

## BLOCKCHAIN : LES ENJEUX EN DROIT FRANÇAIS



Gilles KOLIFRATH &  
Avocat



Mélanie GOUPY  
Juriste

La « *Blockchain* », ou littéralement « chaîne de blocs », est une technologie inventée en 2008 par un anonyme connu sous le pseudonyme de Satoshi Sakamoto. Son fonctionnement est *a priori* simple : il s'agit d'un historique électronique immuable et inviolable de transactions conclues au fil de l'eau, distribué entre plusieurs intervenants sur le réseau. L'ensemble de ces transactions constitue ensuite une base de données qui recense tous les échanges effectués entre les différents intervenants depuis sa création.

Pourquoi le terme « *Blockchain* » ? Il illustre en lui-même le fonctionnement de la technologie : un ensemble de données ou de transactions (« *block* »), combiné à un historique (« *chain* »). Ce terme traduit l'ajout de blocs au sein d'une chaîne, qui s'allonge au fur et à mesure des interventions des acteurs de la *Blockchain*, ou de l'ajout de nouvelles données. Il s'agit toutefois de porter une attention particulière aux termes et de distinguer LA *Blockchain* comme technologie et UNE *blockchain* spécifique que toute organisation pourra potentiellement déployer (par exemple, Bitcoin ou Ethereum)<sup>(1)</sup>.

La technologie *Blockchain* est très prometteuse, tant ses applications pratiques sont variées. C'est d'ailleurs la raison pour laquelle, depuis maintenant quelques années, elle fait l'objet d'un très fort intérêt, tant de la sphère privée (à l'image des banques ou des entreprises d'assurance) que de la sphère publique (les gouvernements). C'est dans ce cadre que le Trésor a récemment proposé une ordonnance sur la transmission de titres grâce à la *Blockchain*, qui n'est que l'une des nombreuses applications concrètes de cette technologie.

Le corollaire naturel de cette multitude d'applications est l'encadrement juridique d'une telle technologie. Si la définition de la *Blockchain* tend aujourd'hui à s'affiner (I), ses applications, tant juridiques, qu'économiques et financières, pourraient révolutionner les rapports entre ses intervenants (II). C'est la raison pour laquelle un cadre juridique doit nécessairement émerger (III).

1. Comprendre la *Blockchain* – Livre blanc Uchange, janvier 2016, p. 11.

## I. Définir la *Blockchain*

Afin de définir la *Blockchain* et d'en tirer une définition juridique (A), il convient d'expliquer son mode de fonctionnement (B).

### A. En pratique

La *Blockchain* est un logiciel qui s'exécute sur un ordinateur appelé « nœud ». Chaque nœud est relié au réseau et peut soumettre et recevoir des transactions. Les nœuds collectent et regroupent les transactions validées dans un bloc. Les blocs composant la *Blockchain* sont des conteneurs numériques à l'intérieur desquels sont stockées des informations variées : transactions, contrats, titres de propriétés, œuvres d'art... Ces blocs, pris dans leur ensemble, forment une base de données semblable aux pages d'un grand livre de comptes<sup>(2)</sup>. Ce « livre de compte » a vocation à contenir toutes les données utilisées par les intervenants depuis sa création.

La technologie de la *Blockchain* repose sur deux grands principes qui font sa force :

- la décentralisation : il n'y a pas d'organe de contrôle de la *Blockchain* ;
- la sécurité : elle est en principe infalsifiable.

La *décentralisation*, ou désintermédiation, résulte de l'absence de tout organe central ou organe de contrôle. Cela est rendu possible car la *Blockchain* n'est pas « hébergée » par un serveur unique central mais par une partie des intervenants, qui peuvent vérifier à tout instant la validité de la chaîne de blocs.

La question est donc la suivante : comment fonctionne ce réseau décentralisé ? En d'autres termes, comment les intervenants assurent-ils la gestion de la *Blockchain* ? La réponse réside dans le processus de validation de l'intégration d'une donnée au sein de la *Blockchain*, qui s'appelle le « minage » (ou « *mining* » en anglais). Avant qu'un nouveau bloc soit ajouté à la chaîne, il doit être validé par plusieurs intervenants sur le réseau (appelés les mineurs en français et « *miners* »

2. *Ibid.*

en anglais) qui vérifient sa conformité en résolvant un problème cryptographique (une sorte de problème mathématique) complexe. Tous les mineurs ont le même objectif : assurer le fonctionnement régulier de la *Blockchain*.

