Table ronde

AVEC > **ÉRIC CAPRIOLI**, AVOCAT À LA COUR DE PARIS, **BENOÎT CHARPENTIER**, ANCIEN DIRECTEUR JURIDIQUE, ENTREPRENEUR, **VALÉRIE CHAVANNE**, AVOCATE À LA COUR, **JÉRÔME DE LABRIFFE**, PRÉSIDENT DE KINGERI GROUP, **DOMINIC O'KANE**, PROFESSEUR AFFILIÉ EN FINANCE À L'EDHEC BUSINESS SCHOOL, **CHRISTOPHE ROQUILLY**, PROFESSEUR DE DROIT À L'EDHEC BUSINESS SCHOOL,, DIRECTEUR DU CENTRE LEGALEDHEC,, DOYEN DU CORPS PROFESSORAL ET DE LA RECHERCHE, **ARNAUD TOUATI**, COFONDATEUR DU CABINET ALTO AVOCATS, **ÉDOUARD VIGUIER**, JURISTE, KINGERI GROUP

2 BLOCKCHAIN ET SMART CONTRACTS : ENJEUX TECHNOLOGIQUES, JURIDIQUES ET BUSINESS

« Bitcoin », « Blockchain », « Smart contracts » : autant de concepts qui sont des réalités technologiques et même business pour certains experts, et des notions encore bien mystérieuses pour les non-sachants. Cependant, l'évolution - ou la révolution selon les points de vue - semble être en marche. Au moment où nous écrivons ces lignes, une requête sur le moteur de recherche Google à partir du mot-clef « Blockchain », dans la partie Actualités, fait apparaître bon nombre d'articles très récents publiés dans des médias et sites web : « Blockchain, cette inconnue dont tout le monde prononce le nom », « La blockchain, un outil green ? », « Blockchain, la révolution de la confiance ? », « Blockchain, c'est quoi ? », « Devoir de vigilance et Blockchain, une flûte enchantée 2.0 ? », « Les apports de la blockchain ne seront pas révolutionnaires », etc.

Pour apporter des éclairages sur ce que sont réellement la blockchain et les smart contracts, leurs enjeux juridiques, ainsi que leurs applications concrètes dans notre économie, cette table ronde, dirigée et pilotée par Christophe Roquilly, en partenariat avec le Centre de recherche LegalEdhec de l'EDHEC Business School, réunit plusieurs experts, ayant des compétences, métiers et expériences complémentaires. Jérôme de Labriffe et Édouard Viguier nous proposent une introduction synthétique et très claire de ce qu'est la blockchain, en mettant en évidence la distinction fondamentale entre blockchain publique et blockchain privée. Valérie Chavanne la complète en nous livrant quelques pistes de réflexion sur les enjeux juridiques. Puis, Éric Caprioli, Benoît Charpentier, Dominic O'Kane et Arnaud Touati partagent leurs analyses et opinions sur la qualification juridique des smart contracts, les questions juridiques qu'ils posent et les grands enjeux, en particulier pour l'industrie financière.

Nous les remercions infiniment pour le temps qu'ils ont y consacré et nous vous souhaitons une très bonne lecture, en langage naturel !

EDHEC BUSINESS SCHOOL
Centre de Recherche LegalEdhec

Christophe Roquilly : Que doit-on savoir de la blockchain en tant que technologie et quels sont ses enjeux juridiques ?

Jérôme de Labriffe et Edouard Viguier : Avant de se plonger plus avant dans les défis juridiques entourant la blockchain et les smart-contracts, il est nécessaire de réaliser que le terme "blockchain", employé à tort et à travers pour des raisons marketing, englobe plusieurs réalités profondément différentes.

Souvent le lecteur est confronté à des analyses sur les blockchains « publiques », « privées, ou de consortium », lesquels considèrent que les défis juridiques passionnants entourant les blockchains dites publiques concernent également leurs homologues dites privées. Il s'agit ici de nuancer ce propos, afin d'arriver à une meilleure compréhension des enjeux.

Afin d'explorer cette distinction nous retiendrons ici la définition de la blockchain publique posée par Vitalik Buterin dans un de ses articles sur le sujet : « une blockchain publique est une blockchain que quiconque dans le monde peut lire, à laquelle quiconque peut envoyer des transactions et les y voir incluses si elles sont valides, et au mécanisme de consensus de laquelle quiconque peut participer - le mécanisme de consensus déterminant quels blocs sont ajoutés à la chaîne et l'état actuel d'icelle ». Les règles particulières quant aux mécanismes de consensus et au fonctionnement d'une blockchain publique sont librement établies par les différents acteurs de l'écosystème prenant part à son développement.

Ainsi, dans une blockchain publique, la confiance dans une entité centrale (banque, gouvernement, etc.) est remplacée par ce mécanisme de consensus parfois qualifié de « cryptoéconomique », combinant diverses incitations économiques à des procédés de vérification cryptographiques. C'est ce mécanisme qui fait la particularité d'une blockchain publique et lui permet de fonctionner sans aucun système de permissions (système de définition des droits d'accès aux ressources permettant de discriminer les utilisateurs dans leurs droits de lecture, d'écriture ou d'exécution au sein d'un système informatique), tous les utilisateurs jouissant des mêmes droits d'accès au système.

Ce mécanisme et les principes d'ouverture d'une blockchain publique emportent un certain nombre de conséquences telles que l'irrévocabilité d'une transaction, l'accès public et libre aux informations qui y sont stockées, le pseudonymat des utilisateurs, etc. Ces conséquences, qui sont vues comme des avantages par les défenseurs des blockchains publiques, sont bien souvent des freins à une utilisation par des sociétés qui, ne serait-ce que juridiquement, ne peuvent les accepter.

À l'inverse, une blockchain privée ou de consortium est un système reposant sur les mêmes bases techniques mais dénué de mécanisme de consensus économique. Elle dispose d'un système de permission permettant de discriminer les droits des utilisateurs au même titre que les solutions déjà utilisées dans les entreprises. Dans ce cadre-là, les données ne sont accessibles qu'aux utilisateurs autorisés par les administrateurs du système, de même que seuls les utilisateurs autorisés peuvent écrire dedans ou exécuter certaines fonctions.

