Les smarts contrats, véritable révolution pour l'entreprise ou simple évolution numérique ?

Mesdames et Messieurs, Chers collègues, Chers étudiants,

Il n'est pas simple d'aborder ce sujet sur les smarts contrats ou ces « contrats intelligents » pour s'assurer qu'ils sont le signe d'une évolution ou une révolution pour les entreprises. Pourquoi ? parce que la **définition** de ceux-ci n'est claire pour personne (ou presque, peut-être y a-t-il dans la salle quelques personnes en pointe. . .).

Je vais donc m'efforcer **d'expliquer** d'abord ce qu'ils sont, essayer d'en donner des **exemples** pour ensuite **vérifier** si juridiquement, ils représentent une si grande **innovation** que ce que l'on nous annonce.

PARTIE 1 : DÉFINITION ET EXEMPLES

Si nous commençons par essayer d'en donner une définition **globale**, nous pourrions dire que :

Les smarts contrats sont des contrats numériques reposant sur la technologie de la blockchain et ils ont donc pour principale caractéristique de s'auto-exécuter.

Quand nous avons dit cela, nous n'avons **rien expliqué** ou presque puisque cette technologie de la blockchain n'est pas encore connue de tous, surtout des juristes. . .(qui passent souvent pour des dinosaures dans le domaine, à tort ou à raison. . . je ne sais pas. . . je n'oserai me prononcer. . .).

Cette **ignorance** est d'autant plus **dommageable** que la blockchain, cette « chaîne de blocs » est décrite comme une deuxième révolution numérique comparable à l'arrivée d'Internet.

Pour appréhender cette nouvelle technologie, nous pouvons reprendre une définition **répandue** selon laquelle « la blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle ».

Si on **reprend** cette définition, on comprend qu'

Elle présente deux **fonctions** : stockage et transmission d'informations

Et trois **avantages** : transparence, sécurité et l'absence de dépendance d'un organe central de contrôle.

Pour améliorer notre compréhension, rien n'est plus explicite qu'un **schéma**.

C'est ce que nous allons **réaliser** : rassurez-vous, ce schéma pourrait être intitulé « la blockchain pour les nuls » ou pire « la blockchain expliquée à ma mère ». . . C'est pour cette raison que les informaticiens voudront bien m'excuser des termes simples que je vais employer par la suite qui ne sont pas forcement les termes les plus justes.

DÉJÀ REMETTRE CE QUI CE PASSAIT AVANT DANS LE CADRE DU CONTEXTE DU CONTRAT ÉLECTRONIQUE C'EST-À-DIRE MAINTENANT !

Exemple de la location d'un film sur Internet. (oui, chers étudiants, le streaming payant vaut mieux que le téléchargement de vidéos clandestines. . .)

Pour cela, l'ordinateur du loueur et celui de l'étudiant de l'IUT de Rodez qui veut regarder un film sont reliés ensemble par un serveur central. Une sorte de gros ordinateur géré par une société tierce.

Le schéma est différent dans la blockchain.

Étape 1 : M. A effectue une transaction envers M. B

Pour cela A passe par un **programme** spécial installé sur son ordinateur préalablement. Il **rentre**, les informations nécessaires à l'exécution de cette transaction, comme le lieu de cette exécution par exemple. Les informations partent sur le **réseau** et M. A n'a plus aucune prise sur celles-ci, il ne peut plus les modifier.

Étape 2 : Ensuite plusieurs transactions passées dans cette application sont regroupées entre elles en bloc.

On retrouve ici la fonction de stockage. Et les blocs vont circuler.

Étape 3 : Le bloc est vérifié avant d'être validé.

C'est ici que la **décentralisation** joue un rôle.

L'ensemble des ordinateurs sur lesquels le programme est installé vont **participer** à cette **vérification**, en constituant ce que l'on appelle un « nœud »(et les ordi sont appelés les « mineurs »). On part de l'hypothèse qu'ils sont nombreux. Donc un ensemble d'ordinateurs, un nœud.