La complexité du calcul dépend de la capacité de calcul des intervenants qui doivent garder un temps de résolution d'environ 10 minutes<sup>(3)</sup>. Le résultat du calcul est vérifiable par le groupe de mineurs grâce à ce qu'on appelle le « *Proof of Work* », qui est le résultat du problème à résoudre pour qu'un nouveau bloc soit ajouté. En pratique, lorsqu'un mineur arrive à résoudre le problème, il transmet son résultat aux autres mineurs, qui arrêtent alors d'essayer de résoudre le problème et s'accordent uniquement sur la validité de la « *Proof of Work* ». Lorsque plus de la moitié des mineurs valident la « *Proof of Work* » (cette action s'appelle le « consensus »), celui-ci vient s'ajouter à la *Blockchain*<sup>(4)</sup>.

Nous retiendrons donc que l'un des principes qui irriguent le fonctionnement de la *Blockchain* est le consensus : personne ne fait confiance à personne – et surtout pas à un organe central –, donc un consensus est nécessaire pour s'assurer de la conformité du bloc et garantir l'intégrité de la *Blockchain*.

Cette décentralisation sert le second principe de la *Blockchain* : la création de la confiance nécessaire pour que les intervenants puissent échanger des données sécurisées sans le contrôle d'un tiers de confiance.

La sécurité est l'un des principaux facteurs du développement de la *Blockchain* : les données qui la composent sont réputées infalsifiables et inviolables, du fait de l'immutabilité des données enregistrées. Il n'est en effet pas possible de modifier l'historique. La confiance est donc un élément clef, puisqu'il s'agit pour la *Blockchain* de permettre d'éviter aux intervenants d'avoir recours à un tiers de confiance.

Gérard Dréan explique à ce sujet que la *Blockchain* est « un ensemble de blocs, protégés contre toute modification, dont chacun contient l'identificateur de son prédécesseur » et ajoute « mais n'importe qui peut librement émettre des transactions, devenir mineur ou nœud du système, y compris avec l'intention de nuire ou avec des versions non standards des logiciels. Aucun participant ne peut donc écarter l'hypothèse que ce qu'il reçoit est erroné, voire carrément frauduleux ou dangereux, et chacun doit en vérifier la validité à toutes les étapes. Les transactions ou les blocs erronés ou frauduleux n'ont pratiquement aucune chance d'échapper à ces contrôles et de parvenir jusqu'à la *blockchain*, et le fraudeur se retrouve très vite isolé »<sup>(5)</sup>.

La sécurité de la *Blockchain* repose sur le principe de la puissance de calcul du réseau et le fait qu'il faille créer

un nombre très important de nœuds pour réussir à le prendre à défaut. Il faudrait en effet prendre de vitesse le « chaînage » des blocs, en créant une chaîne plus longue que la *Blockchain* originale : il faut donc avoir une puissance plus forte que le reste du réseau. C'est donc l'architecture décentralisée de la *Blockchain* et la nécessité de trouver la « *Proof of Work* » qui garantissent l'intégrité des informations.

Il convient cependant de nuancer le propos consistant à louer l'invulnérabilité et la sûreté des données contenues dans la *Blockchain*. D'une part, car la sécurité d'un logiciel n'est jamais acquise, et la *Blockchain*, aussi performante soit-elle, ne fait pas exception à cette règle. D'autre part, car il convient de garder à l'esprit que la *Blockchain* reste encore aujourd'hui une technologie de niche, que l'on pourrait qualifier avec précaution d'« immature ». En raison de la multiplicité des consensus disponibles, des différents types de *Blockchain* et des protocoles cryptographiques complexes sous-jacents, les professionnels de la sécurité ont du mal à bien comprendre les flux de données et par conséquent d'identifier les potentielles failles de sécurité<sup>(6)</sup>.

