Blockchain et professions réglementées

Emmanuel Netter, maître de conférences HDR en droit privé
Centre de droit privé et de sciences criminelles d'Amiens (EA 3911)[1]

« Les notaires sont des zombies. Ils sont morts, mais ne le savent pas encore »[2]. À défaut du sens de la nuance, reconnaissons à ce fondateur de start-up le sens de la formule. La technologie responsable de ces bouleversements annoncés est celle des blockchains. « La » blockchain, comme elle est souvent dénommée, a pu être définie comme une technique « de stockage et de transmission d'informations, fonctionnant grâce à un système distribué et des procédés cryptographiques. Ce grand journal public, contenant l'historique de tous les échanges effectués entre les utilisateurs depuis sa création, est partagé et constamment vérifié ; son mode de gouvernance, par consensus distribué, le rend en principe infalsifiable. Chaque utilisateur peut ainsi participer à son bon fonctionnement en vérifiant la validité de la chaîne de blocs de transactions et prendre connaissance des transactions effectuées, ce qui en garantit la publicité et la traçabilité »[3]. Aucun processus informatique ne peut être considéré comme parfaitement sécurisé, mais postulons pour la suite de cette étude que le niveau de fiabilité atteint par une chaîne de blocs est très élevé.

Il est à présent bien connu que la cryptomonnaie *Bitcoin* a constitué la matrice de cette technologie. Assurer la tenue de comptes dans une devise revient à tenir un registre mondial, permanent et exhaustif des transactions dans lesquelles cette monnaie est échangée. Deux grandes méthodes sont alors envisageables. La première, classique, consiste à s'en remettre à un ou plusieurs tiers de confiance – en l'occurrence les banques. La seconde, innovante, dissémine dans les machines de milliers d'utilisateurs des automatismes associés à des techniques de chiffrement, capables de se coordonner sans la moindre intervention centralisée pour stocker des morceaux du journal et en vérifier l'intégrité à tout instant. La confiance n'est plus localisée ni personnifiée : vaporisée en gouttelettes microscopiques, elle se trouve partout à la fois.

À ce stade de la démonstration, les notaires peuvent encore dormir tranquilles et ce sont les établissements de crédit, les prestataires de services d'investissement et autres chambres de compensation qui sont poussés à revoir leurs modèles en profondeur. Il n'est donc pas surprenant

1 L'auteur souhaite remercier Me Mathieu Fontaine, rapporteur sur les questions de nouvelles technologies pour le Congrès des notaires, qui lui a accordé de précieux entretiens téléphoniques sur le sujet ici traité. Les propos tenus ici ne sauraient toutefois l'engager.

2 J. Hamel, fondateur « d'Académie Bitcoin », cité par D. Jung, « Les notaires sont-ils condamnés à disparaître ? », article droit-inc. com du 5 avril 2018.

3 C. Zolynski, « La *blockchain* : la fin de l'ubérisation ? », *Dalloz IP/IT*, 2017, p. 385.

que les premières empreintes laissées par ces techniques dans nos textes législatifs se trouvent dans le Code monétaire et financier ainsi que dans le Code de commerce[4].

Mais en réalité, le fonctionnement qui vient d'être décrit permet de figer dans le marbre numérique une information quelconque. C'est alors un vaste renouvellement des techniques probatoires qui se dessine. Ainsi, conserver une description horodatée d'une création de l'esprit permettrait à un auteur de démontrer aux tiers l'antériorité de son droit. Une chaîne de blocs pourrait servir de registre de publicité foncière. On pourrait encore confier à sa mémoire supposée infaillible le souvenir de la conclusion d'un contrat et de son contenu. La menace est à présent identifiée. La confiance que suscite aujourd'hui une preuve isolée ou un registre pris dans son ensemble tient souvent, aujourd'hui, à l'intervention de professionnels du droit, soumis à un lourd statut qui garantit tout à la fois leur compétence et leur intégrité. Cette confiance aujourd'hui placée dans les hommes pourrait être demain déléguée à la technique, qu'on présente comme plus rapide, moins chère et d'une fiabilité inégalée.

