérées comme des données personnelles soumises aux règles du GDPR.

La blockchain utilise généralement des identifiants non nominatifs, dont l'objet est de pouvoir réidentifier les participants à une opération sans pour autant rendre publiques les données nominatives les concernant.

Quand bien même certains commentateurs mentionnent que les blockchains qui traitent des opérations entre individus sont "anonymes", il s'agit de données pseudonymes, c'est-à-dire de données personnelles qui sont soumises aux règles du GDPR.

2. Le droit à l'effacement selon le GDPR

Selon le GDPR, le droit à l'effacement est le droit dont dispose un individu de demander à ce que les données personnelles le concernant soient effacées notamment lorsque les conditions suivantes sont remplies :

---

[119] Règlement (UE) 2016/679 du parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Le RGPD étant applicable à compter du 25 mai 2018 et se substituant à la loi française n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, nous ne détaillerons pas les différences pouvant exister avec le droit à l'effacement tel que prévu par celle-ci.

[120] Voir article 17 du RGPD, intitulé « droit à l'effacement (« droit à l'oubli ») ». Si le terme « droit à l'oubli » est souvent utilisé, nous emploierons le « droit à l'effacement », dès lors qu'il apparait plus précis.

[121] Selon le RGPD, la pseudonymisation est « *le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable* ».

- les données personnelles ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ;

- la personne concernée retire son consentement au traitement et celui-ci ne peut être fondé sur une autre base juridique ; ou

- la personne concernée s'oppose au traitement sans qu'il n'existe de motif légitime impérieux pour le traitement.

Par ailleurs, quand bien même le GDPR prévoit des exceptions à l'exercice du droit à l'effacement, par exemple lorsque le traitement est nécessaire à des fins archivistiques dans l'intérêt public ou à des fins statistiques, ces exceptions ne nous paraissent pas applicables au cas des opérations entre individus enregistrées dans une blockchain.

Si la définition de la blockchain semble incompatible avec le droit à l'effacement, existe-t-il des solutions permettant de remédier à cette situation ? A défaut de modification du GDPR, deux approches peuvent être envisagées.

Tout d'abord il nous semble qu'à partir du moment où une personne concernée serait clairement et préalablement informée qu'en cas de participation à une blockchain les conditions d'exercice de son droit à l'effacement sont rendues inapplicables, et que cette renonciation est acceptée, ce droit à l'effacement pourrait devenir indisponible de manière légitime. Il serait envisageable d'informer la personne concernée du fait que :

- la finalité même d'une blockchain est la conservation des données des opérations qui y figurent de manière inaltérable dans le temps, et que par conséquent les données seront toujours nécessaires au regard des finalités pour lesquelles elles ont été collectées ;

- au-delà de l'opération qu'elle réalise, son consentement concerne la conservation inaltérable de ses données dans la blockchain, nécessaire à son fonctionnement, et que dans tous les cas l'intérêt légitime du responsable du traitement pourrait fonder ce traitement ;

- malgré son opposition au traitement, la fiabilité de la blockchain dans le temps est un motif légitime impérieux justifiant que les données ne soient pas effacées.

A contrario, nonobstant la définition précitée, une blockchain peut être modifiée par le consensus de sa communauté, notamment pour la corriger ou la faire évoluer, comme le démontrent la récente scission du Bitcoin en 2017 ou celle de The DAO en 2016. Les communautés pourraient donc décider d'organiser dans des cas limités et bien définis des procédures permettant l'exercice du droit à l'effacement, sous une forme ou une autre. En effet,

l'objectif du droit à l'effacement (ou droit à l'oubli) est de rendre une donnée personnelle inaccessible ; résultat qui peut être obtenu par l'effacement, mais aussi par exemple par l'anonymisation irréversible. Dès lors qu'il n'est plus possible d'identifier directement ou indirectement un individu à travers l'opération à laquelle il a participé, l'objectif du droit à l'effacement est atteint. Ainsi s'il n'est pas possible d'effacer une opération, il est probablement possible de la masquer ou de rendre inaccessibles les données personnelles de cette opération, de façon irréversible.

Sous réserve de la faisabilité technique d'une telle solution d'anonymisation, chacune de ces deux approches pourrait permettre de réconcilier le fonctionnement de la blockchain avec les impératifs de la protection des données personnelles.

D. BLOCKCHAIN ET SIGNATURE ELECTRONIQUE

La signature électronique est un processus qui permet principalement l'identification d'un signataire, cette identification étant garantie dans la plupart des cas grâce à l'intervention d'un tiers de confiance.

A première vue, la blockchain et la signature électronique semblent tout à fait incompatibles. Elles sont pourtant intimement liées par la technologie sur laquelle elles reposent toutes les deux : la cryptographie asymétrique (**1**). On pourra dès lors s'interroger sur la possibilité d'utiliser la technologie de la blockchain afin de développer une solution de signature électronique permettant de remplir les exigences de sécurité et de confiance de la règlementation française et européenne (**2**).

Une telle solution pourrait permettre de pallier certaines lacunes des solutions classiques de signature électronique (**3**). Cependant, cette solution présenterait également de nouvelles difficultés (**4**).

1. La cryptographie asymétrique

La blockchain et la signature électronique reposent toutes les deux sur les avancées mathématiques du siècle dernier et en particulier sur le chiffrement.

Le chiffrement, en tant que technique permettant de rendre incompréhensible un message pour celui qui ne connaît pas la clé de déchiffrement, n'est pas une création récente : il était d'ores et déjà utilisé depuis de nombreux siècles pour transmettre des messages. Cependant, l'invention au siècle dernier des ordinateurs a pu permettre, grâce à leur grande puissance de calcul, de créer des codes de chiffrement mathématique de plus en plus efficaces.

Les avancées de la technologie ont également permis de développer une nouvelle technique de chiffrement reposant sur deux clés.

Dans le chiffrement classique (le chiffrement symétrique), le message était chiffré et déchiffré grâce à une seule et même clé. Cette technique posait de grandes difficultés de transmission du code et de vulnérabilité du chiffrement lorsque ce code était connu d'un trop grand nombre de personnes.