Cette vérification se fait à l'aide de **techniques** cryptographiques c'est-à-dire en la résolution d'algorithmes par les systèmes informatiques. **Chaque** ordinateur offre sa puissance de calcul pour résoudre ces algorithmes. La vérification permet de s'assurer que la transaction cherche bien à passer par le programme proposé, avec les **fonctionnalités** qu'il propose. Qu'il n'y a pas d'erreur de « routage » en quelque sorte.

Grâce à cela les transactions sont protégées.

Étape 4 : le bloc est daté (on dit « horodaté) et ajouté à la chaîne de blocs de transactions du même ordre.

De cette manière, la transaction obtient une **date** certaine indépendamment de la participation de A ou de B, les parties à la transaction.

Étape 5 : Transmission des informations liées aux transactions

Les informations liées aux différentes transactions sont transmises à deux types de personnes : B. le destinataire final mais aussi les autres participants.

Une **transparence** est alors assurée à propos des transactions. En effet, chaque personne qui participe à une transaction ou bien en tant qu'ordinateur de calcul peut « **lire** » l'ensemble de celles-ci. Il y a donc un **stockage** des données avec un libre accès aux utilisateurs du programme.

Résultat : ce **processus** prend un certain temps qui peut être d'une dizaine de minutes à quelques secondes en fonction des applications.

De la sorte, les applications de cette technologie peuvent être classées en trois catégories :

- **Première application : Pour le transfert d'actifs monétaires,** mais pas uniquement : **aussi des titres, votes, actions, obligations…)**

Il faut rappeler que, la première blockchain est apparue en 2008 avec la monnaie numérique **bitcoin**. Ainsi, grâce à la blockchain, cette nouvelle forme de monnaie virtuelle s'échange entre les personnes **sans organe central**. Il existe des places de **marché** avec cette monnaie qui lui donnent son cours. Il est possible de **dépenser** celle-ci grâce à des entreprises qui les acceptent. Elles sont listées sur un site internet dédié.

Cela a donné lieu au développement de ce que l'on appelle la « fintech ».

- **Deuxième application : En tant que registre c'est-à-dire en tant que recueil d'écritures.**

Cela se produit, grâce à la transparence et au stockage de données qu'assure cette technologie, il est possible qu'elle serve comme un **recueil de transaction** dont les pages s'écrivent les unes après les autres.

C'est dans ce cadre-là qu'il faut évoquer l'introduction dans le Code monétaire et financier d'un début de reconnaissance de la blockchain en tant que registre. Depuis une ordonnance du 28 avril 2016, il est reconnu que certains bons de caisse appelés « minibons » peuvent être échangés grâce à (je cite) « un dispositif d'enregistrement électronique partagé ».

En fait, il s'agit d'accompagner le développement des **plateformes** Internent de **financement participatif**. Vous connaissez sûrement ces systèmes qui permettent de **prêter** de l'argent en vue de la promotion d'un projet ou d'un artiste dans l'espérance, dans les cinq ans, de **récupérer** sa mise et une somme **d'intérêts**.

- **Enfin, troisième application, Pour les smart contrats (enfin, me direz-vous, nous y sommes !) : il s'agit de programmes autonomes qui exécutent automatiquement les conditions et termes d'un contrat, sans nécessiter d'intervention humaine une fois démarrés.**

Par conséquent, ils ne sont **pas de vrais contrats** mais les **supports** numériques de contrats. Ainsi, sur la blockchain, la « transaction » qui sera transmise sera un contrat. Pour exécuter ce contrat, il faudra que le **programme** prévu à cet effet ait **accès** à des **informations**. Elles **déclencheront** automatiquement l'exécution.

La principale nouveauté réside dans le fait que les informations indispensables au déclenchement de l'exécution ne seront **pas données** ni par les **parties** elles-

mêmes ni par un **tiers**, et donc par un **intermédiaire** mais directement par le réseau informatique qui a pu capter cette information, mise à disposition par ailleurs.