Les promesses des chaînes de blocs ne s'arrêtent pas là. Certains ont imaginé graver dans le registre, de façon irréversible, les termes d'un accord entre deux parties appelé *smart contract*[5]. L'exemple suivant se rencontre en doctrine[6]. Un contrat de location saisonnière est transformé, à l'aide d'un langage de programmation, en lignes de code aux termes desquelles la blockchain vérifiera, chaque lundi, que le loyer a bien été viré par le locataire sur le compte du bailleur. Si tel n'est pas le cas, un ordre sera envoyé à la serrure connectée du logement et la porte ne s'ouvrira plus. La phase d'exécution des actes juridiques se trouverait déléguée à son tour à la technique, et la machine pratiquerait expulsions et saisies plus sûrement qu'un huissier.

On imagine les professionnels du droit anxieux, si ce n'est pétrifiés par les perspectives qui viennent d'être dressées. Voici pourtant les notaires qui annoncent en fanfare le lancement de leur propre blockchain[7]. Certains auteurs expliquent ainsi que ce n'est pas une « désintermédiation », mais une « réintermédiation » du droit qui est à l'oeuvre[8]. Plutôt que d'être évincés par cette technologie nouvelle, les professions du droit souhaiteraient s'y intégrer et en améliorer la mise en œuvre.

---

4 Art. L. 223-12 CMF ; art. L. 228-1 al. 6 C. com. dans sa version entrant en vigueur au 1er juillet 2018.

5 Sur ce thème, V. not. C. Zolynski, « Blockchain et smart contracts : premiers regards sur une technologie disruptive », *RDBF*, n° 1, janvier 2017, dossier 4 ; G. Guerlin, « Considérations sur les smart contracts », *Dalloz IP/IT*, octobre 2017 ; E. Caprioli et al., « Blockchain et smart contracts : enjeux technologiques, juridiques et business », *Cahiers de droit de l'entreprise*, n° 2, mars 2017, entretien 2 ; T. Verbiest, « Quelle valeur juridique pour les smart contracts ? », *RLDA*, 2017, n° 129 ; A. Touati, « Tous les contrats ne peuvent pas être des smart contracts », *RLDC*, 2017, n° 147.

6 A. Touati, « Tous les contrats... », art. préc.

7 Annonce publique de M. D. Coiffard, président du CSN, le 15 mars 2018.

8 M. Mekki, « Blockchain, smart contracts et notariat », Solutions notaires hebo, Francis Lefebvre, 2018, n° 10.

Il nous faudrait par conséquent déterminer si les évolutions qui se dessinent seront, pour les professions réglementées, destructrices ou facteurs de progrès. Mais une autre question, plus fondamentale encore, mérite d'être posée : le bouleversement annoncé aura-t-il bien lieu ? Pour prendre la juste mesure de son impact sur le monde du droit, il faut présenter le potentiel et les limites de la technologie blockchain (I). À cette approche générale succédera une mise en situation de ces techniques à l'aide de quelques illustrations particulières (II).

I – Caractéristiques générales de la technologie blockchain

Un vaste écosystème s'est développé autour des chaînes de blocs. De jeunes entreprises et des armées de consultants se sont attachées, en France et dans le monde, à convaincre de leurs mérites. Ils sont réels. Mais un examen attentif révèle d'une part que cette technique ne peut pas tout faire, d'autre part que ce qu'elle sait faire est parfois réalisable dans de meilleures conditions – de rapidité, de coût – par d'autres moyens informatiques. Pour mieux comprendre l'intérêt et les limites de ce grand registre distribué, demandons-nous ce qu'il enregistre (A) et comment il l'enregistre (B).