Christophe Roquilly

Christophe Roquilly est professeur de droit et doyen du corps professoral et de la recherche à l'EDHEC Business School, où il dirige aussi le Centre LegalEdhec. Ses travaux portent sur les relations entre le droit et la stratégie d'entreprise, le management des risques juridiques et la compliance. Il a publié dans de nombreuses revues nationales et internationales et est membre du comité scientifique de plusieurs think tanks, ainsi que de l'Advisory Board d'ECLA (European Company Lawyers Association) et de l'Advisory Board du cabinet Arsene Taxand.

Ce système de permissions est établi selon les désidératas de l'entreprise ou du consortium, et fait de la blockchain privée un système "classique" dénué des caractéristiques jugées indésirables des blockchains publiques, notamment le libre accès aux données et l'irréversibilité des transactions. À ce titre, on peut noter que l'entreprise R3CEV, qui a su surfer sur la « hype » blockchain, est la première à reconnaître que son produit n'est en aucun cas une blockchain, illustrant bien l'intérêt douteux de nommer ce genre de systèmes « blockchains privées » et la confusion qui en résulte.

C. R. : Qu'en est-il des professionnels du droit et de l'innovation ? Peut-on parler de cercle vertueux ?

Valérie Chavanne : L'innovation technologique sollicite, encore une fois, l'innovation juridique. Tout le monde s'accorde à dire qu'il s'agit d'une union nécessaire de talents complémentaires ayant des objectifs communs : le développement et la promotion de l'innovation. Il est primordial de faciliter ces discussions pour encourager les promoteurs de l'innovation technologique à créer sereinement, tout en invitant les professionnels du droit à lire et encadrer, avec compréhension et créativité, les progrès de la science. Ces évolutions encouragent définitivement des rapprochements devenus évidents et stratégiques.

Instinctivement, les professionnels du droit cherchent à appliquer le droit existant aux nouveaux usages, mais nous savons que beaucoup de textes sont entrés en vigueur avant les

innovations - notamment avant la blockchain - et qu'il est impératif de revisiter certaines règles lorsque les outils juridiques ne trouvent pas de réponses pragmatiques et efficaces aux nouveaux usages, ou lorsque les règles de droit mériteraient d'être adaptées.

C. R. : Quelles sont les premières questions juridiques spécifiques que pose la blockchain ?

V. C. : Nous sommes, à ce stade, très loin d'avoir fait le tour des problématiques juridiques engagées par la blockchain. Ces réflexions extrêmement intéressantes prendront certainement encore un peu de temps. Nous pensons qu'il faudrait encourager urgemment une lecture affinée des professionnels du droit des smart contracts - contrats dessinés et rédigés par des techniciens et qui régissent actuellement la majeure partie des relations de la blockchain dite publique. Il semble également urgent et important de clarifier les questions du droit applicable et des juridictions compétentes. Ce premier exercice de débroussaillage offrira une meilleure lecture aux juridictions saisies avec des règles simplifiées et uniformisées sur l'appréciation des lois et des juridictions compétentes. L'arbitrage, largement utilisé dans la résolution de discussions actuelles de la blockchain, pourrait être identifié comme une piste à privilégier. Faut-il voir l'arbitrage comme un facilitateur dans la résolution de confits transfrontaliers ou comme un mécanisme adapté pour soutenir l'innovation ? Sur les autres problématiques juridiques importantes engagées dans la discussion de la blockchain, nous pensons, à ce stade, qu'il faudrait porter une attention toute particulière à deux disciplines du droit : la protection des données personnelles et la propriété intellectuelle. Elles sont, notamment, confrontées à la question de l'irréversibilité de certaines démarches engagées dans la blockchain.

C. R. : Pourriez-vous nous donner quelques pistes de réflexion ?

V. C. : Nous pensons qu'il faudrait concentrer nos premiers efforts sur le développement d'outils pédagogiques et de formation tant pour les professionnels que pour le grand public. Les nouveaux usages de la blockchain doivent être compris par tous (industriels, législateurs, pouvoirs publics, utilisateurs, etc.) pour que nous puissions adresser les bonnes questions et trouver les meilleures solutions. Un premier exercice d'analyse des pratiques existantes (smart contracts, notamment) pourrait aider les professionnels du droit qui ont la lourde responsabilité d'édicter des éléments de cadrage de la blockchain. Enfin, s'il est pragmatique et naturel de chercher des solutions juridiques au sein du droit existant, il nous semble intéressant d'engager, dès à présent, des réflexions européennes et/ou globales pour éviter de construire des règles de droit susceptibles d'être challengées par des pratiques sans frontières.

C. R. : Quel est le lien entre « blockchain » et « smart contracts » ? Peut-on considérer que ces derniers sont un process digitalisé permettant d'exécuter un contrat préalablement conçu par des juristes « êtres humains » ? Peut-on également considérer qu'un tel contrat puisse être généré automatiquement à partir de lignes de codes se nourrissant non pas d'un contrat déjà rédigé, mais d'un ensemble d'informations juridiques pouvant être agrégées ?

^ Jérôme de Labriffe

Jérôme de Labriffe est président de KINGERI Group, société de consulting stratégique dans le domaine de la cyber sécurité, le développement des crypto-monnaies et de la blockchain et la protection des données. Il a été successivement directeur du développement digital puis directeur de l'innovation puis du développement du big data chez BNP Paribas, où il était en charge de la mise en place de la stratégie de la banque à distance sur les nouveaux canaux et sur l'ensemble des territoires retail où le groupe est présent. Entré chez BNP en 1998, il a développé et structuré la présence et l'offre de la banque sur internet et sur le mobile dans le cadre de la banque de détail en France. Entre 2005 et 2014, il a été élu président de l'Interactive Advertising Bureau France (IAB), ou il a assuré le développement et l'autorégulation de la publicité sur internet en France.

Éric Caprioli : Comme j'ai déjà eu l'opportunité de le préciser à l'occasion d'une interview *(V. E. Caprioli, La blockchain ou la confiance dans une technologie : JCP G 2016, 672)*, la blockchain (ou chaîne de blocs) est une technologie de stockage et de transmission d'informations visant à faire communiquer des serveurs entre eux, choisis de manière aléatoire en fonction de leur capacité de calcul, et en utilisant des clés cryptographiques asymétriques et des algorithmes de hachage. Ainsi sont assurées intégrité et authenticité des transactions. Celles-ci peuvent être vérifiées par chaque utilisateur sur un registre numérique anonyme et sécurisé. Il est à noter qu'il existe 3 types de blockchain : publique (ouverte à tous et gratuite ; par exemple, les bitcoins utilisent la blockchain), privée (seuls certains acteurs peuvent y accéder et l'utiliser ; par exemple, dans le secteur bancaire) et hybride. La blockchain a recours à plusieurs smart contracts dont l'exécution est contrôlée et vérifiable.