Pour pallier ces difficultés, la cryptologie asymétrique a été développée. Cette méthode de chiffrement est basée sur l'utilisation d'une double clé de déchiffrement : une clé privée (connue uniquement de son titulaire) et une clé publique (qui peut être connue de tous). La clé publique est calculée de manière unique à partir de la clé privée. Seule la clé privée peut déchiffrer un message chiffré grâce à la clé publique qui y est associé. Ce dédoublement du code permet de limiter la transmission des clés : si une personne A veut transmettre un message confidentiel à B, elle pourra le chiffrer avec la clé publique de B (qui peut être transmise librement) et B sera le seul à pouvoir déchiffrer ce message grâce à sa clé publique.

Le contraire est également vrai : seule la clé publique associée à la clé privée peut déchiffrer un message chiffré grâce à la clé privée. Dès lors, cette méthode présente un intérêt particulier pour identifier des personnes : comme par hypothèse seul le titulaire connaît sa clé privée, le chiffrement d'un message grâce à cette clé privée permet de s'assurer que le message a bien été envoyé par la personne.

La signature électronique repose donc sur cette méthode de chiffrement asymétrique. Le signataire va en premier lieu créer un *hash* de son message c'est-à-dire un condensé cryptographique présenté comme une séquence de caractères alphanumériques de longueur fixe qui représente le contenu d'un message, sans le révéler, et dont la valeur unique est produite par un algorithme de hachage. Le signataire va ensuite utiliser sa clé privée pour signer son message. Grâce à un tel procédé, toute modification du message rendrait la signature invalide car le hash ne correspondrait plus au message.

Le destinataire du message peut ensuite déchiffrer le *hash* à l'aide de la clé publique de l'émetteur. Si les deux clés correspondent, le destinataire peut être relativement assuré de l'identité de l'émetteur et de la provenance du message.

La blockchain fonctionne également grâce à cette méthode de la cryptologie asymétrique. Lors de sa première utilisation de la blockchain, l'utilisateur va se voir attribuer une paire de clés publique et privée. Son "adresse" blockchain sera calculée à partir de sa clé publique. Lorsqu'il souhaite effectuer une transaction sur la blockchain, l'utilisateur va chiffrer le hash de son message avec sa clé privée. Les mineurs vérifient ensuite que la clé privée correspond à la clé publique qui est stockée dans la blockchain pour valider la transaction. Lorsqu'il s'agit d'une

transaction portant sur de la monnaie cryptographique, les mineurs vont ainsi s'assurer que l'émetteur possède bien les fonds nécessaires à la transaction.

2. Blockchain et règlement eIDAS

Dès lors que la blockchain est essentiellement, comme l'a décrite son créateur Satoshi Nakamoto, « *une chaine de signatures électroniques*[122] », il pourrait être envisagé de créer une blockchain permettant de signer électroniquement des documents et des contrats.

La difficulté de la création d'une telle solution tiendra alors au respect des dispositions du règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (**Règlement eIDAS**[123]) qui règlemente notamment les signatures électroniques. Le Règlement eIDAS distingue entre trois types de signatures électroniques, qui correspondent aux trois types de signatures identifiés par la directive de 1999 et par le décret français de 2001[124].

Les trois niveaux de signatures sont la signature simple, la signature avancée (correspondant à la signature sécurisée en France) et la signature qualifiée (correspondant à la signature présumée fiable en France). A chacun de ces niveaux correspond un certain nombre d'exigences qui constituent autant de contraintes potentielles pour l'utilisation de la DLT.

L'article 25 du Règlement eIDAS pose le principe de non-discrimination entre les différentes signatures électroniques sur le plan probatoire. Aux termes de cet article, toutes les signatures électroniques doivent être acceptées à titre de preuve. Il revient néanmoins à celui qui s'en prévaut de rapporter la preuve de leur fiabilité. Seule l'utilisation d'une signature qualifiée permet de renverser la charge de la preuve, et de bénéficier ainsi d'une présomption de fiabilité.

Lors de la création d'une solution de signature électronique reposant sur la blockchain, il conviendra d'évaluer la nécessité de se conformer aux dispositions très strictes relatives à la signature qualifiée au vu du risque probatoire posé par les deux autres types de signatures.

2.1. La signature simple

[122] Satoshi Nakamoto, *Bitcoin: a Peer-to-Peer Electronic Cash System*, 31 octobre 2008.

[123] Règlement 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

[124] Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.

En ce qui concerne la signature simple, il n'existe pas d'encadrement règlementaire particulier à ce jour. Toute acceptation d'un contrat en ligne – par la simple action de cocher une case d'acceptation des conditions générales de vente par exemple – est une signature électronique simple.

Ce type de signature pourra donc être mis en place sans difficulté dans une blockchain puisque c'est d'ores et déjà ce qui est utilisé aujourd'hui pour effectuer des transactions. Cependant, ce type de signature comprend un fort risque probatoire puisqu'il sera très difficile d'identifier le signataire et de démontrer la fiabilité du procédé de signature électronique.

2.2. La signature avancée

En ce qui concerne la signature avancée, quatre conditions cumulatives doivent être satisfaites.

Premièrement, la signature doit être liée au signataire de manière univoque. Ensuite, cette signature doit permettre d'identifier le signataire. Par ailleurs, la signature doit être créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif. Enfin, la signature doit être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

Les trois premières conditions de la signature avancée sont liées à la création, au stockage et à l'utilisation de la paire clé publique/clé privée délivrée au signataire.

Concernant la première condition, c'est le principe de la cryptographie asymétrique qui permettra, par le biais de sa clé publique, d'identifier le porteur de la clé privée. Puisque la clé publique correspond de manière unique à la clé privée, et que la clé privée est secrète, la paire permet de vérifier que la signature correspond de manière univoque au signataire.

La deuxième condition fait référence quant à elle à la nécessité de lier la paire clé publique et clé privée à l'identité d'une personne donnée, de telle sorte que l'on puisse s'assurer que c'est bien un individu identifié qui utilise la paire de clés en question. De manière générale, cette condition est remplie grâce à la délivrance, concomitamment à celle de la paire de clé, d'un certificat indiquant l'identité de la personne et sa clé publique. Le certificat est lui-même délivré après vérification de l'identité du signataire. Cette vérification peut être réalisée de plusieurs manières qui peuvent être plus ou moins contraignantes : envoi des documents d'identité, vérification grâce à l'envoi d'un code par SMS ou par mail, rendez-vous en face à face, etc. Plus la méthode de vérification de l'identité sera contraignante, plus la preuve de la fiabilité du certificat sera simple à rapporter.