En résumé, la *Blockchain* peut être définie en trois mots : « confiance, partage et consensus ». C'est un registre distribué dans la mesure où tous les acteurs de la *Blockchain* disposent d'une copie du registre. C'est un registre fiabilisé par les intervenants de la *Blockchain*. C'est un registre décentralisé puisqu'aucun organe ne joue le rôle d'un tiers de confiance<sup>(7)</sup>.

## B. Définition juridique

En France, la technologie de la *Blockchain* a été définie par le législateur dans l'ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse, prise sur le fondement de l'article 168 de la loi n° 2015-990 du 6 août 2015 pour la croissance, l'activité et l'égalité des chances économiques.

En précisant que l'émission de minibons pouvait être inscrite dans un dispositif d'enregistrement électronique partagé, le législateur français a en effet dû définir la *Blockchain*. L'article L. 223-12 du Code monétaire et financier définit la *Blockchain* comme étant « un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations, dans des conditions, notamment de sécurité, définies par décret en Conseil d'État ».

L'article L. 223-13 énonce quant à lui que « le transfert de propriété de minibons résulte de l'inscription de la cession dans le dispositif d'enregistrement électronique mentionné à l'article L. 223-12, qui tient lieu de contrat écrit pour l'application des articles 1321 et 1322 du Code civil. À défaut, par dérogation aux dispositions

3. La *Blockchain* pour les entreprises – Livre blanc – BCG, p. 18.

4. Comprendre la *Blockchain* – Livre blanc Uchange, *op. cit.*, p. 12.

5. bitcoin.fr.

6. DELOITTE, « Points de vue – La sécurité du *blockchain* ».

7. D. LEGEAIS, « *Blockchain* », *JurisClasseur*.

de l'article 1323 de ce Code, le transfert de propriété de minibons résulte de leur inscription au nom de l'acquéreur dans le registre prévu à l'article L. 223-4 ». En d'autres termes, le transfert de propriété via la *Blockchain* tient lieu de contrat écrit.

Il s'agit donc de la première reconnaissance juridique de la validité de cette technologie, et même de sa première définition : l'ordonnance précise qu'il s'agit d'un « dispositif d'enregistrement partagé » permettant l'authentification des opérations de cession.

On retrouve donc dans cette définition la notion de partage et de garantie de l'inviolabilité et de sécurité des données qui y circulent. Toutefois, la notion de décentralisation – pourtant essentielle – a été occultée par le texte.

Le décret d'application, très attendu, n'est toujours pas paru au *Journal Officiel*. Il devrait donner les modalités de mise en œuvre du « dispositif d'enregistrement électronique », notamment en termes de sécurité, et indiquer si ce dispositif sera public ou privé. Une certaine doctrine a estimé qu'une *Blockchain* publique répondrait davantage aux impératifs de sécurité définis par les textes, car elle offrirait davantage de garanties et permettrait également de respecter certaines exigences d'identification et de connaissance des clients. La piste de la *Blockchain* privée n'est toutefois pas à exclure mais devra alors être aménagée en ce sens<sup>(8)</sup>.

Le Trésor a récemment mené une consultation publique sur la transmission de certains titres financiers au moyen de la technologie *Blockchain* et a publié un projet d'ordonnance « relative à la transmission et la représentation de titres financiers au moyen d'un dispositif d'enregistrement électronique partagé ». Cette ordonnance modifiera à la fois le Code monétaire et financier et le Code de commerce pour introduire la possibilité de représenter certains titres sur la *Blockchain*, ce qui offre une nouvelle possibilité d'inscription des titres, qui était réservée depuis la loi de dématérialisation<sup>(9)</sup> à la seule inscription en compte.

En droit français, la *Blockchain* se définit donc avant tout par sa fonction d'inscription et de transmission des titres financiers, donc une application essentiellement financière, alors que son objet est en réalité beaucoup plus large et pourrait à terme s'appliquer à un grand nombre de domaines.

## II. Les applications de la *blockchain*

Les applications pratiques de la *Blockchain* sont très variées, il conviendra par conséquent de circonscrire notre analyse. La plus connue et la plus médiatisée est le *Bitcoin*, qui est la première *blockchain* et qui a servi

de modèle à toutes les autres. Compte tenu de son importance, l'application financière de la *Blockchain* nécessite de s'y attarder (A). Les juristes seront également particulièrement intéressés par les évolutions juridiques promises par cette technologie (B).