Benoît Charpentier : Un smart contract, ou contrat intelligent, est un code informatique qui déclenche automatique-

ment des actions liées à la survenance de certaines conditions prédéfinies. Le terme « contrat intelligent » fait référence au fait que le contrat est capable de s'exécuter automatiquement sans l'intervention d'un tiers. Le programme peut définir des règles et des conséquences strictes de la même manière qu'un document juridique traditionnel, mais contrairement à un contrat traditionnel, il peut également prendre en compte des données externes, les traiter selon les règles énoncées dans le contrat et prendre les mesures programmées à l'avance. Les contrats intelligents ne sont pas nécessairement encodés sur la blockchain. Néanmoins, l'avènement des protocoles cryptographiques et de la blockchain offre un nouvel élan aux contrats intelligents. Ces contrats sont prometteurs dans les cas où l'exécution est suffisamment simple et standard pour être automatisée. Les contrats nécessitant (i) une appréciation subjective, (ii) une réversibilité des transactions, (iii) la mise en œuvre de normes interprétatives, et (iv) faisant appel à des données externes au contrat, rendront l'exécution automatisée plus ardue. En l'état de la technologie, les contrats intelligents ne sont pas encore en mesure de refléter la subtilité et la richesse des contrats rédigés en langage naturel ou d'assurer l'exercice du pouvoir discrétionnaire accordé à une partie. Lorsque l'exercice d'un pouvoir discrétionnaire est exigé de l'une des parties, il peut être envisagé de mettre en place un mécanisme permettant la suspension temporaire de l'exécution du contrat intelligent et l'intervention d'un tiers de confiance.

E. C. : Parler de contrat « intelligent » signifierait que les autres ne le sont pas, car empreints d'émotion, sans doute de ce qui constitue le fondement du contrat : le consentement. Il se définit comme un contrat programmé qui s'exécute automatiquement conformément au code informatique inscrit dans le marbre ; si la condition/instruction est vérifiée, alors elle s'exécute. Selon Nick Szabo, l'informaticien qui a inventé ce concept en 1997, « Les contrats intelligents combinent les protocoles, les interfaces utilisateur et les promesses exprimées à travers ces interfaces, pour formaliser et sécuriser les relations sur les réseaux publics. Cela nous donne de nouvelles façons de formaliser les relations numériques qui sont beaucoup plus fonctionnelles que leurs ancêtres papier inanimés. Les contrats intelligents réduisent les coûts de transaction mentaux et informatiques, imposés soit par les principaux acteurs, soit par des tiers, soit par leurs outils ». On le voit d'emblée, ces contrats ne sont pas des contrats à proprement dit, car le plus souvent, ils ne sont pas conçus par des juristes ; l'objectif étant plutôt de se passer des juristes ! D'ailleurs, outre le « contrat intelligent », on observera que le jargon utilisé par les informaticiens ne parle que de droit : « code is law », « proof of work », « proof of stake », etc., et cela ne correspond pas à la réalité juridique. Pour répondre plus précisément à la question, on peut estimer avec Madame Primavera de Filipi qu'« un smart contract est un logiciel. Au vu de leur appellation, on a tendance à les assimiler à des contrats, mais ils n'ont pas en eux-mêmes d'autorité juridique. Lorsqu'un contrat juridique existe, le smart contract n'est qu'une application technique de ce contrat ».

^ Valérie Chavanne

Valérie Chavanne compte 20 ans d'expérience en entreprise dans les secteurs des médias et des nouvelles technologies en France et à l'international. Elle a défini la stratégie juridique de ces entreprises dans un contexte en forte mutation et a porté leurs voix auprès des associations professionnelles, des autorités et des pouvoirs publics. Vice-présidente de l'IAB France depuis 2014, elle a contribué à la création et au développement des travaux de la commission Affaires Publiques, ainsi qu'à son rayonnement. Dernièrement, Valérie occupait le poste de directrice juridique et directrice des affaires publiques pour l'Europe du Sud chez Yahoo. Elle développe aujourd'hui une activité libérale dédiée au service des entreprises du digital.

Arnaud Touati : Le smart contrat n'est pour moi pas véritablement un contrat, mais bien un logiciel. En effet, il n'a pas en lui-même d'autorité juridique, et il s'agit davantage de l'application technique et automatique d'un contrat ayant une valeur juridique (par exemple, le paiement d'un loyer qui génèrerait automatiquement une facture, etc.). Le fait qu'une facture soit générée automatiquement n'est pas un contrat. Il s'agit plutôt de la conséquence, automatique, de la vérification d'une opération par un logiciel (paiement effectif du loyer) qui, une fois validée, autorise ensuite une action (l'émission de la facture). Un tel contrat peut également être généré automatiquement à partir de lignes de codes se nourrissant d'informations juridiques pouvant être agrégées. Mais il devra s'agir d'opérations simples. En effet, comment un logiciel pourrait-il comprendre des termes juridiques soumis à une appréciation comme « délai raisonnable », « mettre en œuvre tous les moyens », « agir en bon père de famille », etc. ? L'intérêt pour les smart contracts est grandissant. En témoigne notamment, dans le domaine des start-ups sur lequel nous nous sommes spécialisés chez Alto Avocats, Slock.it, une start-up allemande, qui a levé plusieurs millions de dollars relativement à la création de smart contracts en matière de location d'appartement entre particuliers de type Airbnb. La location offre un champ d'application pratique : ainsi, le cas d'un contrat de location saisonnière portant sur un appartement dont la serrure serait

une clef électronique et qui permettrait au propriétaire de verrouiller à distance son logement lorsque son loueur n'exécute pas ses engagements (en cas de non-règlement ou de règlement partiel d'un loyer).

C. R. : Peut-on réellement parler de questions juridiques spécifiques à ces smart contracts, en dehors des règles de droit commun s'appliquant à la formation et à l'exécution du contrat ?

