Fiabilité et sincérité des systèmes blockchain

Nicolas Herbaut[1] and François-Vivien Guiot[2]

[1]Université Paris 1 Panthéon Sorbonne
[2]Université Toulouse 1 Capitole

Introduction

Le terme de "Système" est un terme qui a priori fait sens aussi bien pour les juristes que pour les "vrais" scientifiques. Il devrait donc constituer un bon vecteur de convergences. Il n'est cependant pas certain que la notion fasse tout à fait sens de la même façon pour les uns et pour les autres. Ainsi, si dans le domaine du numérique on devrait accepter de retenir le système comme un " ensemble d'éléments qui dépendent réciproquement les uns des autres de manière à former un tout organisé " (Lalande, 1926 : 1097), au sein de la doctrine juridique on s'arrêtera également et peut-être davantage sur une seconde acception qui voit dans le système un " ensemble d'idées logiquement solidaires et tendant à offrir une vue cohérente d'un objet ou d'un champ d'étude " (id.). D'un côté le système est l'objet de la pensée, tandis que de l'autre il est une qualité de la pensée elle-même – pensée qui vise alors à la systématisation.[1]

Quoiqu'il en soit de ces nuances, il semble que la notion de système a soulevé lors de nos travaux préparatoires une même préoccupation chez les différents intervenants au premier atelier des convergences du droit et du numérique, qu'ils soient juristes ou scientifiques : celle de la confiance. Peut-on avoir confiance dans le système ? Que l'on appréhende le système construit par les algorithmes, en tant que tel, ou dans sa relation avec une pratique qu'il entend "disrupter", la mécanisation, l'automatisation, ou – plus globalement – la logicisation sont ou restent sources de méfiance.

C'est ainsi à travers la double problématique de la fiabilité et de la sincérité que nous avons décidé de converger à propos d'un objet d'intérêt commun, les systèmes Blockchain. Il s'agissait pour le juriste d'adopter une approche critique suivie de longue date par la recherche en informatique visant à démythifier le caractère infaillible comme l'objectivité des systèmes informatisés.

Il existe un terme qui exprime très bien cela : celui de " système inéquitable numérique ". Le"SIN" a pour objet de désigner un système qui pêche par ce qu'il fait peser le coût de certains dysfonctionnements sur l'utilisateur – lequel sera évidemment la partie juridiquement et économiquement faible en cas de litige[2]

Dans certains cas, c'est au législateur qu'il est revenu d'intervenir pour rétablir l'équité face au système. En vertu de la loi, c'est ainsi à la banque d'assumer l'essentiel des risques liés à l'utilisation de la carte bancaire (même en absence d'opposition, la responsabilité de l'utilisateur est limitée à 150 euros en vertu de l'art. L 133-19 du Code mon. et fin.).

[1]A dire vrai, il y a dans cette présentation des approches respectives de la science et du droit une forme de réduction puisque dans le champ juridique les deux acceptions de la notion de système sont connus. La question de savoir si c'est l'objet juridique en lui-même qui est organisé, ou si cette organisation est l'œuvre de son observateur est ainsi une question bien connue de la théorie du droit (Grzegorczyk 2002).

[2]Il est possible de prendre un exemple topique avec le cas du défaut de validation d'un titre de transport : l'utilisateur ne peut pas prouver qu'il a bien entendu le composteur biper à la présentation de sa carte numérique.

Confiance dans les systèmes blockchain

Compte tenu du rôle de plus en plus prépondérant des solutions Blockchain dans l'organisation de la vie économique et sociale, de leurs potentialités et de leurs risques[3], nous avons souhaité investir notre travail dans la question de la fiabilité et de la sincérité de ce type de système.

Présentation de la blockchain

La blockchain est perçue comme un composant d'une architecture logicielle permettant d'atteindre un consensus distribué pour les données transactionnelles sans recourir à un tiers de confiance (Xu et al. 2016). Ces systèmes consistent en une base de données permettant la lecture et l'ajout d'information sous forme d'une liste d'enregistrements chaînés appelés les blocks. Par construction, les systèmes de blockchain ne peuvent être falsifiés ou modifiés puisque chaque block contient un marqueur temporel couplé à un lien vers le block précédent (Bozic, Pujolle, and Secci 2016). La blockchain offre donc supposément l'assurance que les données ne peuvent être modifiées rétroactivement une fois enregistrées.