### A. Applications financières

La première application financière trouvée à la *Blockchain* est sa fonction de paiement. En effet, il est désormais pratiquement impossible d'évoquer la *Blockchain* sans parler de *Bitcoin*. La première *Blockchain* en activité est la « *blockchain Bitcoin* ». Le premier bloc a été miné le 1<sup>er</sup> mars 2009 et la *blockchain Bitcoin* compte aujourd'hui environ 500.000 blocs<sup>(10)</sup>, soit près d'un demi-million de transactions.

La *blockchain Bitcoin* un système de crypto-monnaie décentralisée dont le *Bitcoin* est l'unité de compte<sup>(11)</sup>. Ses utilisateurs ont chacun le pouvoir d'agir et un devoir de contrôle sur les transactions. La *blockchain Bitcoin* est une illustration très concrète de l'application de la *Blockchain* en tant que « livre de comptes » puisqu'elle permet de consulter l'intégralité des transactions qui ont eu lieu depuis la création du premier bloc.

L'impact du développement du *Bitcoin* pourrait être très important pour les acteurs traditionnels du secteur bancaire. Comme l'indiquent José Luu et Martin C. W. Walker : « le *Bitcoin* est une unité arbitraire dont la comptabilité est au grand jour, accessible et contrôlable par tous. Des techniques de transmission en réseau de pair à pair sont utilisées pour diffuser les mises à jour et les demandes d'ajout de transactions, et des techniques cryptographiques sont utilisées afin de rendre inaltérables les mouvements comptables déjà enregistrés [...]. Grâce à ce mécanisme, il n'est point besoin d'une gestion centrale et l'on peut échanger ces unités arbitraires sans tiers de confiance, c'est-à-dire *sans banque* si l'on considère qu'il s'agit d'unités de nature monétaires »<sup>(12)</sup>.

La représentation juridique, la transmission et la livraison de titres financiers constituent l'une des autres séries d'applications financières de la *Blockchain* qu'il convient d'aborder du fait de son actualité.

Une consultation publique a été lancée par la Direction générale du Trésor le 24 mars 2017 et a pris fin le 19 mai 2017. Le but recherché par la Direction générale du Trésor est la rédaction d'une ordonnance appliquant les dispositions de l'article 120 de la loi n° 2016-1691 du 9 décembre 2016 (dite « Sapin 2 ») qui a habilité le Gouvernement à réformer, avant le 9 décembre 2017, le droit applicable aux titres financiers et aux valeurs mobilières, afin d'en permettre

8. D. LEGEAIS, « La *blockchain* », *RTD com.*, 2016, 830.

9. Loi n° 81-1160 du 30 décembre 1981 et son décret n° 83-359 du 2 mai 1983.

10. Comprendre la *Blockchain* – Livre blanc Uchange, *op. cit.*, <https://blockchain.info/fr>.

11. <https://bitcoin.fr/>.

12. J. LUU et M. C. W. WALKER, « La *blockchain* et la nature de la monnaie », *Revue Banque*, octobre 2016.

la représentation et la transmission, au moyen d'un dispositif d'enregistrement électronique partagé (donc d'une *blockchain*).

Sont concernés par ce texte (i) les titres de capital des sociétés non cotées<sup>(13)</sup>, (ii) les parts ou actions d'organismes de placement collectifs, (iii) les titres de créance négociables. Par ailleurs, le texte exclut les titres qui sont admis aux opérations d'un *Central Securities Depository* (« CSD ») ou livrés dans un système de règlement-livraison d'instruments financiers.

La consultation précise que, pour ce qui est de la représentation des titres, la *Blockchain* pourrait assurer trois fonctions. La première serait la tenue de compte-titres. Dans ce cadre, la *Blockchain* ne remplacerait pas le compte-titres dans lesquels sont inscrits les titres au nom de leur propriétaire (les titres financiers « ne sont matérialisés que par une inscription en compte de leur propriétaire »<sup>(14)</sup>), mais pourrait servir de technologie sous-jacente (réconciliation et transmission des titres de comptes à comptes). La seconde serait d'établir la preuve de la propriété des titres : l'inscription au sein de la *Blockchain* aurait force de preuve de propriété des titres<sup>(15)</sup>. La troisième est la représentation juridique des titres par la seule inscription au sein de la *Blockchain*. Pour le dire autrement, l'inscription dans la *Blockchain* serait considérée comme une inscription dans un compte-titre traditionnel.