La troisième condition revient à prouver que le signataire est seul maître de sa clé privée qui ne peut être utilisée par personne d'autre et qui ne peut être contrefaite. Nous notons cependant qu'à ce jour, aucune norme définitive n'a été adoptée pour préciser ce que constitue un *« niveau de confiance élevé de contrôle exclusif »*, ni quels sont les moyens acceptés pour identifier les signataires. A cet égard, l'Agence Nationale de la Sécurité des Systèmes d'Information (**ANSSI**) a publié un document précisant que *« les moyens mis en œuvre doivent permettre de garantir un niveau de sécurité suffisant et de pallier le risque de fraude à la signature »* [125]. L'ANSSI donne comme exemple l'utilisation d'un code PIN réservé à cet usage, qui permettrait au signataire de débloquer l'utilisation de sa clé privée, qui peut être contenue sur son terminal : ordinateur, téléphone portable, etc.

En ce qui concerne la dernière condition, celle-ci est généralement remplie en effectuant un *hash* du message avant de le signer électroniquement, ce qui assure l'intégrité dans le temps du message ainsi signé, comme détaillé ci-dessus.

Ce deuxième type de signature permet de constituer un faisceau d'indices qui pourrait permettre en cas de litige de rapporter la preuve de la signature, de sa fiabilité et de l'identité du signataire. Cette solution intermédiaire est bien souvent celle privilégiée par les entreprises. Notons néanmoins qu'il semblerait que les différents acteurs de la signature électronique (autorités de certification, éditeurs de logiciel, etc.) préfèrent utiliser, en pratique, des normes éditées par des comités européens pour la signature qualifiée, même pour les signatures avancées[126].

Ces normes prévoient notamment la délivrance d'un certificat après une rencontre physique directement avec l'autorité de certification ou un tiers, ainsi que la fourniture du certificat sur un support cryptographique matériel, par exemple une clé USB. Cela rendrait l'adoption d'un niveau avancé de signature électronique beaucoup plus contraignante sans renverser la charge de la preuve.

En ce qui concerne son implantation dans la blockchain, il conviendra d'une part de s'assurer que toutes les paires de clés utilisées dans la blockchain sont délivrées grâce au même protocole, de manière à éviter qu'une clé privée puisse correspondre à deux clés publiques délivrées par deux opérateurs différents grâce à des protocoles différents.

Par ailleurs, les conditions d'attribution des paires de clés et des certificats devraient être renforcées pour permettre de remplir les conditions listées ci-dessus. Les opérateurs devraient être en mesure de procéder à la vérification de l'identité de la personne et la paire de clés ainsi que le certificat devraient être transmis de manière sécurisée et associé à un code PIN que le signataire est le seul à connaître.

[125] ANSSI, *Règlement eIDAS – Foire aux questions*, 2 juin 2016

[126] Notamment les normes CEN (European Committee for Standardization) et ETSI (European Télécommunications Standards Institute) avec la norme ETSI EN 319 411 - 1

2.3. La signature qualifiée

En ce qui concerne la signature qualifiée, trois conditions cumulatives doivent être satisfaites.

Premièrement, la signature doit être une signature électronique avancée (et donc remplir tous les critères précités). Ensuite, la signature doit être créée à l'aide d'un dispositif de création de signature électronique qualifié[127]. Enfin, ce dispositif doit reposer sur un certificat qualifié de signature électronique[128] délivré par un prestataire de service de confiance, c'est-à-dire un prestataire agréé par une entité nationale, lequel doit notamment vérifier l'identité de la personne par un face à face[129].

Ce type de signature nécessiterait qu'un prestataire de services de confiances développe un protocole de signature électronique fonctionnant sur la blockchain. Par ailleurs, ce protocole devra respecter toutes les normes techniques posées par la Commission Européenne.

3. L'intérêt pratique d'une telle solution

La solution classique de la solution électronique peut présenter plusieurs enjeux au niveau technique et organisationnel qui pourraient être évités en utilisant une solution blockchain.

En premier lieu, une solution de signature électronique nécessite l'intervention de plusieurs acteurs : le tiers certificateur, le prestataire d'horodatage, le prestataire d'archivage et le fournisseur du logiciel de signature. Cela multiplie le risque d'erreurs et de difficultés techniques tout en diluant la responsabilité envers le client.

Or, une solution de signature électronique blockchain pourrait potentiellement nécessiter le recours à beaucoup moins d'acteurs puisque chaque bloc est horodaté et permet également l'archivage du document signé. Le recours à un tiers certificateur reste cependant obligatoire si la signature mise en place est une signature qualifiée.

Par ailleurs, le prix par signature proposé par des opérateurs classiques est relativement élevé et il doit être ajouté aux coûts entrainés par l'archivage des documents. Les transactions blockchain pourraient être proposées pour une somme modique.

[127] Article 29 et annexe II

[128] Article 28 et annexe I

[129] Article 27 1 a

Enfin, la solution de signature électronique serait bien plus sécurisée sur la blockchain.

La solution blockchain, pour les signatures électroniques semble donc être une solution moderne bien plus pragmatique, efficace, économe et sécurisée.

4. Les difficultés de l'utilisation de la blockchain comme solution de signature électronique

Outre les difficultés de mise en conformité eIDAS mentionnées ci-dessus, une solution de signature électronique blockchain semble poser deux difficultés majeures mais qui pourraient, selon nous, être résolues.

Ces deux difficultés tiennent à la nature publique du réseau blockchain et des informations qu'il contient, ce qui pourrait effrayer les contractants/signataires qui souhaitent d'une part que les termes de leur engagement restent confidentiels et d'autre part que leur identité et la personne avec qui ils contractent ne soient pas accessibles à n'importe qui.

La première difficulté est assez facilement évitée : il suffit d'intégrer dans le bloc signé par les parties uniquement un *hash* du contrat et non le contrat en entier. Cela a par ailleurs l'avantage d'alléger le poids du bloc en question et de nécessiter bien moins d'espace de stockage.