Un tel consensus décentralisé peut être atteint à l'aide d'algorithmes tels que proof-of-work (Nakamoto 2008) (preuve de travail), proof-of-stake (Kiayias et al. 2017) (preuve d'enjeu) ou d'algorithmes dits tolérants aux fautes Byzantines (BFT) (Veronese et al. 2013). Les blockchain peuvent être utilisées dans une grande variété de cas d'utilisation tels que les transactions financières comme Bitcoin, les dossiers médicaux ou encore le contrôle des réseaux (Herbaut and Négru 2017).

Les implémentations les plus répandues des blockchain, telle celle utilisée pour le réseau Bitcoin, ont démontré leur efficacité dans la gestion de transactions très simples, comme l'échange de devises. Néanmoins, le manque de moyen technique permettant une programmabilité extensible à d'autres cas d'utilisations plus complexes ont conduit au développement d'une nouvelle génération de blockchain. Celle-ci étend la sémantique des transactions au travers l'utilisation de "Smart Contracts" (Szabo 1997).

Parmi les différents essais lancés à grande échelle sur les marchés, l'épisode de *The DAO* (Jentzsch 2016) a constitué notre point d'entrée dans notre réflexion sur la problématique de la confiance des systèmes Blockchain.

The DAO ou l'échec de la confiance

The Dao a été fondé le 30 avril 2016, en tant qu'organisation autonome décentralisée et formait un fond d'investissement piloté directement par ses actionnaires, en fournissant un nouveau business model décentralisé appliqué à l'organisation des entreprises commerciales et organismes sans but lucratif.

Au démarrage de l'activité, le système a été techniquement déployé sur la blockchain Ethereum et était dépourvu de structure managériale ou de conseil d'administration. Son code fut publié sous licence open-source. Issu d'un financement participatif, il a détenu le record de capitalisation pour ce type de création. En Juin 2016, une vulnérabilité dans son code a permis à des utilisateurs malveillants de détourner un tiers de la valeur du fond (Atzei, Bartoletti, and Cimoli 2017).

En Juillet 2016, la communauté Ethereum a décidé de revenir en arrière sur ces transactions délictueuses en les supprimant de ses registres. Dans la controverse, une partie de la communauté, opposée à ce "hard fork" continue de maintenir la blockchain Ethereum dans son état non modifié sous le nom d'Ethereum Classic. Les deux communautés s'opposent de façon quasi philosophique sur ce retour en arrière.

- La communauté pro-fork **Ethereum** soutient que l'intentionnalité du smart contrat défectueux n'avait pas été respectée, et que les dé-

[3] dernièrement soulignés par Christine Lagarde en sa qualité de directrice du FMI : https://blogs.imf.org/2018/04/16/

tenteurs de theDao n'avaient pas exprimé leur accord sur les transactions frauduleuses.
- La communauté anti-fork **Etherum Classic** soutient que le code contenu dans les Smarts Contracts représente le plus haut niveau de vérité, et qu'il fait loi (selon le principe "code is law" : (Lessig 1999)). Ces représentants arguent également que la propriété d'immutabilité de la blockchain, sur laquelle repose la confiance des utilisateurs doit être garantie.

Dans la suite de cet article, nous proposons un modèle pragmatique qui est un compromis entre les deux approches. D'une part, puisqu'il est difficile aujourd'hui de prouver mathématiquement qu'un smart contrat ne peut être exploité par un utilisateur malveillant à des fins contraires à l'intentionnalité de l'auteur du contrat, nous proposons d'exprimer un ensemble d'invariants très simple, permettant de s'assurer que les cas limites ne peuvent entraîner d'exploitation abusive. D'autre part, nous proposons qu'une fois que les invariants ont été vérifiés, les transactions soient inscrites dans la blockchain de manière immuable.