A – L'objet de l'enregistrement

Une blockchain se nourrit d'informations. Elle les capture, les dépose en son sein et les y conserve durablement. Mais ces informations, comment y accède-t-elle ? Comment s'assure-t-elle de leur véracité, de leur conformité au réel ? Une blockchain est myope. Elle ne voit clairement que ce qui passe à sa portée ; le reste est flou. Ce n'est pas un hasard si son usage optimal consiste à assurer la tenue de comptes en devises numériques. Pour accomplir cette tâche, elle n'a besoin que de données auxquelles elle a immédiatement accès : l'utilisateur A lui dit qu'il souhaite virer 0,03 bitcoin à l'utilisateur B, et il faudra actualiser les soldes des comptes en conséquence. Pourquoi ces parties souhaitent-elles s'échanger cette valeur ? Cette question est pour elle sans réponse. Cela reste vrai si l'on ajoute à une blockchain une fonctionnalité de *smart contract*. Prenons l'exemple du contrat d'assurance Fizzy développé par Axa[9]. Un passager peut se garantir contre le retard d'un vol transatlantique de plus de deux heures et, si le sinistre se produit, être indemnisé de manière purement automatisée. La police d'assurance une fois conclue est traduite en code informatique et figée dans une chaîne de blocs. Mais pour savoir si le vol considéré est arrivé avec un retard tel que l'indemnisation doit être déclenchée, la blockchain doit accéder à une base de données recensant les atterrissages, qui lui est extérieure. Puis, s'il lui faut payer une indemnité en euros et non en cryptomonnaies, elle doit donner un ordre de virement qui sera exécuté par des banques

9 fizzy.axa.

traditionnelles. Ces interfaces avec le reste du monde sont appelées « oracles » par la pratique. Le recours à ces systèmes devient rapidement indispensable dès que l'on confie à une blockchain des missions sophistiquées. Le registre ne parvient pas à fonctionner en autarcie. Or, ces tiers qu'il interroge pourraient se tromper, voire mentir. Du point de vue de la confiance qu'il inspire, le processus d'ensemble a donc la valeur du plus faible de ses maillons.

Un exemple particulièrement important d'oracle, pour le juriste, est celui qui permettrait la vérification par une blockchain de l'identité des intervenants. Il s'agit là encore d'une information issue du monde « hors ligne », à laquelle le registre décentralisé ne peut accéder par lui-même[10]. Une modalité technique parmi d'autres envisageables consiste à utiliser des cartes d'identité dotées d'une puce électronique, comme le fait la Belgique, ce qui permet à chaque citoyen d'utiliser en ligne une clé de chiffrement qui lui est propre. Il insère sa carte dans un lecteur connecté à son ordinateur et révèle un secret connu de lui seul – typiquement, un code PIN – et fournit ainsi à une blockchain ou à tout autre service en ligne une preuve crédible de son identité. Mais la délivrance initiale de la carte à puce requiert bien l'intervention d'un tiers hors-ligne (un service de l'État, un notaire, un huissier…) qui aura procédé aux vérifications nécessaires.

Une blockchain a donc besoin « d'oracles ». Ce n'est pas tout. S'il s'agit d'inscrire dans le registre non pas le constat d'un fait brut, mais un jugement de valeur, il faudra faire appel à un oracle justifiant d'une compétence lui permettant de porter ce jugement. Par exemple, si l'on veut faire constater par le registre non pas seulement « A et B déclarent avoir passé un contrat de vente immobilière », mais « A et B se sont valablement vendus un bien immobilier », le recours à un « oracle » juriste ne peut être évité.

Le potentiel et les limites de la technologie blockchain se révèlent donc dans le type d'information qu'elles sont aptes à saisir. Ils apparaissent, par ailleurs, dans la manière dont l'information est cristallisée.

B – Le mode d'enregistrement

Deux chercheurs suisses en informatique ont proposé une étude intitulée « Avez-vous besoin d'une blockchain »[11] ? Ils rappellent qu'il existe plusieurs variantes de cette technologie. La plus connue, celle qui est au fondement du Bitcoin, est dite « sans autorisation »[12]. Chacun est libre de la rejoindre, d'en lire le contenu, de participer au processus d'écriture dans le registre. Son fonctionnement requiert une débauche d'énergie à mesure qu'elle grandit : pour valider l'écriture d'un nouveau « bloc » de la chaîne, les ordinateurs participant au système – les « mineurs » -