Pour ce qui est de la transmission des titres, la *Blockchain* permet aujourd'hui d'effectuer des « virements » entre différents intervenants, il s'agit donc de reconnaître cette possibilité en droit positif<sup>(16)</sup>. À cet égard, les transactions conclues sur la *Blockchain* étant inscrites sans possibilité de modification ou de falsification et conservées pour une durée indéterminée, l'inscription dans la *Blockchain* pourrait également avoir une force de preuve de transfert de propriété des titres et viendrait donc s'ajouter à l'inscription de compte, du compte vendeur au compte acheteur, lors des transactions sur instruments financiers<sup>(17)</sup>. Par ailleurs, nous avons vu que le principe de la transmission des titres par la seule inscription sur la *Blockchain*<sup>(18)</sup> a déjà été acté par l'ordonnance relative aux bons de caisse qui précise que le transfert de propriété est réalisé par l'effet de la seule inscription sur la *Blockchain*.

Le point qui appellera sans doute le plus de problèmes techniques est la livraison des instruments

financiers contre un règlement en espèces. La livraison contre espèces suppose, en effet, soit (i) que les espèces soient représentées sur la *Blockchain*, ou (ii) qu'elle puisse mouvoir les comptes-titres traditionnels.

Ces trois principales innovations semblent être actées par le projet d'ordonnance du 19 septembre dernier. Le projet d'ordonnance prévoit néanmoins que les titres financiers concernés ne pourront être inscrits sur une *Blockchain* que (i) si les statuts de la société émettrice l'y autorisent, et (ii) sur décision expresse de ladite société<sup>(19)</sup>. Le système d'inscription sur un compte-titre reste donc, en tout état de cause, le droit commun.

La synthèse de la consultation de la Direction générale du Trésor précise toutefois que la question de la gouvernance de la *Blockchain* sur laquelle seraient représentés et inscrits les titres n'est pas résolue. L'essence même de la technologie étant l'absence de contrôle par un organe central, la Direction générale du Trésor indique à cet égard que « le rôle du superviseur fait débat, une majorité de répondants souhaitant limiter son intervention, éventuellement via la délivrance d'un agrément aux « gestionnaires » de *blockchain* pour certaines activités ». L'essentiel est de comprendre ici que cette technologie qui a vocation à reposer sur la confiance et la cohésion entre ses acteurs a pour but même de s'autoréguler : tenter d'instaurer une gouvernance extérieure semble donc plutôt antinomique.

## B. Applications juridiques

L'application juridique qui aura le plus de résonance parmi les juristes est indéniablement le développement des *smart contracts*. Ces contrats sont dits intelligents (« *smart* ») car lorsque les conditions d'exécution sont réunies, ceux-ci s'exécutent automatiquement sur la *Blockchain*, en prenant en compte l'ensemble des conditions et des limitations qui avaient été programmées dans le contrat à l'origine<sup>(20)</sup>. Pour le dire autrement, la vérification de la réunion des conditions de la réalisation des obligations prévues au contrat n'est pas effectuée par un tiers de confiance ou par les parties elles-mêmes, mais par la *Blockchain*. Ces *smart contracts* ont déjà leur application sur la *blockchain Bitcoin*, sur laquelle ils se matérialisent en un transfert de valeurs automatisé fondé sur des conditions mutuellement convenues<sup>(21)</sup>.

En droit français, le contrat est défini par l'article 1101 du Code civil comme étant « un accord de volontés entre deux ou plusieurs personnes destiné à créer, modifier, transmettre ou éteindre des obligations ». Le

13. Y compris les titres donnant accès au capital.

14. Proposition de modification de l'article L. 211-3 du Code monétaire et financier.

15. Modification de l'article L. 211-4 du Code monétaire et financier.

16. Modification de l'article L. 211-15 du Code monétaire et financier.

17. Modification de l'article L. 211-7 du Code monétaire et financier.

18. Modification de l'article L. 211-17 du Code monétaire et financier.

19. Modification de l'article L. 211-7 du Code monétaire et financier.

20. [www.ethereum-france.com/](http://www.ethereum-france.com/).