E. C. : Non, il n'y a pas de règles spécifiques aux smart contracts. Le droit commun s'applique : pour les contrats soumis au droit français, ce sont les règles applicables à la formation et à l'exécution des contrats depuis le 1er octobre 2016, suite à l'ordonnance du 10 février 2016. Les seuls contours « spécifiques », mais prévus dans le Code civil, découleront de la volonté des parties, comme par exemple l'aménagement de la preuve avec les conventions sur la preuve. En outre, l'article L. 223-13 du Code monétaire et financier sur les minibons avec blockchain dispose que les transferts de propriété s'opèrent par cession de créance dans le dispositif d'enregistrement électronique qui tient lieu de contrat écrit conformément aux articles 1321 et 1322 du Code civil. Ou encore, pour la signature électronique et l'horodatage, il faudra être conforme au règlement européen eIDAS du 23 juillet 2014 applicable directement dans tous les États membres. On n'oubliera pas non plus les nombreuses règles imposées aux blockchains en matière de respect de la vie privée et de protection des données personnelles (droit à l'oubli/effacement, responsable de traitement, etc.), de conformité au règlement européen du 27 avril 2016, ou encore de « connaissance client » (KYC).

A. T. : De mon point de vue, il y a effectivement des questions juridiques spécifiques qui sont posées relativement à ces smart contracts : quel est le droit applicable à ces opérations dans la blockchain ? Quelle est la force juridique (probatoire ou force exécutoire) des informations inscrites dans ces contrats ? Faut-il attacher davantage d'importance au langage naturel ou à sa traduction codifiée ? D'autres questions de nature juridique se posent également, notamment au regard de la régulation de ces smart contracts et du caractère international de certaines opérations. De plus, certains contrats ne peuvent pas être des smart contracts parce qu'ils bénéficient déjà de l'enregistrement dans un registre certifié, à l'instar de la fiducie qui est un contrat écrit enregistré aux services des impôts, et déclaré au registre national des fiducies.

B. C. : Concernant la formation du contrat, un code fonctionne uniquement d'après les informations et les directives précises fournies. Les parties doivent s'assurer que le contrat intelligent reflète bien l'intention des parties et s'exécutera conformément à leur volonté. Dans de nombreuses juridictions, la législation impose que certains contrats soient écrits, signés par les différentes parties, signés d'une certaine façon (légalisation, apostille) ou devant un officier ministériel, afin d'être légalement valables. Les parties devront s'assurer que les contrats intelligents se conforment aux règles de forme imposées par les législations locales. La technologie cryptographique des clés publiques/privées est généralement utilisée pour la signature d'un contrat intelligent. Est-ce que l'utilisation des clés publiques/privées suffit à considérer que la signature du contrat est valable ? Une analyse juridique des circonstances factuelles et de la technologie utilisée aux fins de la conclusion d'un contrat intelligent sera nécessaire afin de déterminer si les moyens utilisés pour la signature électronique sont conformes à la législation en vigueur, et notamment le règlement (UE) n° 910/2014 régissant les signatures électroniques. De plus, deux points me semblent devoir être soulignés. D'une part, les transactions effectuées sur une blockchain publique peuvent l'être sous pseudonyme. Comment vérifier qu'une contrepartie a bien une capacité juridique de signer un contrat intelligent ? Un tribunal pourrait-il considérer qu'un contrat intelligent est valable s'il n'est pas possible de déterminer l'identité d'une partie ? En outre, si un litige surgissait en ce qui concerne un contrat intelligent, comment une partie lésée pourrait-elle identifier l'autre partie pour intenter une action en justice contre elle ? Ce sont là des préoccupations importantes. D'autre part, par analogie avec les contrats d'adhésion, les tribunaux s'assureront, qu'avant la formation du contrat, le consommateur a eu accès aux dispositions du contrat, en aura pris connaissance avant d'y adhérer en cliquant sur le bouton « J'accepte ». Lorsque le code est le contrat, les parties, et plus particulièrement les clients profanes en programmation, auront des difficultés à prouver qu'elles ont eu un consentement éclairé au moment de l'acceptation et qu'elles avaient une parfaite compréhension de l'objet du contrat. Le code étant un langage spécifique, le professionnel devra donc systématiquement mettre à disposition du

^ Edouard Viguier

Juriste de formation (Panthéon-Assas) et spécialiste des questions de sécurité et de défense, Edouard Viguier a rejoint l'aventure de KINGERI pour apporter ses compétences d'analyste, sa passion pour les développements de la blockchain, et sa connaissance du droit.

consommateur une traduction du code en langage naturel. Que se passera-t-il si un contrat intelligent n'est pas assorti d'une traduction en langage naturel ou que la version code est différente de la version en langage naturel ? Les parties devront s'accorder pour déterminer la version (code ou langage naturel) qui prévaudra en cas de litige. En l'absence d'une version en langage naturel, les tribunaux seront enclins à désigner un expert pour déterminer la signification du code. Enfin, l'émergence des contrats intelligents pourrait être perçue par le législateur comme une opportunité de renforcer la protection du consommateur. Il pourrait exiger des professionnels qu'ils codent certaines dispositions dans les contrats intelligents conclus avec des consommateurs.

C. R. : Si le contrat est mal "encapsulé" dans des lignes de code, qui sera responsable d'un point de vue juridique ?

E. C. : La question de la responsabilité est intrinsèquement liée à la gouvernance de la blockchain, en d'autres termes la personne morale qui organise les droits et pouvoirs de chacun afin d'assurer le bon fonctionnement de l'ensemble, en ce y compris la sécurité du système d'information qui sous-tend l'ensemble des opérations de la blockchain. À ce titre, on rappellera un exemple de smart contract qui a mal tourné suite à une erreur de programmation en juin 2016 de « The DAO » avec un transfert « illicite » d'environ 50 millions de dollars. Vers qui se seraient retournées les personnes lésées si la hard fork, qui est une modification de l'historique des transactions de la blockchain (votée par un consensus de moins de 20 % dans un délai de 27 jours) n'avait pas bloqué le processus ? Juridiquement, on doit toujours avoir une personne responsable. Sans cela, comment avoir confiance ? Ceci explique pourquoi les projets de blockchain les plus aboutis reposent sur des blockchains dites de consortium ou hybrides, dont le domaine bancaire et financier nous donne des exemples, à mon sens, les plus effectifs, ou sur des blockchains privées. Par ailleurs, on pourrait penser à la responsabilité de l'éditeur du logiciel ; or, on est ici en présence de logiciel libre, sans éditeur au sens juridique et face à la « communauté » sur laquelle on n'aura pas de prise à défaut d'identification de l'auteur du dommage, c'est-à-dire un sujet de droit.