La question de la confidentialité des signataires se pose ensuite. Cette question est particulièrement délicate puisque tout l'intérêt d'une solution de signature électronique est justement de permettre de vérifier l'identité des signataires. Il faudra donc développer une signature permettant à tous les signataires d'être identifiés les uns envers les autres mais également de cacher leur identité à tout tiers à la transaction.

Or, l'utilisation de la cryptologie asymétrique telle que décrite ci-dessus pourrait permettre à toute personne disposant de la clé publique d'un signataire d'avoir accès à tous les contrats signés par ce dernier.

Ce problème pourrait néanmoins être contourné par l'utilisation de signatures multiples ou de *ring signatures,* qui permettent à leur tour de lier les clés publiques des différents signataires afin de créer une nouvelle clé publique unique à la transaction. Les signatures multiples sont d'ores et déjà supportées par certaines blockchains mais devraient être améliorées pour permettre la validation de la transaction seulement lorsque tous les signataires auront signé le bloc.

Cette question, hautement technique, devrait faire l'objet de développements plus poussés qui pourront être menés dans un document séparé.

E. BLOCKCHAIN ET CYBERSEURITE

La blockchain et la cybersécurité sont deux notions clés de l'ère du numérique. Si la première constitue le symbole actuel de l'évolution du monde digital, la seconde en revanche matérialise les dangers et les risques inhérents à ce domaine.

La cybersécurité est définie par l'ANSSI comme « *l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles* »[130]. La cybersécurité serait donc l'état idéal à atteindre dans un cyberespace où les risques afférents et inhérents aux systèmes informatiques seraient réduits au minimum.

La cybersécurité constitue aujourd'hui un enjeu croissant : les incidents liés à la cybercriminalité intervenaient en début d'année au rythme de quatre par semaine[131]. Ainsi, l'AMF dans sa cartographie des risques 2017[132] qualifie comme "élevé" le risque de cyber-attaques pour l'année en cours et prévoit un accroissement pour l'année 2018. Elle relève que dans l'industrie de la finance, les acteurs les plus touchés à ce jour après le secteur bancaire sont les plateformes d'échange de crypto-monnaie[133], premiers acteurs économiques connectant le grand public aux blockchains et autre registres distribués.

Actuellement, la cybersécurité est essentiellement encadrée par les dispositions de lutte contre la cybercriminalité[134] ciblant tant les attaques visant les systèmes d'informations (**1.**), que les attaques utilisant ces systèmes d'informations (**2.**). Dès demain, une législation naissante spécifique au secteur financier confiera des responsabilités propres aux acteurs du secteur en matière de cybersécurité (**3.**).

Ces outils juridiques peuvent être appliqués à la blockchain afin d'appréhender les différents types d'attaques qui seraient susceptibles de porter sur ce système ainsi qu'aux données qui y sont contenues.

---

[130] Définition issue du site officiel de l'ANSSI : https://www.ssi.gouv.fr/entreprise/glossaire/c/

[131] « Panorama de la cybercriminalité du CLUSIF : l'industrie du malware ne connait pas la crise ! », *Global Security Mag*, janvier 2017.

[132] AMF cartographie des risques 2017, juillet 2017.

[133] 120 000 bitcoins volés lors du piratage de Bitfinex en août 2016.

[134] Définition de l'ANSSI de la cybercriminalité : « *ensemble d'infractions pénales réprimant les actes contrevenants aux traités ou aux lois, et utilisant les réseaux ou les systèmes d'informations comme moyen de réalisation d'un délit ou d'un crime, ou les ayant pour cible* ».

1. Les outils juridiques de protection contre les attaques visant les systèmes d'informations

Dans l'industrie des marchés financiers où des informations sensibles sont échangées, la sécurité de la blockchain constitue une préoccupation majeure des entreprises qui envisagent d'intégrer la solution blockchain à leur activité.

Or, dès à présent, la blockchain, en tant que plateforme ou système digitalisée, peut être appréhendée par le droit en appliquant les règles existantes qui ont été élaborées afin de sanctionner les actes répressibles visant les systèmes d'information.

Une protection par le droit est en effet assurée par des dispositions pénales réprimant les attaques visant les systèmes d'informations[135]. Le code pénal contient un volet spécifiquement consacré aux atteintes aux systèmes de traitement automatisé de données (**STAD**).

Si la loi n'a pas défini les STAD, les travaux parlementaires de la loi du 5 janvier 1988 relatifs à la fraude informatique ont pu proposer la définition suivante[136] : « *un ensemble composé d'une ou plusieurs unités de traitement, de mémoires, de logiciels, de données, d'organes d'entrées-sorties et de liaisons qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité* »[137].

Il paraît raisonnable de considérer que les blockchains et autres registres distribués qui devront être mis en place pour enregistrer et transférer la propriété de titres financiers rentrent dans le champ des STAD tels que défini ci-dessus, et peuvent ainsi bénéficier de la protection des dispositions pénales qui leur sont applicables.

Ces dispositions du Code pénal relatifs au STAD répriment tout type d'intrusions ou modifications non autorisés dans ces systèmes. Il peut s'agir de l'accès frauduleux dans un STAD, le fait d'entraver ou de fausser son fonctionnement, d'introduire, de modifier ou encore supprimer des données dans un système de traitement automatisé de données.

L'accès frauduleux a été par exemple retenu lorsqu'un agent, titulaire de code d'accès au système, avait accédé à ce dernier et procédé à des modifications sans ordre de sa hiérarchie[138].

Outre les atteintes directes visant ces systèmes, le législateur a également entendu appréhender les groupes organisés aux fins de mener des cyberattaques. Ainsi, l'article 324-3 du Code pénal réprime le délit de participation à un groupement en vue de commettre une atteinte sur un STAD

[135] Article 323-1 à 323-8 du Code pénal.

[136] Cass. Crim., 12 juillet 2016, nº 16-82.455.

[137] Sénat, Rapport n°214 au nom de la Commission des lois constitutionnelles, de législation, du suffrage universel, du règlement, de l'administration générale sur la proposition de loi adoptée avec modifications par l'assemblée nationale en deuxième lecture relative à la fraude informatique, 22 décembre 1987, page 13.