10 I. Renard, « Fonctionnement de la Blockchain », RDBF, janvier 2013, dossier 3.
11 K. Wüst et A. Gervais, « Do you need a blockchain ? », 2017 : https://eprint.iacr.org/2017/375.pdf.
12 « Permissionless ».

doivent travailler à la résolution de problèmes mathématiques de plus en plus complexes. Cette puissance de calcul entraîne une dépense électrique et a par conséquent un coût ainsi qu'un impact environnemental. Les participants sont cependant incités à contribuer au processus en percevant une récompense – par exemple des fractions de bitcoins - si leur machine est la première à résoudre l'énigme soumise à tous. Les autres formes de blockchain sont dites « à autorisation » : une entité aura décidé à l'avance d'attribuer le droit d'écrire dans le registre à un nombre limité d'intervenants. Ces chaînes « à autorisation » peuvent ensuite être « publiques » si tout le monde a le droit d'aller lire le registre, ou « privées » si même la simple consultation des informations qui y figurent est réservée à un cercle fermé. Pour schématiser, les chaînes « à autorisation » sont beaucoup moins gourmandes en ressources – et bien plus rapides – car elles n'organisent pas une compétition entrent des milliers d'ordinateurs pour valider l'écriture d'un bloc : quelques machines triées sur le volet recherchent un consensus entre elles seules.

D'après les chercheurs suisses, il n'est justifié d'utiliser une blockchain « sans autorisation » que dans des cas précis : s'il y a plus d'une personne autorisée à écrire dans le registre, que de surcroît il n'est pas possible d'avoir recours à un tiers de confiance et qu'enfin il n'est pas possible de savoir par avance qui doit avoir le droit d'inscrire des informations.

Si une seule entité dispose du droit d'écriture, s'il est possible de faire appel à un tiers de confiance, ou si le droit d'écrire dans le registre est conféré à un nombre fini d'entités qu'on peut considérer comme fiables, une blockchain n'a aucune utilité. La ou les personnes dotées du pouvoir d'écriture utiliseront une base de données classique, qui est une technique maîtrisée depuis des décennies. Elle peut être chiffrée et dupliquée pour la protéger contre des attaques de tiers.

Restent les situations où les blockchains « à autorisation » sont pertinentes. Il s'agit selon Messieurs Wüst et Gervais des hypothèses, assez rares, où un cercle fermé d'utilisateurs doit écrire dans le registre, mais ces entités ne sont pas fiables et se méfient les unes des autres.

Conservant à l'esprit la dépendance des blockchains à l'égard « d'oracles » et l'existence de techniques concurrentes, comme les bases de données centralisées, qui se révèlent plus pertinentes en de nombreuses hypothèses, nous pouvons à présent étudier quelques scénarios concrets.

II – Applications particulières de la technologie blockchain

Les blockchains « sèches » intéressent le domaine des preuves (A). Dotées d'une couche logicielle supplémentaire, elles peuvent jouer un rôle en matière d'exécution des contrats (B).

A – En matière de preuves

Envisageons tout d'abord la preuve d'événements isolés. La technologie blockchain est bien adaptée à la preuve d'antériorité en matière d'oeuvres de l'esprit, et elle est déjà utilisée à cette fin[13]. Il doit s'agir d'une blockchain « sans autorisation », le modèle le plus pur, puisqu'on ne peut déterminer *a priori* qui sera amené à écrire dans le registre. La vulnérabilité de la chaîne lorsqu'il lui faut s'informer sur le monde qui l'entoure n'est pas un obstacle, ici : si une personne a été capable de lui soumettre pour horodatage une œuvre de l'esprit, plusieurs mois avant qu'elle ne soit diffusée par autrui, cela constitue en soi une information accréditant une antériorité au profit de l'enregistrant. Le problème est très différent si l'on entend dresser un « constat » d'une situation temporaire, comme le ferait un huissier de justice, par exemple la présence d'un individu en un certain lieu à une certaine date. Si l'on soumet une photographie à une blockchain via une application pour téléphone mobile, il est très difficile de déterminer si l'image n'est pas en réalité datée d'il y a deux jours, ou de trois mois. « L'oracle » que constitue l'application peut mentir. La sécurité apportée par le tiers de confiance qu'est l'huissier ne peut pas être véritablement égalée dans une telle hypothèse.