A. T. : En l'état actuel du droit positif, il n'y a, selon moi, pas de réponse formelle. Nous pourrions, en revanche, imaginer la chaîne des responsabilités possibles comme étant la suivante : le smart contract mal encapsulé dans les lignes de code autorise une action par la partie qui subit un dommage. Cette partie engage une action en réparation de son préjudice à l'encontre de son cocontractant direct qui disposerait, ensuite, par le biais d'une action récursoire, d'un moyen de se retourner contre l'auteur responsable de cette erreur. Il s'agira ensuite – mais là sera la réelle problématique – de retrouver celui qui est à l'origine du mauvais « encapsulage » et de répartir les niveaux de responsabilités entre chacun des intervenants. De manière générale, il s'agira plus vraisemblablement du programmeur, mais les parties ou d'éventuels conseils pourraient également avoir participé de près ou de loin à la genèse de cette erreur.

^ Arnaud Touati

Arnaud Touati est cofondateur du cabinet Alto Avocats spécialisé dans l'accompagnement des startups. Fort de son expertise dans le lancement et l'accompagnement d'entreprises innovantes, il a développé une expertise dans le domaine des nouvelles technologies, et plus particulièrement de l'intelligence artificielle, de la robotique et de la blockchain.

B. C. : Les tribunaux chercheront vraisemblablement le niveau de contrôle que les parties ont sur le programmeur et quel a été le partage des tâches/responsabilités entre les parties au contrat et les programmeurs. À considérer que le « code est le contrat », le tribunal pourrait être enclin à traiter une erreur de code de la même manière qu'il le fait pour une erreur matérielle manifeste (ou un mot/une phrase manquant (e)). Il pourrait corriger l'erreur de programmation, et ce, d'autant plus que la version en langage naturel (laquelle serait exempte d'erreur) du contrat prévaut. Pour parer aux incertitudes liées à des erreurs de programmation, il est important que les parties définissent en amont les diligences devant être accomplies par tous, les clauses limitatives ou exonératoires de responsabilité, ainsi que préciser les cas de force majeure (indisponibilité du réseau, corruption de données pendant le transport ou l'hébergement, cyber intrusion, cyber attaque, etc.). Il incombera au juge d'analyser les relations contractuelles entre programmeurs, conseils, parties, tiers de confiance afin de déterminer qui a failli dans l'exécution de ses diligences, et trancher, si partage de responsabilité il y a, le quantum des dommages-intérêts. Des régimes de responsabilité spécifiques pourront s'appliquer (selon que le juriste ou l'informaticien a failli à une obligation de moyen ou de résultat). J'aimerais également ajouter que certains points restent à éclaircir, en dehors même de la question de la responsabilité dans le cas que vous soulevez. Un contrat intelligent encodé sur la blockchain, dès lors qu'il a été mis en mouvement, ne peut plus faire l'objet d'une modification. Or, l'irrévocabilité de l'exécution du contrat intelligent peut soulever un certain nombre de questions. En effet, certaines opérations doivent, en

vertu de dispositions d'ordre public, pouvoir être annulées et faire l'objet d'une réversibilité. Je pense surtout aux nullités qui peuvent avoir différentes causes (incapacité, erreur, dol, etc.). Comment concilier le caractère irrévocable et irréversible d'un contrat intelligent (d'un point de vue opérationnel) avec l'existence de principes juridiques permettant à une partie de résilier un contrat ? Des conseils juridiques appropriés seront nécessaires afin de mettre en place de telles dispositions et évaluer les alternatives existantes. Également, comment procéder à l'exécution forcée d'un contrat si le code ne l'autorise pas ? Concernant le contentieux, à défaut de mention de la « loi applicable », du « tribunal compétent », ou encore d'une "clause d'arbitrage" dans le contrat intelligent, et dans la mesure où un contrat intelligent s'exécute automatiquement (parfois) à l'échelle de systèmes informatiques distribués, il sera très difficile pour un tribunal de déterminer le lieu d'exécution d'une prestation. La détermination de la loi applicable ou du tribunal compétent s'avèreront cornéliens.

C. R. : Les smart contracts sont-ils en train de révolutionner l'industrie du droit ?

E. C. : Les smart contracts ne révolutionneront pas le droit, à tout le moins à l'instant T. Cependant, il faut que les lignes de codes soient écrites en collaboration avec des juristes, qu'elles soient valides au sens du droit des contrats *(V. C. civ., art. 1128)*, qu'elles correspondent à des droits et des obligations découlant de dispositions contractuelles, qu'elles respectent les exigences de forme et de preuve. À défaut, on se trouvera au mieux en prise avec des contrats d'adhésion, et au pire dans une réalité qui n'existe pas et qui n'a jamais existé (nullité). Comment revenir à la situation antérieure si le contrat ne peut être modifié et qu'il est gravé dans le marbre de la blockchain ? Sauf pour des contrats simples, a-t-on déjà vu un contrat exclusivement constitué de clauses conditionnelles, comme dans les instructions des smart contracts avec la fameuse logique informatique « si..., alors... (If..., Then...) » ?

B. C. : Les contrats intelligents nécessitent de nouveaux types de compétences et de diligences pour s'assurer que le code est bien exécutoire et reflète bien la volonté des parties. Les contrats intelligents rendant difficile la transposition de concepts subjectifs ou de normes interprétatives, il y a fort à parier que les juges, médiateurs et arbitres qui auront à traiter de litiges issus de contrats intelligents auront peu d'éléments subjectifs à apprécier. L'irréversibilité des opérations rendra nécessaire la négociation. Plus généralement, et par rapport à l'industrie du droit, des expertises en matière de programmation vont être de plus en plus requises.