[138] CA Paris 18 novembre 2010 09/07206.

ou « *association de malfaiteurs informatiques* »[139].

De même est sanctionnée par le Code pénal la mise à disposition d'équipements, instruments ou programme informatique conçus ou adaptés pour commettre des infractions aux STAD[140].

Si cette dernière infraction vise usuellement à punir les acteurs créant des outils de piratage, elle est parfois appliquée pour sanctionner des personnes sans intention malveillante particulière mais tirant des revenus de données permettant d'exploiter des failles de sécurité. Ainsi, le gérant d'un site permettant à des sociétés abonnées d'accéder à un répertoire de failles de sécurité contre rémunération, a été déclaré coupable de mise à disposition de données conçus pour commettre des atteintes aux systèmes de traitement de données automatisée[141].

Le parallèle avec la faille dans le code source de la plateforme décentralisée d'investissement The DAO[142] est manifeste. Pour mémoire, une clause du *smart contract* de The DAO n'était pas conforme à l'objet de l'engagement souhaité par les parties et a permis à une personne ayant identifié cette faille d'en profiter en siphonnant l'équivalent en crypto-monnaie de plusieurs dizaines de millions de dollars. L'infraction susvisée pourrait alors être le chef du développeur du *smart contract* ayant commis l'erreur de programmation, de l'utilisateur qui a identifié cette erreur et l'a exploitée ou encore des autres utilisateurs connaissant cette erreur (le code dudit *smart contract* étant public) mais qui n'ont pas empêché son exploitation[143].

En conséquence, l'arsenal répressif disponible permet d'ores-et-déjà d'appréhender et de réprimer les intrusions ou outils et moyens techniques développés aux fins de nuire à l'intégrité de la blockchain ou de porter atteinte à son contenu

2. Les outils juridiques de protection contre les attaques utilisant les réseaux

La cybersécurité est également assurée grâce aux dispositions du Code pénal qui sanctionnent ou préviennent les actes illicites commis par l'intermédiaire des réseaux.

En premier lieu, l'infraction d'extorsion, réprimée à l'article 312-1 du Code pénal, a déjà été retenue en jurisprudence lorsqu'elle était commise par l'intermédiaire d'un système informatique. Ainsi, un gérant d'une société avait organisé des attaques informatiques à l'origine de la paralysie des services d'une société concurrente pour obtenir, sous contrainte, le rachat de cette société. Ce gérant a été condamné, outre pour entrave à un système de données,

[139] Article 323-4 du Code pénal.

[140] Article 323-3-1 du Code pénal.

[141] CA Montpellier, 3e ch correctionnelle, 12 mars 2009 08/01431.

[142] « *Decentralized Autonomous Organization* ».

[143] Développements civilistes complémentaires dans JCP / La Semaine Juridique, Edition Administrations et Collectivités Territoriales, n° 28, 17 Juillet 2017 : « Commande publique et technologie *blockchain* : un avenir, mais quel avenir ? », Julien Moiroux, avocat à la Cour, Simmons & Simmons LLP.

pour extorsion.[144]

On peut imaginer que ce type de comportement visant à obtenir communication d'informations confidentielles portées par la blockchain, ou d'un support comme une clé cryptographique, ou tout simplement de porter atteinte au bon fonctionnement de la blockchain aux fins de dérober une somme d'argent ou des titres financiers pourrait être réprimé de manière similaire. Néanmoins, le caractère décentralisé de la blockchain réduit en pratique les possibilités d'actes d'extorsion par l'intermédiaire d'une blockchain.

Par ailleurs, la jurisprudence a transposé au domaine numérique la soustraction frauduleuse de la chose d'autrui en qualifiant de « *vol de données* »[145], l'accès, le maintien frauduleux dans un système de données et le téléchargement de données. Une qualification similaire pourrait aisément être appliquée à tout vol de données commis sur une blockchain.

Il en découle que l'arsenal répressif disponible permet également d'appréhender et de réprimer les infractions privatives de propriétés commises sur une blockchain.

3. Responsabilités propres aux acteurs du secteur financier en matière de cybersécurité

Indépendamment du volet pénal, un niveau de qualité de la sécurité doit être garanti au sein des blockchains au titre de législations plus spécifiques, par exemple, et comme évoqué ci-dessus, dans le cas où il serait procédé au sein d'une blockchain au traitement de données à caractère personnel ou en cas de recours à des outils d'authentification électronique.

A l'échelle du droit des marchés financiers, la cybersécurité n'était jusqu'au 2 septembre 2017 qu'un élément non spécifiquement défini compris dans la plus vaste obligation de disposer de moyens humains et matériels suffisant au regard des activités règlementées exercées et notamment d'assurer la robustesse des systèmes informatiques ainsi que de mettre en place des plans de continuité d'activité.

Avec la transposition de la DSP2[146], la notion de *cyber-attaque*[147] fait son apparition dans la définition plus large d'*incident de sécurité* intégrée, avec effet au 13 janvier 2018, aux mesures

---

[144] TGI Paris 12e, 19 mai 2006.

[145] Cass, Crim, 20 mai 2015 n°14-81-336.

[146] Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur.

[147] *« Un événement ou une série d'événements imprévus résultant de processus internes inadaptés ou défaillants ou d'évènements extérieurs affectant la disponibilité, l'intégrité, la confidentialité et la continuité des systèmes d'information et de communication et/ ou les informations utilisées pour la fourniture de services de paiement. Ceci inclut les incidents provenant de cyber-attaque ou de la non pertinence des mesures de sécurité physique ».* Nouvel alinéa ak) de l'article 10 de l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution (modifié par l'arrêté du 31 août 2017).

de contrôle interne applicables aux secteurs bancaire et financier dont notamment les intermédiaires et personnes habilités en vue de l'administration ou de la conservation d'instruments financiers[148]. Ainsi, à compter du 13 janvier 2018, tout incident majeur qualifié de cyber-attaque devra être notifié *« sans retard injustifié »* à la Banque de France[149].

La référence au nouvel article L. 521-10 du Code monétaire et financier semble suggérer que cette obligation ne s'appliquera à l'origine qu'aux prestataires de services de paiement, toutefois, une clarification de l'Autorité de Contrôle Prudentiel et de Résolution (**ACPR**) et, à défaut, une extension de son application aux autres acteurs visés par l'arrêté du 3 novembre 2014 précité serait bienvenue.