Reprenons, en le développant, **l'exemple** donné par Monsieur Nick SZABO, un informaticien, juriste et cryptographe américain qui a qui a publié le premier article sur le sujet en 1995 du contrat de location de voiture intelligent.

Il faut imaginer un contrat de location de voiture intelligent.

Imaginons qu'une personne, M. X, veuille louer une voiture de la société Y alors qu'il habite à Rodez et que la société est basée à Toulouse, sans volonté d'établir une antenne propre à Rodez.

Il manque ici un **tiers de confiance** qui ferait le lien entre M. X et la société Y.

On peut très bien envisager de créer un programme, « un Code » dirait les informaticiens, dédié à cette activité.

Chaque participant, M. X comme la société Y **installe** ce programme sur son ordinateur. Cela a pour conséquence, qu'ils **autorisent** le programme à avoir accès, en même temps, au contenu du contrat premièrement, au comptes bancaires des parties, deuxièmement et enfin, au contrôle à distance de la voiture (il existe déjà des logiciels qui servent au pilotage de nos voitures, ce n'est pas que dans James Bond ou autre, mes références datent un peu. . .).

Le contrat entre eux serait créé par **l'intégration** de son contenu dans le programme dédié sur Internet. D'une part, la société Y a déjà rentré son nom, ses coordonnées bancaires, le prix de la location de la voiture au mois par exemple, le lieu où elle devait être restituée en fin de contrat (liste incomplète, partons des informations de base).

D'autre part, M. X n'a lui, ensuite, qu'à rentrer ses propres coordonnées bancaires pour déclencher la mise en œuvre du contrat.

Le programme, une fois le paiement validé, donnera le contrôle de la voiture à M. X soit par la récupération d'un Code qui permet de déverrouiller la voiture et de la démarrer soit le par la récupération d'une clef après ouverture d'un boîtier la libérant.

Et bien, **en cas de manquement de règlement** du montant de la location un mois, détecté par l'absence de dépôt du solde sur le compte du loueur, le

programme aura la possibilité automatiquement de **bloquer** la mise en route de la voiture et d'en redonner le contrôle à la société loueur.

Dans le même ordre d'idées, si en fin de contrat, la voiture n'est **pas restituée** au lieu prévu, l'usager pourra perdre le contrôle du véhicule. L'information du retour au lieu de restitution ne sera pas donnée directement par l'une ou l'autre des parties mais sera mais grâce, par exemple, au **réseau** informatique d'un **parking** privé dans lequel la voiture doit être garée pour être considérée comme rendue. (vous avez sûrement déjà vu que maintenant dans les parkings, le temps que votre ticket d'entrée sorte, votre plaque d'immatriculation est enregistrée).

- **A partir de cet exemple, on comprend bien pourquoi le secteur de l'assurance a commencé à s'emparer de cette technologie**. Dès lors, s'est développé ce que l'on appelle l'insurtech. Mais, les champs d'exploitation sont **immenses** : santé (e-santé), industrie musicale (pour lier l'écoute un titre d'un artiste avec sa juste rémunération), énergie(calcul automatique de la consommation), ce que l'on appelle la « supply chain » c'est-à-dire la logistique dans de nombreux secteurs : agroalimentaire, commerce international, aéronautique, luxe, etc.

De façon générale, les smarts contrats appuyés sur la blockchain pourraient remplacer « les tiers de confiance » centralisés comme les notaires, les banquiers par exemple (mort de ces métiers).

- De plus, si le processus semble approprié pour des contrats standardisés,

On nous **promet** aussi qu'il peut permettre d'exécuter des contrats **complexes** qui intéressent la vie de l'entreprise comme les pactes d'actionnaires.

Rappelons qu'un pacte d'actionnaires est un contrat conclu entre tous ou certains des actionnaires d'une société, qui offre un droit de préemption aux signataires en cas de vente des droits sociaux. Le **but** est de garder le contrôle de la société entre les mains de quelques actionnaires et pas faire entrer personnes extérieure.