Envisageons ensuite les preuves collectives que constituent, en quelque sorte, les registres. Imaginons qu'on entende confier à une blockchain la gestion d'un registre particulièrement crucial, celui de la publicité foncière. Pourra-t-on alors évincer les notaires des transactions immobilières, comme certains l'espèrent ? Il faudrait que la chaîne accède à nombre d'informations objectives du monde « hors ligne » : elle doit savoir qui sont véritablement les parties ; s'il existe une décision les plaçant sous un régime de protection des majeurs ; si les acheteurs ont constitué un dépôt de garantie ; pour le cas où ils prétendraient, postérieurement au compris de vente, n'avoir pas trouvé d'établissement de crédit pour les financer, la chaîne doit vérifier s'ils ont procédé à des recherches suffisantes afin de savoir si une clause pénale doit jouer ou non... Il faudrait aussi et surtout que le registre distribué soit capable de porter des jugements de valeur experts : de discerner si les consentements sont éclairés, de mesurer la compétence des intervenants pour leur expliquer autant que nécessaire les parties techniques de l'acte… autant de missions qu'une blockchain est évidemment incapable d'accomplir[14].

Mais pourquoi alors ne pas faire appel aux notaires comme « oracles », en leur conférant le pouvoir d'écrire dans une chaîne de blocs « à autorisation » ? Cela ne garantirait-il pas le stockage le plus sûr et le plus durable d'informations cruciales ? À suivre Messieurs Wüst et Gervais, cette solution ne s'impose pas d'évidence. Nous nous trouvons dans une situation où un nombre limité de

13 Par exemple blockchainyourip.com.
14 En ce sens : M. Mekki, « Les mystères de la blockchain », D., 2017, 2160.

personnes sont habilitées à écrire dans le registre, et où elles devraient normalement toutes être considérées comme fiables – qu'il s'agisse d'agents de l'État ou, dans un avenir prévisible, des notaires eux-mêmes. La plus-value d'une blockchain, même dans sa version « à autorisation », reste à démontrer dans de tels cas.

Terminons cette étude en évoquant l'usage des *smart contracts*.

B – En matière d'exécution

Le *smart contract* se présente au premier abord comme un contrat d'un genre nouveau. Pour sa bonne exécution, il pourrait se passer d'huissiers de justice et, plus radicalement, de toute la chaîne située en amont et qui aboutit à la délivrance d'un titre exécutoire. C'est que le *smart contract* contourne en réalité le système juridique dans son ensemble : il n'en est pas issu, et gravite au sein d'un ordre normatif numérique qui lui est propre. Rien ne dit que les lignes de code qui le matérialisent constituent le décalque d'un contrat au sens juridique du terme, de surcroît valable et méritant le concours de la force publique pour son exécution.

Le *smart contract* se conçoit bien dans les quelques sphères professionnelles où l'on paie d'abord et l'on discute ensuite : ainsi du monde des garanties autonomes à première demande. Ailleurs, il risque d'être un instrument d'iniquité et de pression du fort sur le faible[15]. Certains pronostiquent par conséquent que les *smart contracts* renforceront paradoxalement le rôle des avocats[16]. Dans le meilleur des cas, ils interviendront en amont pour garantir aux parties que leur projet contractuel, d'abord conforme au droit, est ensuite traduit de manière adéquate en code informatique. Dans la pire des hypothèses, ils ne seront consultés qu'en aval, lorsqu'une partie convoquera tardivement le droit en espérant reprendre ce que la machine lui aura pris.

**

Les blockchains provoqueront-elles des ajustements au sein des professions du droit ? C'est certain. De véritables bouleversements ? C'est une éventualité. Leur éradication ? C'est exclu.

15 En ce sens, G. Guerlin, art. préc.
16 A. Touati, « Blockchain et smart contracts », Cah. dr. de l'entreprise, mars 2017, entretien 2.