Ainsi, le droit semble être suffisamment équipé pour exiger des créateurs, exploitants ou gestionnaires de blockchains un niveau de sécurité élevé, mais également de protéger le système en cas d'intrusion. Si néanmoins, les évolutions techniques permettaient de contourner ces remparts virtuels[150], le droit devra alors évoluer afin de suivre ces avancées.

F. GOUVERNANCE D'UNE BLOCKCHAIN DANS LES ACTIVITES DE POST-MARCHE

La gouvernance d'un réseau distribué et décentralisé comme celui de la blockchain est au cœur des enjeux de pouvoirs et financiers. Or, il n'existe pas une gouvernance de la blockchain, mais autant de modes de gouvernance qu'il existe de types de réseaux distribués. En fait, le mode de fonctionnement d'un réseau distribué détermine sa gouvernance.

La *Proof of Work* (preuve de travail) et la *Proof of Stake* (preuve d'enjeu ou de possession) sont les deux manières de valider les blocs les plus connues. Elles impliquent deux mécanismes de consensus très différents, détaillés plus amplement ci-dessus.

Il est impossible dans un système informatique de calcul distribué de garantir en même temps (c'est à dire de manière synchrone) les trois contraintes suivantes :

- cohérence : tous les nœuds du système voient exactement les mêmes données au même moment ;

- disponibilité : garantie que toutes les requêtes reçoivent une réponse ; et

[148] Article 1 de l'arrêté du 3 novembre 2014 précité.

[149] Article 249-1 différé de l'arrêté du 3 novembre 2014 précité.

[150] Les autorités ukrainiennes ont récemment démantelé un atelier de contrefaçon de bitcoins cf KyivPost, 10 août 2017 https://www.kyivpost.com/technology/police-find-illegal-bitcoin-farm-ukrainian-state-institute.html

- tolérance au partitionnement : aucune panne moins importante qu'une coupure totale du réseau ne doit empêcher le système de répondre correctement.

Tout système de calcul distribué ne peut garantir à un instant *t* que le respect de deux de ces contraintes, mais pas les trois. C'est à ce défi que doit répondre le mode de gouvernance. Celle-ci est différente selon que l'on est en face de chaînes publiques, semi-publiques ou privées.

L'atout principal de la blockchain étant dans la sécurité des transactions, la gouvernance de celle-ci dépend du mode de son mode de fonctionnement.

Pour ne pas être falsifiable, une blockchain utilisant une méthode de consensus de la preuve du travail requiert qu'aucun opérateur hostile ne détienne, à aucun moment, plus de la moitié de la puissance de calcul de la chaîne.

Dans les chaînes de blocs publiques, la gouvernance est entre les mains de mineurs, c'est-à-dire ceux qui valident les transactions. Les utilisateurs (*stockholders*) n'ont pas ou peu de voix au chapitre. Une illustration de ce constat peut être trouvée dans le *fork* du Bitcoin durant l'été 2017. A la fin des fins, ce sont les mineurs qui ont décidé d'adopter une modification du protocole.

Il apparaît clair que dans les blockchains sur les marchés financiers, le régulateur aura un rôle de premier plan à jouer dans la surveillance de la non-falsifiabilité des chaînes de consensus.

Un autre enjeu de gouvernance dérive de la compatibilité entre les normes anti-blanchiment et la structure du bloc où les transactions sont enregistrées sous pseudonyme, à travers des clés publiques, en complément à des clés privées.

Dans le domaine des activités de post-marché, la question de la gouvernance est tout autant un enjeu essentiel. En fait, il s'agit de déterminer si le fonctionnement de la tenue de registres décentralisés et distribués peut être confié à des individus ou entités tierces, sans même parler du fait que s'agissant des blockchains publiques les mineurs sont localisés hors d'Europe (en pratique en Asie et en particulier en Chine) ce qui pose nécessairement une question de souveraineté.

Bien sûr, si la technologie de chaine de blocs utilisée dans les activités de post-marché est une chaîne privée, donc fermée, la gouvernance se rapprochera alors de celle d'un consortium, voire tout simplement d'une société anonyme, c'est-à-dire d'un partage du pouvoir entre les détenteurs de la technologie.

G. CONFLITS DE LOIS DANS LES ACTIVITES DE POST MARCHE

Dans la mesure où un juge aura tôt ou tard à se prononcer à l'occasion d'un litige relatif à une DLT, se pose la question de déterminer la compétence de ce juge au regard des règles de droit international privée.

La question prend une tournure encore plus précise en matière de titres financiers où différents textes viennent établir ou préciser les règles de compétence en matière de conflits de lois.

Au niveau international, la Convention de La Haye du 5 juillet 2006 sur la loi applicable à certains droits sur des titres détenus auprès d'un intermédiaire, bien que ratifiée par un nombre très limité de pays, constitue une référence importante dans les critères de détermination de la loi applicable aux titres.

Au sein de l'Union européenne, différentes règles harmonisées sur les conflits de lois existent qui trouvent à s'appliquer en matière de titres financiers :

- Directive sur le caractère définitif du règlement en ce qui concerne les titres de compte fournis en garantie aux participants des systèmes de règlement, de la BCE ou de la banque centrale des États membres ;

- Directive sur les sûretés financières en ce qui concerne les titres inscrits en compte dans le cadre de contrats financiers ;

- Directive relative à la liquidation concernant l'application des droits de propriété sur les titres inscrits en compte dans les procédures d'insolvabilité des établissements de crédit et des sociétés d'investissement.

Dans ces textes, les trois règles de conflit de lois sont basées sur une approche similaire : le concept PRIMA, tel que retenu dans la convention de La Haye, c'est-à-dire le lieu de l'intermédiaire pertinent.

Les facteurs de connexion dans les trois directives européennes diffèrent en détail, mais peuvent être résumés comme suit : il s'agit d'un registre, d'un compte ou d'un système de dépôt centralisé. Mais, les notions de "registre" ou "compte" ne sont pas définies ou mal définies dans ces textes. En fait, ces règles de conflit de lois ne précisent pas où le compte / registre, le système de dépôt centralisé est "situé" ou "maintenu".