Code is law vs code by law

Il s'agit d'envisager la possibilité de concevoir des Smart Contracts " non directement et automatiquement opposables ", en ajoutant au système un mécanisme d'appel ou d'arbitrage au stade de l'exécution du contrat. Au-delà d'une réflexion sur les valeurs du cyberespace, à laquelle nous invite le constitutionnaliste américain Laurence Lessig depuis le début des années 2000, il y a un enjeu très pragmatique : comme ce fut le cas pour toute innovation du monde économique, depuis la monnaie scripturale à Airbnb, c'est sur la confiance que repose la capacité des Smart Contracts à se développer.

En pratique, il existe deux voies essentielles et complémentaires afin d'assurer une bonne diffusion de cette nouvelle technologie : il faut tout d'abord travailler sur l'architecture du système, c'est-à-dire sur le code lui-même afin de sécuriser son fonctionnement et l'automatisation de ses fonctions. Il faut ensuite réfléchir à la manière dont le droit peut ou doit garantir les parties contractantes, non plus uniquement de la bonne exécution des engagements réciproques, mais de l'existence des conditions propres à garantir une bonne auto-exécution du contrat. Cela revient à adopter deux approches : une première, "code is law", qui tire les conséquences du fait que pour tout système numérique, c'est d'abord sa conception qui régule son fonctionnement ; une seconde, "code by law", qui s'interroge sur la capacité du droit à investir ce système afin d'y exercer son pouvoir normateur.

Code is Law

Les Smart Contracts sont généralement écrits à l'aide de langages de programmation non spécialisés (Dannen 2017) (Androulaki et al. 2018) afin de permettre au développeur les réalisant une productivité similaire au développement d'applications traditionnelles. On peut concevoir les Smart Contracts comme l'exécution de code déterministe ayant comme entrée un état donné de la blockchain et produisant des sorties également inscrites dans la blockchain. Entrées et sorties peuvent être considérées comme un ensemble de valeurs rattachées à un compte utilisateur, les contrats permettant de transférer des valeurs d'un compte à un autre.

Face aux difficultés de sécuriser les Smart Contracts par la production de preuves (Bhargavan et al. 2016) (Hirai 2017) ou par l'emploi de chasseur de prime pour détecter les exploitations possibles des anomalies des Smart Contracts (Breidenbach et al. 2018), nous proposons une approche complémentaire basée sur l'encapsulation des Smart Contracts dans des containers d'exécution arbitraux (CEA), présenté Figure 1 possédant différentes propriété que nous allons décrire.

Containers d'Exécution Arbitraux

Premièrement, l'exécution du Smart Contract dans le CEA reste similaire aux smart contacts classiques. Ils accèdent aux même données, et leurs résultats sont

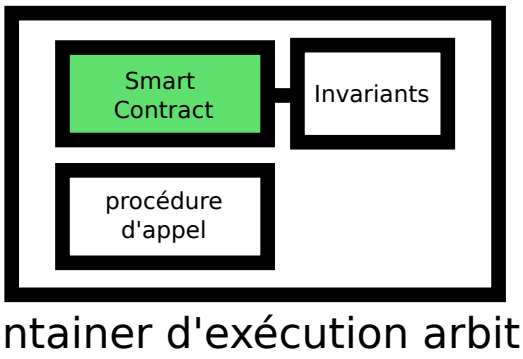

Figure 1: Encapsulation du Smart Contract dans son container d'exécution

également stockés dans la blockchain. Tout code exécuté dans le container avec les mêmes conditions initiales doit aboutir au même état de sortie. La principale différence entre le contrat exécuté directement dans la blockchain et le contrat rattaché à un CEA est que le CEA ajoute une série d'invariants concernant les entrées et sorties des contrats. Ainsi, le CEA consiste en un environnement d'exécution de plus haut niveau que le contrat initial, permettant de vérifier si certains invariants exprimables en fonction des paramètres d'entrée et de sortie sont vérifiés lors de l'exécution du contrat, comme montré sur la Figure~2.