A. T. : Les smart contracts sont aux balbutiements de leur développement, et je considère qu'ils ne sont pas encore à un stade susceptible de révolutionner l'industrie du droit. En revanche, il est incontestable que cette innovation peut modifier substantiellement les pratiques et les modèles économiques des professions juridiques, dont notamment celles des notaires et des avocats. Les smart contracts constituent une rupture fondamentale avec les concepts reconnus en matière

^ Éric Caprioli

Éric Caprioli est avocat à la Cour de Paris, docteur en droit, habilitation à diriger des recherches en droit. Il est spécialisé en droit des nouvelles technologies, de l'informatique et de la communication et en droit de la propriété intellectuelle. Il est membre de la délégation française aux Nations-Unies en matière de droit du commerce électronique depuis 1993, et également vice-président de la Fédération des Tiers de confiance du Numérique (FNTC) et du Club des Experts de la Sécurité de l'Information et du Numérique (CESIN). Il est chargé d'enseignement à l'Université Paris II Panthéon-Assas (droit de la sécurité de l'information) et à l'Université de Paris I, Panthéon-Sorbonne (blockchain et banque en ligne).

de responsabilité et de protection du consommateur. Cette technologie ne pourra toutefois être efficace que si la fiabilité des outils utilisés pour les transactions est garantie et que les responsabilités en cas de défaillance sont précisément identifiées. C'est d'ailleurs tout le paradoxe des smart contracts que d'octroyer aux conseils un rôle fondamental, alors même que la technologie blockchain sur laquelle il se forme a justement pour but la désintermédiation ultime !

C. R. : De nombreux médias et articles affirment que la blockchain va « disrupter » de nombreuses industries, et en particulier le secteur financier. Qu'en pensez-vous ? Quelles sont – ou pourraient être – les applications concrètes ? La blockchain apportera-t-elle plus de sécurité et constituera-t-elle un outil efficace pour la compliance dans l'industrie financière ?

Dominic O' Kane : Il est trop tôt pour dire si la blockchain va « disrupter » l'industrie financière. Beaucoup des projets initiaux sont encore en développement et ne seront visibles qu'en 2018. Sur le court terme, je pense que l'impact de la blockchain aura plus à voir avec la standardisation des data. Elle pourrait aussi stimuler les banques à remplacer des systèmes dépassés. S'il y a disruption, elle sera limitée à certaines applications spécifiques où il y a un besoin d'intégrité des données. Les registres d'actifs et livres de compte semblent

constituer l'application la plus évidente. L'introduction, en 2008, de livres de compte distribués, protégés par chiffrement et inviolables, qui utilisent le mécanisme de « proof of work » (« preuve de travail ») afin d'assurer la confiance sans qu'il ne soit besoin de recourir à une autorité centrale, était le parfait exemple de tempête technologique qui rendait possible la crypto-monnaie bitcoin. En effet, on peut avancer que, plus que la blockchain, le « proof of work » était la véritable innovation technologique, dans la mesure où c'était ce mécanisme qui permettait de créer de la confiance tout en se passant d'une autorité centrale. Ceci dit, les besoins de l'industrie financière sont différents de ceux de la crypto-monnaie. Le mécanisme de « proof of work » est probablement trop lent et consommateur d'énergie pour être appliqué facilement au monde de la finance. Et il existe des alternatives. Par exemple, la confiance peut aussi être créée à travers des mécanismes tels que le « proof of stake » (« preuve d'enjeu ou de possession »), limité aux blockchains privées. Mais cela affaiblit l'intégrité de la blockchain et enlève celle-ci du domaine public où plus d'innovations disruptives pourraient apparaître. Une grande partie de la « hype » autour de la blockchain doit être considérée sobrement, et son impact ultime sur l'industrie financière pourrait être moins important que beaucoup ne le pensent.

Je vois deux raisons principales à l'engouement de certaines institutions bancaires pour la blockchain. D'une part, une réponse à la vague de changements réglementaires apparus depuis 2008. Ces changements ont diminué les marges, en générant des coûts que les banques aimeraient réduire. Leurs départements IT peuvent aussi percevoir la blockchain comme une opportunité de remplacer des systèmes hérités du passé, qui sont coûteux et archaïques. Transférer les bases de données communes de la banque vers une blockchain publique fait disparaître le coût de réconciliation et synchronisation des données, en particulier des données de « trade position ». La seconde raison est leur crainte d'être dépassée si les business models dans l'industrie bancaire finissent par être disruptés. Les banques en sont conscientes, et c'est pour cela que nombre d'entre elles prennent part à des consortiums tels que R3, qui inclue maintenant environ 70 des plus grandes institutions financières mondiales. Ceci étant dit, certaines nouvelles idées ont le potentiel disruptif que la blockchain pourrait faciliter. L'une d'entre elles est le smart contract. Les smart contracts pourraient être utilisés afin d'automatiser des process tels que la trade finance, déclencher des obligations, voire créer de nouvelles formes de contrat dérivé. Il y a également un concept émergent d'organisations autonomes décentralisées (DAO) qui sont essentiellement des entités basées sur des règles que de tels contrats pourraient générer. Il existe aussi des domaines de la banque où la blockchain aura un impact plus limité. Par exemple, les tâches spécifiques au domaine bancaire et qui exigent plus des analytiques complexes que des données. Un exemple est le risk management.

En matière d'applications concrètes actuellement développées, je peux citer les systèmes de paiement transfrontaliers, la trade finance, le règlement et la compensation. Pour les paiements transfrontaliers, je pense à Ripple qui travaille avec les banques afin de faire évoluer la manière dont elles envoient de l'argent à travers le monde. L'espoir est ici que le process sera instantané, et non plus une journée ou plus, comme c'est le cas avec des systèmes tels que SWIFT. En éliminant nombre des intermédiaires des systèmes existants, l'objectif est également de réduire les coûts. Ceci est particulièrement important pour les transferts B to B. La trade finance est largement organisée par le biais d'échanges de lettres de crédit et de connaissements entre des parties, selon une certaine séquence, afin que les paiements soient réalisés. Avoir ces documents validés et sécurisés au sein de la blockchain pourrait permettre d'accélérer le process. Barclays a déjà déployé un système interne en ce sens. Enfin, en créant un enregistrement sécurisé et inviolable de la propriété d'actifs financiers, la blockchain peut aussi être utilisée en vue d'assurer beaucoup plus rapidement le règlement et la compensation de titres financiers. Des trades qui prennent généralement 2 à 3 jours pourraient être compensés instantanément, réduisant le risque de contrepartie et éliminant les coûts administratifs. Une application plus disruptive pourrait être utilisée afin de faciliter le process de trading, en recevant les ordres par le biais de smart contracts qui spécifieraient comment le trade doit être exécuté. Un exemple concret de l'application de la blockchain en matière de compensation est la décision prise début 2016 par la Depository Trust and Clearing Corporation de commencer à utiliser la technologie blockchain pour reconstruire sa plate-forme "Trade Information Warehouse" pour la compensation des couvertures de défaillance (« credit default swaps »). On peut débattre sur le fait de savoir si ces applications sont disruptives ou pas. Mais elles pourraient conduire à de nouveaux business models réellement disruptifs.