La règle PRIMA s'écarte des facteurs de connexion traditionnels se référant au lieu d'incorporation de la société émettrice. Au lieu de cela, cette règle se réfère à la loi du compte de titres auquel les titres concernés sont crédités. Cette loi régit tous les titres crédités sur ce compte, qu'ils soient étrangers ou domestiques.

Quel pourrait être le facteur de connexion pour considérer la nature du droit ainsi que les conditions d'acquisition et de disposition dans un système de chaîne de blocs ?

La règle PRIMA présuppose l'existence de comptes et donc d'intermédiaires, qui n'existeront pas en tant que tels dans la mise en place du bloc. Il convient donc d'écarter cette règle de conflit de loi, non adaptée au cas d'un registre distribué et décentralisé.

Premier facteur de connexion possible, la loi de l'émetteur des titres, ou *lex societatis*. Ce critère, qui créerait certes une incertitude juridique importante du fait de la multiplicité de lois potentiellement applicables dans le cas d'un portefeuille international, semble cependant le plus adapté du fait du caractère inapproprié des deux critères détaillés ci-dessous.

Second facteur de connexion possible, le point d'entrée de la chaîne de bloc. Ce facteur ne résout cependant pas le problème dans la mesure où il y a autant de point d'entrée que les participants de la chaîne.

Troisième facteur de connexion possible, la loi de la juridiction où le système est situé ou supervisé. Encore faut-il que le registre de blocs ou l'administrateur de ce registre soit régulé, ce qui n'est pas possible dans une chaine de blocs publique.

En fait, en matière d'activité post-marché, et dans la mesure où le fonctionnement de la blockchain fera plutôt appel à une blockchain privée ou semi-privée, la solution pourrait passer par imposer à l'administrateur gérant le registre distribué d'être agréé par le superviseur du lieu où il est incorporé au titre d'une activité nouvelle, à savoir celle de teneur de registre distribué.

V. REPONSE A LA CONSULTATION DU TRESOR

Comme mentionné en introduction, ce rapport constitue une réponse générale à la consultation de la Direction Générale du Trésor destinée à nourrir la réflexion des pouvoirs publics dans l'élaboration du cadre législatif et réglementaire applicable aux registres distribués.

L'objectif du groupe de travail est de formuler des propositions ou recommandations aux pouvoirs publics afin de permettre l'utilisation de la DLT dans les activités de post-marché. Il s'agit notamment d'utiliser les possibilités ouvertes par la loi Sapin II permettant de légiférer par ordonnance.

Les propositions ci-dessous se limitent aux dispositions d'ordre législatif et ne traitent pas des modifications d'ordre réglementaire.

CONTRIBUTEURS DU COMITE BLOCKCHAIN PARIS EUROPLACE

Président :

Hubert de Vauplane, avocat à la Cour, Kramer Levin Naftalis & Frankel LLP

Membres :

Emilien Bernard-Alzias, avocat à la Cour, Simmons & Simmons LLP

Céline Bondard, avocat à la Cour, Bondard et ass.

Alexis Collomb, Professeur au CNAM

Emilie Danglades-Perez, avocat à la Cour, Simmons & Simmons LLP

Thierry Dor, avocat à la Cour, Gide Loyrette Nouel AARPI

Jean-Gabriel Flandrois, avocat à la cour, Gide Loyrette Nouel AARPI

Alexandre Léger, fondateur et PDG, eCapitalio

Eric Roturier, avocat à la Cour, Allen & Overy LLP

Guillaume Seligmann, avocat à la Cour, Cohen Gresser

AFTI

AFG

Euroclear

BNPP Securities Services

ANNEXE 1

LEXIQUE

Le vocabulaire financier, économique ou informatique fait l'objet d'avis ponctuels de la Commission d'enrichissement de la langue française publiés au Journal officiel. L'avis de la Commission publié au Journal officiel du 23 mai 2017 (NOR : CTNR1713838K) relatif au vocabulaire de l'informatique définit les principaux termes issus de la blockchain. Les termes et les définitions arrêtés par la Commission sont marqués d'un astérisque (*).

Terme anglais	***Terme français***	***Définition***
Block validation	Validation de bloc*	Opération informatique utilisée pour rendre un bloc infalsifiable et le valider dans une chaîne de blocs.*
Consensus	Consensus	Mécanisme permettant de s'assurer que chaque nœud du réseau dispose bien de la même information avant d'enregistrer définitivement une opération dans la blockchain.
Cryptocurrency	Crypto-monnaie ou Cybermonnaie*	Monnaie dont la création et la gestion reposent sur l'utilisation des techniques de l'informatique et des télécommunications.*
Distributed ledger technology	Registre partagé distribué	Registre de données partagé entre tous les participants de la blockchain. Seule la validation d'une transaction par le biais d'un consensus peut opérer la modification de son contenu.
Fiat money	Monnaie légale	Terme désignant les monnaies étatiques ayant cours légal et un pouvoir libératoire. Elles s'opposent notamment aux crypto-monnaies, dépourvue de valeur légale propre.
Fintech	Entreprises de technologie financières	Cette appellation, contraction de « technologie » et « finance », désigne selon le contexte les entreprises de nouvelles technologies spécialisées dans la conception de services innovateurs dans le domaine de la finance, ou les services eux-mêmes.
Miner	Mineur	Personne physique ou morale mettant à disposition sa puissance de calcul informatique pour les besoins du minage.
Mining	Minage*	Validation de bloc donnant lieu à la création de nouvelles unités de compte au profit du participant dont le bloc a été retenu par le réseau.*