21. <https://bitcoin.fr/quest-ce-quun-smart-contract/>.

*smart contract*, pour être valide en droit français, doit donc répondre à cette définition et donc être un accord de volonté destiné à produire des effets de droit. Pour ses détracteurs, le terme de « contrat » est maladroit car il ne s'agit, en l'état de la technologie actuelle, que de mécanismes permettant l'exécution automatique d'un contrat, le plus souvent conclu en dehors de la chaîne de bloc<sup>(22)</sup>.

Cette technologie pourrait aussi trouver une application particulièrement intéressante en droit des assurances par exemple, en permettant de fluidifier les processus de gestion de la souscription, de tarification et de traitement des sinistres. La seule donnée nécessaire à l'exécution des obligations au titre du contrat d'assurance proviendrait d'un tiers qui recueillerait les données nécessaires à la validation des conditions d'exécution du contrat (dénommé « Oracle »). L'exemple souvent utilisé pour illustrer l'application concrète de cette technologie est le capteur (faisant office d'Oracle) qui enregistre l'arrivée d'un train pour attester de son retard et valider le remboursement ou non du billet du passager. Toutefois, les applications peuvent être beaucoup plus variées (par exemple, l'exécution d'un pacte d'actionnaires, une distribution de dividendes, etc.).

Par ailleurs, qu'en est-il de l'utilisation de la *Blockchain* comme substitut à l'acte authentique ? La vocation de la *Blockchain* est effectivement de permettre aux intervenants de se reposer sur un système qui effacerait toute intervention d'un tiers de confiance. On pense immédiatement aux notaires, qui dressent des actes authentiques. À notre avis, la technologie « primaire », qui ne consiste qu'à inscrire des données sur un « grand livre », n'apporte pas la sécurité d'un acte authentique délivré par notaire, pour la simple et bonne raison que le rôle du notaire ne se résume pas à apposer un cachet qui confère au titre la force exécutoire. Évoquer le remplacement des notaires par la *Blockchain* serait une erreur puisqu'on éluderait dans ce cas l'existence du devoir de conseil, pourtant essentiel.

Enfin, il faut se questionner sur le sujet, déjà abordé en amont, de l'inscription sur la *Blockchain* comme mode de preuve. Mais la réponse à cette interrogation ne fait plus guère de doute, puisqu'elle a été implicitement reconnue comme preuve de la propriété de titres financiers dans le projet d'ordonnance du 19 septembre 2017.

### III. Les enjeux juridiques

La régulation applicable à la *Blockchain* reste à écrire et c'est un enjeu de taille tant les sujets sont variés : vie privée (A), responsabilité (B), propriété du réseau (C)

font partie des – nombreux – sujets qu'il appartiendra au législateur de traiter à l'avenir.

#### A. Enjeux de vie privée

La *Blockchain* repose sur un principe de transparence : tout le monde peut consulter les transactions qui ont eu lieu. Par ailleurs, ce n'est pas un réseau dans lequel les intervenants agissent en anonymes : chacun se voit attribuer un pseudonyme allant de 27 à 32 caractères<sup>(23)</sup>. L'utilisation de la *Blockchain* nécessite dès lors la collecte, à un moment ou à un autre, de données à caractère personnel.

Aujourd'hui, les exigences relatives à la protection des données – récemment renforcées par la loi sur la république numérique et le règlement européen sur la protection des données personnelles – sont particulièrement contraignantes. La question notamment du respect du droit à l'oubli (récemment consacré<sup>(24)</sup>) reste ouverte car l'un des principes de la *Blockchain* est justement de conserver une trace indélébile de toutes les données ou transactions qui y ont été inscrites.

C'est d'autant plus vrai qu'étant un mécanisme encore peu régulé, il n'existe pas de responsable du traitement<sup>(25)</sup>, étant donné que la *Blockchain* est par essence un registre distribué et décentralisé.