Dans le cas nominal, tous les invariants sont satisfaits et le résultat de l'exécution du CEA est directement publié sur la blockchain sans attendre. Dans ce cas, l'exécution du Smart Contract originel est directement publiée sur la blockchain et les transactions afférentes à la consommation des ressources des différentes parties prenantes sont définitivement validées. En cas de violation des invariants du CEA, le résultat associé, appelé *résultat transactionnel* est publié sur la blockchain, mais il est décrété *non opposable* (celui-ci n'est pas encore définitif, et les ressources générées par ce contrat ne sont pas utilisables dans d'autres contrats). Le *résultat transactionnel* est associé à un nouveau contrat ad-hoc dit *contrat d'appel* permettant aux parties prenantes de les contester dans le cadre d'une *procédure d'arbitrage*.

Procédure d'Arbitrage

La procédure d'Arbitrage permet aux parties prenantes de contester les résultats de l'exécution d'un contrat sans altérer les propriétés d'immutabilité de la blockchain. En effet, les résultats transactionnels, avant d'être déclarés *opposables* peuvent faire l'objet d'un appel permettant d'aboutir à 3 résultats différents, illustré Figure 3

- Si aucune partie prenante ne souhaite faire appel de l'exécution initiale du contrat, le mécanisme d'arbitrage contourne la violation des invariants. Les conditions initiales du contrat sont validées et les résultats sont inscrits directement sur la blockchain et sont décrétés opposables.
- Si une partie prenante fait appel à un arbitrage, deux cas de figure peuvent intervenir: l'arbitrage peut invalider l'exécution du contrat, jugeant que la violation des invariants est contraire à l'esprit initial du contrat. Dans ce cas, le résultat transactionnel est déclaré non écrit, et les ressources dépensées par les parties prenantes dans le cadre de l'exécution du contrat initial sont restituées conformément à la procédure d'arbitrage.1 Dans le cas contraire, l'arbitrage peut être rendu en conformité avec l'exécution initiale. Dans ce cas, le résultat transactionnel devient un résultat opposable et est écrit en tant que tel sur la blockchain[4].

[4]L'arbitrage pouvant précisé par exemple l'annulation pure

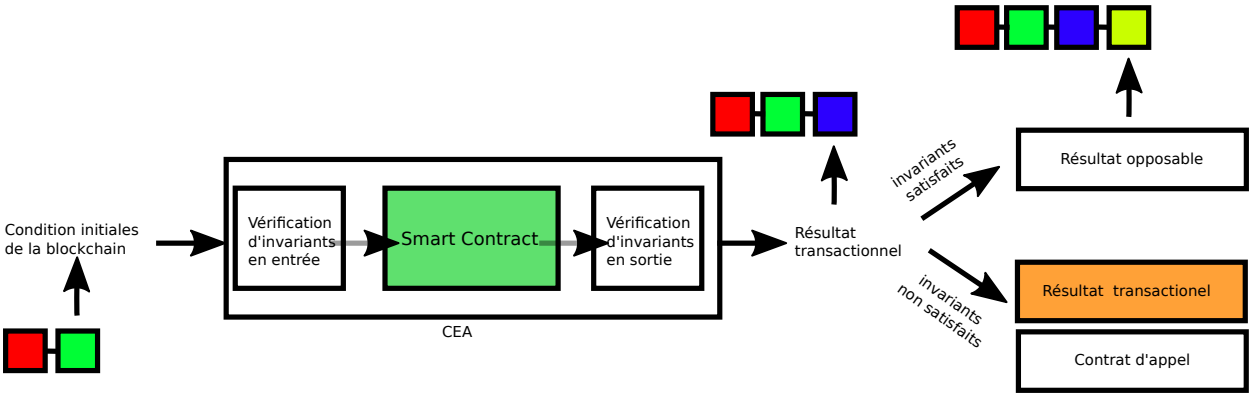

Figure 2: Exécution d'un Smart Sontract encapsulé permettant la vérification des invariants