Terme anglais	*Terme français*	*Définition*
Node	Nœud	Matériel informatique relié à la blockchain qui est chargé d'effectuer les calculs. (v. également « mineurs »).
Peer-to-peer	Pair à pair*	Se dit du mode d'utilisation d'un réseau dans lequel chacun des participants connectés dispose des mêmes droits et qui permet un échange direct de services sans recourir à un serveur central; par extension, se dit d'un tel réseau.*
Private blockchain	Chaîne de blocs* privée (ou « fermée »)	Type de blockchain dont l'accès est réservé à certains participants.
Private key	Clef privée	La clef privée permet de décoder un message précédemment crypté par la clef publique. Contrairement à cette dernière, la clef privée est connue par un seul utilisateur.
Proof of Concept (« PoC »)	Preuve de concept	Démonstration de la faisabilité d'un concept au moyen d'une courte présentation tiré d'un cas concret.
Proof of Work (« PoW »)	Preuve de travail*	Résultat d'une tâche fortement consommatrice de ressources de calcul, dont l'exactitude est facilement vérifiable par tout participant et atteste que cette tâche a bien été effectuée en consommant les ressources nécessaires. La preuve de travail est notamment employée pour contribuer à l'établissement de la confiance des utilisateurs en une cybermonnaie, la fraude étant découragée par la difficulté de la validation de blocs.*
Public blockchain	Chaîne de blocs* publique (ou « ouverte »)	Type de blockchain dont l'accès est ouvert à tout participant qui souhaiterait y intervenir.
Public key	Clef publique	Connue de tous, la clef publique constitue l'adresse de la blockchain. Elle permet d'encoder un message et sera utilisée afin qu'un émetteur puisse désigner un destinataire dans le cadre d'une transaction.
Smart contracts	Contrats intelligents	Contrats numériques permettant d'exécuter les termes qu'ils contiennent sans intervention humaine.
Token	Jeton	Le jeton est une unité de base qui peut être transmise en sein d'un registre distribué (ex : le jeton de la chaîne Bitcoin est le Bitcoin). Le jeton peut également contenir des informations au-

Terme anglais	*Terme français*	*Définition*
		delà de leur aspect quasi-monétaire (information sur la propriété, sur l'orientation d'un vote, ou toute autre chose…).

ANNEXE 2

BIBLIOGRAPHIE

- A. Santo et al. "*Applicability of the Ditributed Ledger Technology to Capital Market Infrastructure*", Japan Exchange Group, Working Paper, 3O August 2016, vol. 15.

- A. Benssoussan, *Le robot créateur peut-il être protégé par le droit d'auteur*, Planète Robot n°42, accessible à l'adresse suivante : https://www.alain-bensoussan.com/wp-content/uploads/2016/12/34125221.pdf.

- BRI, *Central bank cryptocurrencies*, septembre 2017, accessible à l'adresse suivante : https://www.bis.org/publ/qtrpdf/r_qt1709f.htm.

- C. Caron, *Les licences de logiciels dits "libres" à l'épreuve du droit d'auteur français*, D. 2003, p. 1556.

- M. Dantant, *Droit d'auteur des chercheurs, Logiciels, Bases de Données et Archives Ouvertes*, CNRS, Direction des affaires juridiques, 7 juillet 2014.

- W. Diffie et M.E. Hellman, *New Directions in Cryptography*, 6 novembre 1976.

- ECB, *Distributed Ledger Technolgies in securities post trading, revolution or evolution*, Occasional paper series, n° 172, April 2016.

- Euroclear and Oliver Wyman Joint Report, "*Blockchain in the Capital Markets – The Prize and the Journey*", February 2016.

- Euroclear and Slaugther & May Joint Report, "*Blockchain Settlement: Regulation, innovation and application*", November 2016.

- P. de Filipi et B. Jean, *Les smarts contracts, les nouveaux contrats augmentés ?* La revue de l'ACE, septembre 2016, n°137.

- D. Galeon et P. Caughill, *Major Players Unite to Define Blockchain Token Securities Law*, 7 décembre 2016, accessible à l'adresse suivante : https://futurism.com/major-players-unite-to-define-blockchain-token-securities-law.

- IMF Staff Discussion Note, *Virtual Currencies and Beyond: Initial Considerations*, janvier 2016.

- IMF Staff Discussion Note, *Fintech and Financial Services: Initial Considerations*, juin 2017, accessible à l'adresse suivante : http://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2017/06/16/Fintech-and-Financial-Services-Initial-Considerations-44985.

- ISDA Whitepaper, *The Future of Derivatives Processing and Market Infrastructure*, septembre 2016.

- ISDA / Linklaters Whitepaper, *Smart Contracts and Distributed Ledger – A Legal Perspective*, août 2017.

- M. Jacob, *Panorama de la cybercriminalité du CLUSIF : l'industrie du malware ne connait pas la crise*! Global Security Mag, janvier 2017.

- Kramer Levin, *Gestion du passif des OPC et enjeux réglementaires*, juillet 2014.

- L. Lamport, R. Shostak et M. Pease, *The Byzantine Generals Problem*, 5 juillet 1982.

- L. Lessig, *Code is Law*, Harvard Magazine, janvier 2016, accessible à l'adresse suivante : http://harvardmagazine.com/2000/01/code-is-law-html.

- M. Mainelli et A. Milne, *The impact and potential of blockchain on securities transaction lifecycle*, 9 mai 2016, accessible à l'adresse suivante : http://www.swiftinstitute.org/wp-content/uploads/2016/05/The-Impact-and-Potential-of-Blockchain-on-the-Securities-Transaction-Lifecycle_Mainelli-and-Milne-FINAL.pdf.

- S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 31 octobre 2008, accessible à l'adresse suivante : https://bitcoin.org/bitcoin.pdf.

- P. Paech, "Securities, intermediation and the blockchain - an inevitable choice between liquidity and legal certainty?" *Uniform Law Review* (2016) 21 (4) pp.612-639.

- P. Paech, "'Securities, intermediation and the blockchain - an inevitable choice between liquidity and legal certainty?" *LSE Law and Economy Working Paper Series* 20/20150.

- R.L. Rivest, A. Shamir, and L. Adleman *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, février 1978.

- M. Schuler et B. Znaty, *La propriété intellectuelle et la transformation numérique de l'économie*, accessible à l'adresse suivante : https://www.inpi.fr/sites/default/files/1_3_extrait_pi_et_transformation_economie_numerique_inpi.pdf.

- H. de Vauplane, *La Blockchain et la loi*, La finance décryptée par le Droit, 14 février 2016.

- A. Wright and P. De Filippi, "*Decentralised Blockchain Technology and the Rise of Lex Cryptographica*" (2015) Working paper, 11-12, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.

- P. Yolka, *Prendre les « communs » au sérieux*, AJDA 2016. 1.