E. C. : Le terme de rupture (disruption) est purement marketing dans la mesure où les banques disposent des moyens techniques et humains pour absorber les innovations. Elles ont toujours été en pointe dans les communications électroniques depuis les années 70 ; SWIFT, en 1977, constitue un exemple de coopération fondée sur des échanges électroniques. Comment imaginer des Fintech qui se lanceraient seules sur le marché et qui puissent voir les clients de banques adhérer à leurs solutions sans passer par elles en mettant fin à l'intermédiation ? Ce n'est qu'une illusion car les banques (mais aussi les assurances) les financent et elles vont acheter les technologies ou les start-ups, voire créer des partenariats afin de les intégrer dans leurs processus métiers. Au niveau international, il faut signaler le projet R3CEV auquel 60 banques internationales ont adhéré depuis 2014, mais qui vient d'abandonner la blockchain fin février 2017 en raison de ses limites techniques pour les utilisations dans le domaine financier, ou en France, l'initiative LabChain pilotée par la Caisse des dépôts et consignations qui réunit banques, compagnies d'assurances, et start-ups sur des applications telles que la connaissance client ou la gestion des identifiants créanciers SEPA. En second lieu, des applications sur le financement participatif (crowdfunding) doivent être signalées. Mais ce sera sans doute la régulation qui devra être modifiée pour les interventions de l'ACPR et de l'AMF en matière de blockchain. Il est à souligner que ces projets fonctionnent en blockchain de consortium. L'ENISA vient de

publier le 18 janvier 2017 un rapport sur les "distributed ledgers technology" dans le secteur financier. Certains enjeux de cyber sécurité sont classiques (par exemple, gestion des clés, protection de la vie privée, revue des codes informatiques), d'autres spécifiques (par exemple, génération des clés, smart contracts et évolutivité), mais il faudra également prendre en compte les aspects anti-blanchiment et anti-fraude, l'interopérabilité des protocoles de blockchain, et la problématique de la gestion de la vie privée dans le temps. Selon l'ENISA, si la blockchain apporte des réponses positives à certains égards, elle pose d'autres interrogations (notamment juridiques), et tout projet de blockchain dans le secteur financier doit intégrer un questionnement analogue à celui posé au niveau européen (V. *La blockchain dans le secteur bancaire et financier, in Études à la Mémoire de Philippe Neau-Leduc, 2017, à paraître*).

B. C. : Il existe certains défis réglementaires dans l'utilisation de la blockchain au sein des services financiers : identification des clients, lutte contre le blanchiment de capitaux et financement du terrorisme. L'identification des clients impose *a minima* de passer par des blockchains privées et non publiques (la blockchain publique autorisant les transactions sous pseudonyme). Le législateur pourrait exiger que certaines dispositions soient reflétées dans les contrats intelligents avant que les contrats ne puissent être exécutés par les acteurs du marché. Charge aux autorités prudentielles de surveiller les transactions, voire d'autoriser certaines transactions avant leur mise en œuvre. Le législateur devra aussi déterminer dans quelle mesure les autorités prudentielles pourront accéder aux transactions s'opérant via des contrats intelligents encodés sur la blockchain. Il conviendra de prévoir différents niveaux d'accès aux transactions de la blockchain. Les autorités prudentielles devraient pouvoir avoir accès en temps réel aux transactions, aux identités des parties, aux positions et aux valeurs, ainsi qu'au code des contrats intelligents. L'interprétation et l'approbation d'une blockchain et d'un code de contrat intelligent nécessiteront une nouvelle approche réglementaire et de nouvelles compétences et expertises de la part des autorités prudentielles. La coopération nécessaire entre entités régulées et autorités prudentielles sera importante, mais une intégration réussie pourrait renforcer significativement la conformité des activités et des acteurs.

E. C. : Pour moi, efficacité et risques sont à la fois possibles. Tout va dépendre de la constitution (technique) et de la gouvernance (juridique et sécurité) de la blockchain en cause. En effet, il n'existe pas de solution miracle, en dépit de l'utilisation des technologies anciennes et éprouvées, comme une base de données distribuée, un système de signature à clé asymétrique (courbe elliptique) associé à un algorithme de hachage pour assurer l'intégrité des transactions et un mode de fonctionnement en peer-to-peer. Normalement, tous les systèmes de signature électronique fonctionnent avec un organe central de gestion de la sécurité des clés utilisées ; cela permet notamment de gérer les crypto-périodes (quand un algorithme de signature ou de hachage a été attaqué) de validité des clés. Des audits de sécurité et juridiques permettront de détecter les risques de telle ou telle blockchain. Il faut résister au chant des sirènes et

^ Benoît Charpentier

Benoît Charpentier est ancien avocat et ancien directeur juridique. Il est cofondateur et dirigeant de MeilleursHonoraires.com., plateforme d'appel d'offres pour sélectionner son avocat. Il est également fondateur et dirigeant de Charpentier Consulting, société de conseil à destination des professionnels du droit. Il a créé il y a près de deux ans le groupe "Legal Innovation and Technology" sur LinkedIn, groupe qui compte actuellement 7300 membres actifs et auquel il contribue régulièrement.

rester sur les analyses de risques classiques. Je pense qu'il n'y a nul besoin d'un cadre règlementaire plus souple ou spécifique, sauf peut-être en matière fiscale afin d'inciter les Fintech ou s'il existe des blocages juridiques insurmontables (ou adaptation des règles de régulation), car il faut laisser les usages se créer avant de réguler. La régulation ne doit jamais intervenir en amont, mais en aval des usages, et seulement en cas de dysfonctionnement ou d'abus. Or, à ce stade, les usages n'existent pas encore étant donné que l'on n'en est qu'aux expérimentations, sauf « The Dao » pour le crowdfunding. Une régulation native, c'est-à-dire qui précède l'usage est le plus souvent désastreuse et ne sert qu'à faire de la communication. En revanche, lorsqu'elle intervient a posteriori (par exemple, les lois sur l'Internet en 2000 et 2004, la directive de 2000, etc.), au contraire, la régulation accompagne les usages.