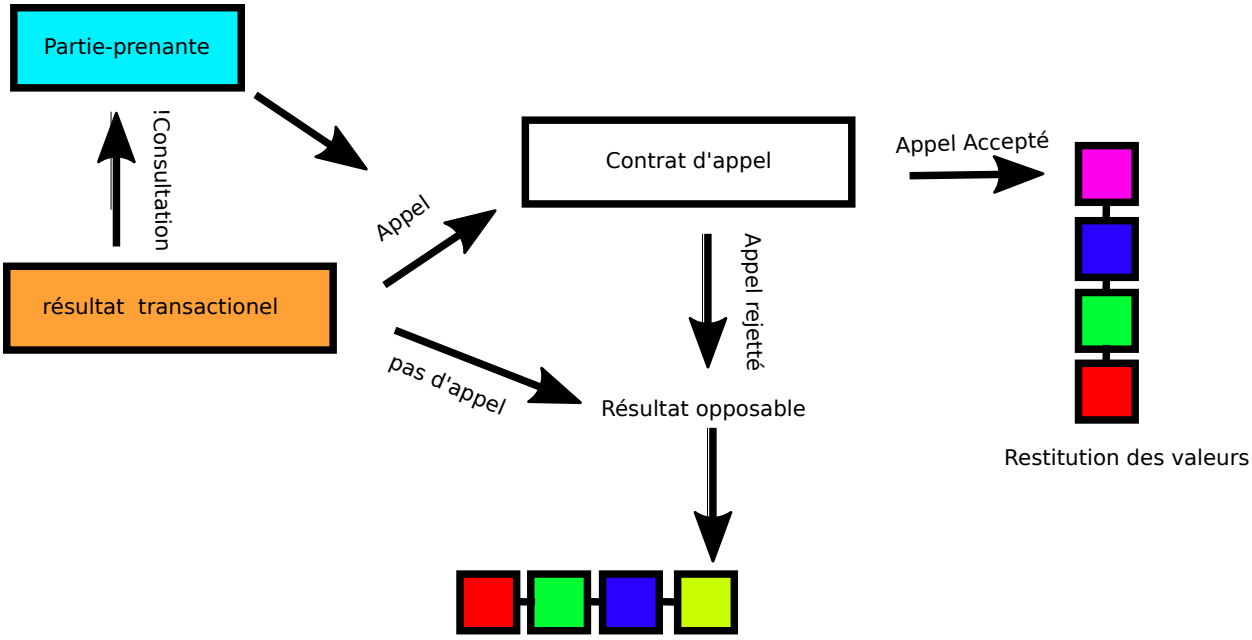

Figure 3: Exécution de la procédure d'arbitrage

Le CEA joue le rôle dépôt fiduciaire, qui ne procède au déblocage des valeurs que lorsque les résultats du smart contrats deviennent opposables.

Exemple du TheMcDAO

Afin d'illustrer l'utilisation des CEA et de la procédure d'arbitrage, nous proposons un exemple basé sur une solution de livraison de repas à domicile basée sur la blockchain: theMcDAO.

Une entreprise autonome theMcDAO propose la livraison de repas à domicile, directement basé sur la blockchain. Le service est basé sur la collaboration de 4 acteurs différents qui vont entrer en jeu pour livrer un hamburger chaud à un client, au meilleur prix. Le premier type d'acteur est le client. Celui-ci spécifie le menu de son choix, basé sur la carte d'une franchise de restauration rapide. Il spécifie également le délai de livraison attendu dans une application mobile et procède au paiement dans une devise définie par la blockchain. Les valeurs sont stockées dans le CEA du contrat de livraison de repas, qui précise la répartition de la valeur ajoutée de la prestation entre la plateforme, le prestataire de livraison et le restaurateur.

Dans un deuxième temps, la plateforme theMcDAO va choisir, parmi une liste de restaurateurs franchisés, celui qui propose de préparer la commande au meilleur prix et dans les délais impartis. Tous les restaurateurs déclarent leur disponibilité et leur prix en temps réel à la plateforme. Dès lors que la commande est réceptionnée et préparée, le hamburger est placé dans une boite témoin spéciale, qui affiche un QRCode unique lorsque la température du contenant atteint une température inférieure à 40°C. Une fois tous les éléments prêts, le sac de transport est fermé et affiche alors un QRCode unique, flashé par le restaurateur. Celui-ci dépose la commande en attendant que le livreur vienne la chercher. Le livreur, qui s'est engagé à prendre en charge la commande dans un délai imparti, arrive au restaurant. Il flash le QRCode du sac de transport et va le livrer chez le client. Lors de la remise de la marchandise, le livreur flash le QRcode du client et termine sa livraison.