Ainsi, si l'un des signataires du pacte que nous appellerons M. A souhaite vendre ses actions, les autres signataires ont le droit de **se porter acquéreurs de manière prioritaire**. Si M. A souhaite vendre ses actions à un **tiers** M. T,

les autres actionnaires parties au pacte pourront préempter, et acquérir les actions avant M. T.

Un des **problèmes bien connu des juristes**, que suscitent ces droits de préemption est celui de leur **exécution forcée**.

M. A, qui a consenti un droit de préemption aux autres parties au pacte, peut être **incité** à ne pas respecter son engagement, notamment parce que le tiers M. T qui lui propose d'acquérir ses actions **sans respecter** le pacte 1) propose à M. A un **prix** très **élevé** et 2) promet à M. A de prendre à sa **charge** les éventuelles conséquences **pécuniaires** de la violation du pacte.

Une fois le contrat de vente passé et exécuté entre M. A et M. T, il n'est pas évident de pouvoir faire **machine arrière**. Pourquoi ? Parce qu'il faut que tous les signataires agissent en justice pour **contester** la vente intervenue au profit de M. T, qu'ils apportent des **preuves** assez **complexes** et que l'issue de leur action n'est pas certaine.

La **réforme** du droit des contrats, mise en œuvre par l'ordonnance du 10 février 2016, vise d'ailleurs à **renforcer** l'efficacité de ces droits.

Néanmoins, l'idée serait, grâce à la blockchain, **d'éviter** que la cession ne puisse intervenir au profit de M. T.

Pour cela, imaginons que société concerné par le pacte d'actionnaires crée des **actions** sous forme **numérique** et les **dépose** sur la blockchain.

Puis que le **pacte d'actionnaires**, soit également **déposé**.

Lorsque l'un des actionnaires vend une action à un tiers **hors du cercle** d'actionnaires actuel de la société, le système de **contrôle** de la vente qui intervient **détecte** le droit de préemption et sa **violation**, il **génère** alors un **nouveau** contrat cette fois-ci à **destination** des autres actionnaires.

L'information de l'existence d'un tel contrat est **notifiée** aux actionnaires sur l'adresse qu'ils ont choisie. Ils disposent d'un **délai** pour accepter ou décliner l'offre. Une fois la nouvelle vente **confirmée**, le **registre** des actionnaires est immédiatement **actualisé** et les documents **nécessaires** pour valider le changement sont **produits** automatiquement.

Un tel système est techniquement réalisable avec les connaissances actuelles.

Encore faut-il qu'il connaisse une régulation car il pose de nombreux problèmes juridiques.

On peut en citer quelques-uns : le problème du respect du **« droit à l'oubli** notamment numérique ». En effet, toutes les transactions qui sont entrées dans un programme de la blockchain sont enregistrées. Elles sont, en plus, liées entre elles. Il n'est pas possible d'en **retirer** la trace. Aucune demande d'effacement ou déréférencement ne pourra donc être pratiquée en principe (à moins de modifier la technique bien entendu).

Sur le **plan de la preuve**, il sera difficile de reconnaître à la blockchain la **qualité** d'une preuve parfaite nécessaire pour prouver un acte juridique comme un contrat numérique. Est-ce qu'une suite de Code pourra être lue par un juge pour être acceptée. Le langage que constitue la blockchain risque d'être un frein, **comme** a été pour la signature électronique.

Pour résoudre ces difficultés, les solutions restent à construire. En effet, il n'existe encore **aucune législation spécifique** à la blockchain. L'ordonnance évoquée plus haut du 28 avril 2016 n'est qu'un début de reconnaissance.

Sur ce même sujet, un projet d'ordonnance relative aux titres financiers a été mis en consultation par le gouvernement. Les contributions pouvaient être déposées jusqu'au 6 octobre dernier. Elle devrait être adoptée avant la fin de l'année en principe en déc. 2017. Cela ferait de la France le premier pays européen à se doter d'une telle législation sur le sujet.

Ce projet a pour intérêt de mettre en lumière **la nécessité de régulation** d'une telle technologie.

Trois possibilités sont **envisageables** :

* **l'absence totale** de régulation : ce serait le plus logique car les créateurs de ce système décentralisé n'ont foi que dans ce qu'ils créent, selon eux « **Code is law** ».