D. O'K. : La blockchain est essentiellement inviolable, permettant un enregistrement hautement sécurisé des transactions. Comme je l'ai déjà dit, il y a un coût, dans la mesure où le process de minage présente une difficulté computationnelle et utilise nombre de ressources informatiques. Le mécanisme de « proof of work » est également lent et constitue potentiellement un goulot d'étranglement pour la croissance de la blockchain. Par exemple, le bitcoin valide uniquement des nouveaux blocs de transaction toutes les 10 minutes. Et une transaction n'est réputée confirmée qu'après que 6 blocs aient été confirmés, ce qui signifie qu'il faut attendre 1 heure. Ceci est trop lent pour la plupart des applications financières. Des voies alternatives et plus rapides existent. Une alternative majeure réside

dans le mécanisme de « proof of stake ». Dans cette approche, un système de vote est utilisé pour valider les blocs où l'identité et l'enjeu (ou la possession) des votants au sein de la blockchain est pris en considération. Le principe sous-jacent est que les participants ayant un intérêt dans l'intégrité de la blockchain seront motivés à valider uniquement l'addition de transactions légitimes. Ce mécanisme est potentiellement moins sécurisé que celui de « proof of work ». Il pourrait conduire à l'utilisation accrue de blockchains privées permettant uniquement aux membres d'une certaine communauté d'accéder à la blockchain, ce qui amènerait une couche supplémentaire de sécurité. Bien sûr, la blockchain est porteuse de menaces en matière de sécurité. Ainsi, si une faille dans le code existe, il pourrait être utilisé malicieusement afin de dérober des actifs ou de saper la blockchain. Une telle possibilité est néanmoins atténuée par la nature "open source" de la blockchain publique, permettant à de nombreuses paires d'yeux de vérifier le code et d'identifier et régler toute faille avant que ce code ne soit opérationnel. Dans l'hypothèse d'incidents, les blockchains utilisées dans le domaine financier vont requérir des règles et des mécanismes de gouvernance capables de réponses rapides, tels que la mise à jour d'un logiciel, le retrait des transactions invalides, etc. Le hack récent sur une DAO Ethereum, qui avait été créée afin de fonctionner comme un fonds de capital-risque, montre bien que les craintes en matière de sécurité sont véritables. Mais il faut noter que ce n'est pas la blockchain elle-même qui a été hackée, mais un ensemble de smart contracts pour une DAO spécifique qui avaient été mal écrits, créant une faille exploitée par un hacker. Finalement, l'utilisation d'une seule solution technologique - ce que la blockchain encourage - représente un risque systémique. Si jamais cette technologie est défaillante, alors ses implications pour le système financier pourraient être significatives et généralisées.

Pour les régulateurs financiers, la blockchain peut être perçue comme un pas vers plus de transparence. Fournir aux régulateurs les clés qui leur permettront d'analyser les données cryptées doit être fait de telle sorte que l'anonymat et le cryptage que la plupart des acteurs rechercheraient dans une blockchain publique, ne soient pas affaiblis. La blockchain va aussi certainement exiger à la fois des changements dans la réglementation, et conduire à de nouvelles lois. Pour commencer, elle peut constituer un outil très utile pour la compliance. L'une des exigences coûteuses pour les paiements transfrontaliers est l'Anti-Money Laundering, KYC. Il y a eu des propositions pour une blockchain universelle qui génèrerait une liste de clients, accompagnée des détails de leur identification vérifiée (passeport et biométrie), et de leur compliance à jour au regard des règles. Cette liste pourrait être consultée en tant que partie du process de paiement, permettant ainsi aux banques de réduire considérablement les coûts de maintenance de leur base de données, et d'accélérer le process de paiement. Ceci étant dit, on peut s'interroger sur le fait de savoir si la blockchain est réellement nécessaire si l'objectif est simplement de créer une base de données centrale de clients. Il y a d'autres implications importantes. Avec une blockchain globale, comment les différentes lois sur le secret des données seront-elles prises en compte ? Par exemple, comment les clients pourront-ils demander réparation s'ils pensent qu'il y a des erreurs dans la blockchain, telle que la base de données KYC ?

^ Dominic O'Kane

Dominic O'Kane est professeur affilié en finance à l'EDHEC Business School. Ses recherches portent sur la régulation financière et les technologies dans le secteur de la finance. Avant de rejoindre l'EDHEC en 2007, il a passé 12 ans dans l'industrie des services financiers, où il a notamment occupé la fonction de Managing Director et Head of Quantitative Research chez Lehman Brothers. Il était responsable du développement des modèles d'évaluation. Avant cela, il a travaillé chez Salomon Brothers. Il est titulaire d'un doctorat en physiques théoriques de l'Université d'Oxford.

B. C. : Pour ma part, j'aimerais, toutes industries confondues, partager ce que je considère comme étant, d'une part, les avantages et opportunités de la blockchain et des smart contracts, et, d'autre part, les inconvénients et limites. Pour les avantages : l'automatisation, la réduction des coûts transactionnels, la réduction de risque, le fait que le législateur pourrait exiger la présence dans les contrats intelligents de dispositions assurant un certain degré de protection de parties faibles dans des secteurs réglementés (investisseurs, consommateurs). Pour les inconvénients et limites : le code est un langage rigide qui ne laisse que peu de place à la subjectivité et à l'interprétation, les erreurs de programmation, la maîtrise du code qui nécessite un certain degré d'expertise, les applications concrètes qui sont encore limitées, le contrat intelligent qui ne peut être utilisé que pour des contrats simples et standardisés, la difficulté de mettre en place une surveillance prudentielle, les interactions limitées du contrat intelligent avec le "monde réel", l'équation économique (coût/bénéfice) hasardeuse, le respect des règles de forme et l'irréversibilité des transactions.