Dans ce scenario, le contrat lie le client, le restaurateur et le livreur. La liste des invariants est définie comme :

1. L'horodatage du livreur respecte les délais d'engagements de livraison (heure de réception, délai de transit)
2. L'horodatage de restaurateur respecte les délais de préparation (heure de service de la commande)
3. L'horodatage du client respecte le délai de livraison (heure de réception).
4. La boite témoin n'indique pas une température inférieure à la température cible.

Si, dans les 5 minutes suivant sa livraison, le client n'a pas fait de remarque sur la qualité de sa commande, les devises sont définitivement acquises et distribuées par le contrat au restaurateur et au livreur. Dans le cas contraire, le client peut faire appel du contrat de livraison, en prouvant soit que (1) le repas lui a été livré en retard à l'aide de l'horodatage du livreur ou (2) le contenu de la commande est arrivé froid comme en témoigne la QR code affiché dans la boite témoin. Une fois transmise l'une ou l'autre des informations à la procédure d'arbitrage, celle-ci pourra soit annuler toutes les transactions de valeurs pour cette commande, soit appliquer des pénalités au restaurateur ou au livreur.

Discussion

Le modèle que nous proposons permet de mieux cadrer deux cas où la validation d'un Smart Contrat dans la blockchain réduirait la confiance globale dans le système.

Premièrement, dans le cas où l'exécution du contrat dans le monde réel n'est pas conforme à la réalité des engagement pris par les parties prenantes d'un contrat. Dans ce cas, la procédure d'arbitrage doit statuer sur la violation *d'invariants exogènes* basé sur des oracles constitués de données hors-chaînes

et simple des transactions ou l'application de pénalités, amendant le transfert de valeur initial.

(c'est à dire non présentes dans la blockchain). Ces oracles visent à vérifier le bon déroulé des engagements réciproques pris par tous les acteurs. En découplant la gestion nominale (transfert de valeur) et la gestion conflictuelle supportée par un mécanisme d'arbitrage, nos propositions facilitent la lisibilité et la compréhension de l'exécution des contrats. A noter que l'arbitrage ne nécessite pas d'être entièrement automatisé, et peut supporter l'utilisation d'un oracle supplémentaire post-exécution, comme par exemple un expert humain.

Un autre aspect prometteur de notre approche et également de pouvoir placer des invariants sur les entrées du contrat, mais également sur l'état au sens large de la blockchain lors du démarrage de l'exécution du contrat (c'est à dire non limité aux seuls états des parties prenantes). De tels *invariants endogènes* pourraient porter par exemple sur le blocage d'un transfert de valeur trop importante (e.g. invariant de valeur absolue des transactions en jeux) ou l'exécution trop répétée d'un contrat (e.g. invariant de seuil de fréquence d'appel d'un contrat). Dans ce cas, la procédure d'arbitrage pourrait être de demander à d'autres parties prenantes de s'assurer de la validité des transactions en jeux *avant* que celles-ci deviennent opposables, c'est à dire avant d'être contraint de violer l'immutabilité de la blockchain. Dans le cas de TheDAO, la communauté aurait pu valider (ou invalider) le transfert massif de fond vers des comptes frauduleux, comme ce qui a été fait a posteriori avec le hard-fork.

Dans tous les cas, la nécessité de l'utilisation d'un procédure d'arbitrage doit relever de l'exception et non du fonctionnement nominal du système. En effet, le positionnement d'invariants trop restrictifs se déclenchant trop fréquemment restreindrait le débit des transactions publiées sur la blockchain en la surchargeant de contrats d'arbitrage et empêcherait l'utilisation de ressources placées dans des procédures d'appel faisant fonction de dépôt fiduciaire.

Notons également que cette approche peut être également couplée à des procédures de vérifications formelles au niveau du contrat, de la procédure d'arbitrage, ou de la procédure de vérification des invariants.