Donc, l'élément central de régulation est ce qui prévu dans le Code.

* **l'auto-régulation (ou régulation volontaire)** via un protocole informatique : la création **par** les utilisateurs de leurs **propres** règles devant respecter le minimum impératif de la législation.

* la **régulation institutionnelle** par l'insertion de règles spécifiques dans le Code civil d'une sous-section consacrée aux obligations contractuelles codées.

- Pour autant, en l'état actuel du droit, aucun vide juridique n'existe.

Rappelons que le smart contrat peut être considéré comme un contrat au sens de l'article 1101 du Code civil. Le Code monétaire et financier à la suite de l'ordonnance du 28 avril 2016 précise bien d'ailleurs que l'inscription de la cession sur la blockchain « tient lieu de contrat écrit ».

Dans ce cas, le droit commun des contrats va s'appliquer.

Et cela est heureux car

- Plus précisément, de **nombreuses difficultés sont liées à l'identification** des parties dans le contrat numérique intégré dans la blockchain et l'identification des autres participants et utilisateurs du programme dédié.

Nous savons que cette identification est indispensable pour vérifier, notamment, que chaque partie a la **capacité** juridique de contracter.

Or, la technologie Blockchain permet à l'utilisateur de rester **anonyme** et c'est un jeu de **clés cryptographiques** qui lui sont attribuées par le programme qui permet d'identifier l'utilisateur. Elles ne sont pas attribuées à une personne mais à une machine, un ordinateur.

Système de clefs

Concrètement, une première **clé privée** va permettre à l'utilisateur **d'effectuer** une opération et de prendre connaissance de son contenu. La seconde **clé qui est publique** et donc partagée va permettre aux participants au réseau de **vérifier** l'opération et la **valider**. Ils pourront seulement lire avec cette clé.

Ce système n'est donc pas satisfaisant car la **personne** derrière la clef n'est pas prise en **considération** dans le programme. Par ailleurs, la clef privée peut être **volée**.

Solution à propos de l'identité : il pourrait néanmoins, être envisagé que le programme d'un smart contrat soit mis en relation avec les registres de **l'état civil** pour connaître la situation d'une partie ou avec le site des **greffes** pour prendre connaissance des décisions judiciaires en la matière.

Là encore, il faudrait renforcer le caractère sécurisé de la technique sur le plan informatique.

Une autre solution pourrait aussi être trouvée en différenciant les blockchain publiques et privées. Seule blockchain privée entrerait dans le Code civil.

(expliquer)

Dans le cas d'une blockchain publique, **tous** les ordinateurs porteurs du programme qui met en œuvre la transaction et donc le smart contrat, peuvent **lire** les données qui y ont été intégrées.

Dans la blockchain privée, seul **un petit nombre** de porteurs du programme sont autorisés à lire à et vérifier les transactions. La **confidentialité** de la transaction et donc de la passation d'un smart contrat sera assurée. Cette **sélection** se produit grâce à l'attribution de clefs d'authentification de manière **maîtrisée**. On peut parfaitement envisager alors qu'il existe dans le programme une **archive** de cette attribution qui pourra être utilisée, une fois décryptée.

- C'est ce même problème de l'identité des parties qui peut conduire à une seconde source de problèmes juridiques lors de l'exécution du contrat.

Déjà, à ce stade du contrat, c'est-à-dire lors de son exécution, il faut **rappeler** que les termes enregistrés dans le programme ne **peuvent plus être modifiés**. S'il y a l'air d'avoir là un élément **nouveau** selon les articles que l'on peut lire sur le sujet, il n'en est rien en réalité. En effet, en principe, nous l'apprenons à nos étudiants au cours de leur première en DUT CJ ou DUT GEA, le contenu du contrat est en principe **intangible** sauf accord commun des parties au contrat ou circonstances exceptionnelles.