#### B. Enjeux de responsabilité

La *Blockchain* repose sur une Organisation décentralisée autonome (« DAO ») qui est un programme informatique qui scelle dans une *Blockchain* l'ensemble des règles régissant son organisation<sup>(26)</sup>. La transparence et l'immutabilité sont totales car ces règles sont inscrites dans la *Blockchain*. Le principe est donc d'éviter les interactions humaines en définissant en amont des protocoles inscrits dans la *Blockchain* sous forme de lignes de code puis exécutés de manière automatique. Pour faire simple : « Code is Law ».

La première question est la qualification juridique de cette organisation. Peut-on la qualifier avec des mécanismes juridiques existants ? Doit-elle être considérée comme une société en participation, une société créée de fait ? La DAO est-elle un « *smart contract* »

22. M. MEKKI, « If code is law, then code is justice ? Droits et algorithmes », *Gazette du Palais*, 27 juin 2017, n° 24.

23. Comprendre la *Blockchain* – Livre blanc Uchange, *op. cit.*, p. 14.

24. C.J.U.E. (gr. ch.), 13 mai 2014, *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos*, aff. C-131/12.

25. Au sens de l'article 3 de la loi du 6 janvier 1978 et de l'article 4.7 du règlement n° 2016/679 du 27 avril 2016, « l'autorité publique, le service ou l'organisme qui détermine les finalités et moyens du traitement ».

26. Comprendre la *Blockchain* – Livre blanc Uchange, *op. cit.*

de société, c'est-à-dire une version « *blockchain* » de statuts ?

La *Blockchain* pose évidemment la question de la responsabilité en cas de faute, et plus particulièrement la question de la répartition des responsabilités entre les intervenants : doit-elle incomber au mineur qui n'a pas détecté la fraude ? Aux autres mineurs qui ne l'ont pas décelée ? À celui qui a créé le logiciel qui comporterait lui-même une erreur ?

Bien entendu, et pour respecter les principes très classiques de la responsabilité au plan juridique, la question de la répartition ne trouvera à se poser que si l'on peut déceler une faute, ayant un lien de causalité avec le préjudice subi.

Par ailleurs, dans les modèles actuels, on retrouve systématiquement un responsable, une loi applicable et un for. Tel n'est pas le cas dans la *Blockchain* qui est considérée par beaucoup encore comme une zone de non-droit. En cas de litige, s'agit-il d'agir par consensus, comme l'exigerait l'« esprit » même de la *Blockchain*, ou faudrait-il inscrire une clause d'attribution de juridiction ou une clause compromissoire et basculer ainsi vers des modes traditionnels de règlement des conflits ?

De plus en plus de personnes, notamment des consommateurs, s'intéressent à la *Blockchain*. Du fait de sa technicité et de son absence de régulation, les risques de fraude sont importants et les préjudices financiers pourraient atteindre des sommes considérables, d'où l'intérêt de mener une réflexion sur la qualification des intervenants, leur rôle et leur responsabilité.

### C. Propriété de la Blockchain et propriété intellectuelle.

À l'origine de la *Blockchain*, comme pour chaque logiciel, il existe un algorithme qui lui permet de fonctionner. Mais si la *Blockchain* est un réseau partagé sur lequel chacun peut intervenir librement et être acteur de son développement, qui en est propriétaire ?

Nous l'avons vu plus haut, il existe deux types de *Blockchain* : l'une dite « publique » et l'autre dite « privée ».

La réponse à la question de la propriété du réseau dépend donc du type de *blockchain* utilisée. Dans la *Blockchain* publique, n'importe qui peut consulter le registre et l'utiliser – c'est le mécanisme de fonctionnement du *Bitcoin*. Le corollaire de ce caractère public est que personne n'est propriétaire des codes sources : il s'agit de l'application de la théorie des biens communs<sup>(27)</sup>.

Dans une *Blockchain* privée, la technologie est développée par l'organisme en charge de sa gestion<sup>(28)</sup>. Or, l'algorithme n'est pas protégé par le droit d'auteur ou le brevet (même si cela est discuté), ce qui pose clairement le souci de la protection des inventeurs qui révolutionneront peut-être, grâce aux *Blockchains* qu'ils développeront, le monde de demain.

27. H. DE VAUPLANE, « La *Blockchain* et la loi », *Les Échos*, 21 février 2016.

28. D. LEGAIS, « *Blockchain* », *op. cit.*