Code by Law

Les auteurs qui s'intéressent aux nouvelles technologies et à leurs relations avec le droit s'opposent généralement sur la question de savoir si le recours aux principes traditionnels des systèmes juridiques sont suffisants ou s'il convient de reconnaître que ces principes sont inadaptés au cyberespace (Raskin 2016). Toutefois, il semble que la majorité s'accorde pour reconnaître qu'il n'y a pas, et ne peut y avoir, d'indifférence du droit à l'égard de ces nouvelles formes d'interactions sociales que véhicule le numérique. Le droit contient suffisamment de principes largement formulés, de raisonnements alambiqués, pour se saisir de tout nouvel objet (sur la possible qualification d'actifs financiers ou de " commotidies " au regard de la législation américaine : (Hansen and Reyes 2017)). Le problème réside davantage dans l'adéquation du traitement juridique ainsi déduit. A cet égard, les Smart Contracts ne font absolument pas exception, ce qui pose donc la question de leur encadrement légal – soit par l'application de règles existantes, soit par l'invention de solutions adaptées à leurs spécificités.

Réfutation de l'hypothèse du non-droit

Le système juridique repose sur une loi fondamentale : celle de sa complétude. Au risque de faire du "panjuridisme", et à l'image de la nature qui a horreur du vide, le juriste, le juge, voir le fonctionnaire des finances publiques trouvera toujours des éléments de droit à appliquer à une situation de fait - fût-ce au prix d'une réflexion intense ou du recours à beaucoup d'imagination. Le droit n'est-il pas la plus puissante école de l'imagination nous disait Giraudaux ? Pour ne prendre qu'un exemple de cette réalité expansive et inclusive, des concepts tel que celui de lex numerica ou de lex informatica sont ainsi venus accompagner le développement du commerce électronique. Cette capacité inventive du droit, même dans des domaines

où l'Etat est a priori peu présent, va directement à l'encontre du sentiment de liberté, voire d'impunité, qui prédomine bien souvent chez les promoteurs du cyberespace (même l'existence d'enjeux économiques peut conduire, à l'inverse, les acteurs du numérique à appeler de leurs vœux une réglementation qui sera source de la confiance indispensable au développement de leur secteur d'activité).

Les promoteurs de the DAO le définissent ainsi comme un "Paradis libertaire", échappant à tout cadre juridique… dès lors que la communauté formée n'aurait pas formellement d'existence. Non seulement les initiatives juridiques proposant de reconnaître à ces communautés la personnalité juridique et donc une forme de responsabilité se sont multipliées, mais en outre le droit existant a trouvé à s'appliquer à travers la qualification de " titres financiers " des actifs acquis par les participants à the DAO (Pailler 2018) (Vamparys 2018). De manière générale, le rapport entre la technologie numérique et le monde juridique est bien souvent biaisé dans les analyses proposées par les promoteurs des Smart Contracts.

A titre d'exemple, Nick Szabo qui est un des précurseurs de cette technologie, considère que le contrat est un texte qui implicitement demande à un juge d'ordonner à une partie d'effectuer un paiement ou de livrer une prestation à l'autre sous certaines conditions. C'est une vision franchement très réductrice du contrat : elle prend l'hypothèse problématique de l'inexécution pour en faire l'essence du contrat. Pour reprendre les termes de Jean Carbonnier, elle n'envisage la vie du contrat que par la pathologie qui est susceptible de l'atteindre. Or, le Contrat a pour finalité première, de savoir à quoi l'on s'engage, que ce soit par écrit ou non, de pouvoir déterminer la teneur de son engagement et les modalités de sa mise en œuvre. Ensuite, cette vision contentieuse du contrat simplifie à l'extrême en prenant un cas très particulier, l'absence d'exécution, comme seule hypothèse de saisine du juge. Bien souvent, l'exécution n'est pas quelque chose de binaire mais un continuum et tout l'enjeu en cas de litige sera d'interpréter le contrat afin de savoir à quoi s'étaient engagées les parties.

Pour en revenir aux Smart Contracts, leurs promoteurs font une double erreur : ils pensent d'une part que l'auto-exécution évite toute possibilité de contentieux (Mik 2017), et d'autre part, que l'absence de contentieux est l'indicateur de l'a-juridicité de la situation " smart-contractuelle ". Ce qui est vrai, par contre, c'est que l'identification de la juridiction compétente, l'identification de la loi applicable, mais aussi celle de la qualification qu'elle implique, restent des questions épineuses et certainement source d'incertitudes pratiques. Si l'on peut alors parler de "non-droit", au sens d'" une baisse plus ou moins considérable de la pression juridique " (Carbonnier), cette baisse n'est qu'un phénomène transitoire et non pas un état stable comme le montre s'agissant des crypto-monnaies l'encadrement juridique croissant partout dans le monde (Blemus 2017).