On peut considérer que les parties à un contrat ont **épuisé leur liberté** de modifier les termes d'un contrat par l'acceptation du **recours** à la blockchain. Par suite, elles sont d'accord pour ne pas avoir la possibilité de modifier ces termes. Il n'y a là rien de **choquant** ni d'illégal ou de compliqué à régler en cas de litige ultérieur sur ce point. (« la notion d'avenant n'est pas des plus compatibles avec les smarts contrats »)

- Surtout, l'identité des parties et des vérificateurs des blocs seraient nécessaire pour engager leur **responsabilité** ou toute autre action en justice en cas de **litige** lors de l'exécution du contrat c'est-à-dire en cas de mauvaise exécution du contrat.

Contre qui agir si le programme informatique ne remplit pas ses promesses et ne permet donc pas d'exécuter le contrat tel qu'il était attendu ?

En l'espèce, c'est bien **l'humain** qui est en cause, car c'est un être humain qui a codé le contrat et paramétré l'ensemble du programme. Il faudra alors que cette identité soit **contenue** dans le programme pour que chaque utilisateur puisse la **retrouver**.

- Dans le même ordre d'idée, **le recours en justice** paraît délicat. En effet, la blockchain a pour objectif de permettre de réaliser des transactions en dehors du système classique donc en dehors du recours au juge.

Et cette absence de recours peut paraître **peu compatible** avec un système efficace de traitement d'un contrat numérique pour lesquels le **risque** de litige est **inhérent**.

Or, si on regarde de plus près, il n'y là rien de choquant.

Il est tout à fait possible de **prévoir** pour les parties un **autre mode** de règlement de leur conflit que le recours à un juge de l'ordre judiciaire.

Les modes alternatifs de règlement des litiges basés sur la conciliation ou la médiation sont parfaitement envisageables.

De la même manière, le recours à un **arbitre** est possible. Et il est tout à fait possible de prévoir les **modalités de** résolution des conflits **à l'avance** pour qu'elles s'exécutent elles-mêmes automatiquement.

Par exemple, il est possible de considérer que si un litige naît entre les **sociétés**, il sera soumis automatiquement à la **chambre arbitrale internationale de Paris**, une instance de la chambre de commerce et d'industrie de paris.

Il est possible de prévoir que la requête sera déposée par une mise à disposition en ligne d'un **formulaire** que la partie lésée pourra remplir.

L'ensemble des autres modalités aussi : les délais, la répartition des coûts avec une saisie directe sur les comptes bancaires des parties, la transmission de la sentence arbitrale donc de la décision de l'arbitre.

Encore faut-il que les termes et les conditions de la blockchain soient suffisamment précis pour contenir tous ces éléments. Ce n'est qu'à ce prix-là que la technologie pourra vraiment être considérée comme une véritable avancée.

Si c'est un problème avec un **particulier**, l'obligation **d'information préalable** à la conclusion du contrat incluse dans notre Code civil récemment devra particulièrement être bien exécutée.

Et pour **garantir cette « qualité »** de la blockchain, quoi de mieux que de passer par une **certification** de celle-ci. Il faudrait alors faire une petite **entorse** à l'absence d'intermédiaire pour laisser par exemple un organisme comme l'AFNOR apposer ou non une certification ISO à une blokchain.

D'ailleurs, il faut signaler en ce sens la **création d'un comité technique** ISO TC 307 dont la mission est de développer des normes génériques pour tous les secteurs dans lesquels la blockchain pourrait connaître une application. Les premières discussions ont eu lieu en **avril 2017** lors de la tenue d'une première réunion entre tous les acteurs internationaux.

On le voit, il va falloir que la technologie de la blockchain qui soutient la réalisation de smarts contrats **gagne en maturité** sans brider l'innovation apportée par la technologie. Pour cela, elle pourrait s'appuyer sur une **normalisation volontaire** et ainsi freiner un encadrement institutionnel, trop éloigné de ses objectifs premiers.

Mais, cela ne suffira pas, il faut aussi un changement des mentalités. Ce n'est qu'à ce prix-là que **l'évolution constatée pourra se transformer en véritable révolution**.

Je vous remercie.