Adaptation du droit

Même si l'hypothèse du vide juridique doit être écartée, la sécurité juridique, qui est la finalité de toute construction juridique, pourrait imposer une intervention en amont et en aval du déploiement d'un tel contrat automatisé et doté d'un mécanisme d'arbitrage recourant à un oracle. Les Smart Contracts suivraient ainsi le précédant causé par le développement du commerce électronique (dont certaines des adaptations qu'il a entraînées paraissent d'ailleurs utiles pour assurer l'exécution de Smart Contracts : (Cohen 2017)).

Au préalable, il faut évoquer une problématique importante, relative à la détermination du droit applicable. En principe, le droit d'un État voit son champ d'application subordonné à la satisfaction soit d'un critère personnel, soit d'un critère territorial. Pour des opérations " déterritorialisées ", comme celles qui prennent place au sein du cyberespace et qui mettent en relation des personnes susceptibles d'être de nationalités différentes, se pose donc une question quant au lien de rattachement avec le droit d'un État (Vauplane 2017). La question est a priori complexe, et peut difficilement être laissée à la seule appréci-

ation des parties. Face à la diversité des règles nationales, définies soit par le droit des affaires, soit par le droit de la consommation selon la qualité des différents cocontractants, le droit international privé offre les outils susceptibles de répondre à cette problématique – fût-ce par la conclusion de conventions internationales afin d'établir des solutions nouvelles et adaptées aux nouvelles technologies. On supposera par la suite que les problèmes de conflits de loi et de juridiction sont résolus ou du moins susceptibles de résolution. Et l'on supposera donc que la compétence des autorités nationales pour réguler en amont et en aval les Smart Contracts est établie.

En amont

Quatre points essentiels devraient justifier une intervention normative destinée à encadrer en amont la mise en place de Smart Contracts dotés de procédure d'arbitrage.

Il s'agit premièrement de la question du niveau de preuve de la fiabilité du système proposé. On peut penser que les Smart Contracts auront vocation à mettre en relation des parties entre lesquelles l'équilibre ne sera pas parfait, et qu'il sera parfois nécessaire de protéger celle qui se trouve en situation de dépendance. Asymétrie d'autant plus à craindre que le langage informatique du code est proprement incompréhensible pour le quidam, même s'il est supposément moins ambigu dans sa formulation (Mik 2017). Il faut donc non seulement réfléchir au niveau d'information requis et aux modalités de preuve qui doivent s'imposer à celui qui propose un Smart Contract (et par exemple s'interroger sur le recours à la validation formelle) dans l'optique d'assurer un consentement éclairé et non vicié (Raskin 2016) ; mais il faut aussi s'interroger sur l'existence possible d'une autorité compétente pour apprécier les informations fournies quant à la fiabilité du système et à la sincérité de l'information transmise, lorsqu'il est envisagé de proposer un certain type de Smart Contract aux particuliers.

Les mécanismes de contrôle prudentiel confiés à l'autorité des marchés financiers, qui veille à la protection de l'épargne et à l'information des investisseurs, ou encore le Mécanisme de surveillance unique mis en place par l'Union européenne depuis la crise financière de 2008 et qui repose sur une mise en réseau de la Banque Centrale Européenne et des autorités nationales pourrait servir d'exemple pour un contrôle permanent et répressif. Il est aussi possible de chercher à s'inspirer des mécanismes d'autorisations de mise sur le marché, délivrées dans le secteur du médicament ou des variétés végétales par exemple, afin d'envisager une procédure préalable d'autorisation ou d'agrément applicable aux Smart Contracts.

Le deuxième point concerne la liberté ou du moins l'égalité des parties dans le choix de recourir à un oracle. A cet égard, si l'on pense contrat d'adhésion et asymétrie du pouvoir contractuel, il apparaît évident que la décision sera souvent imposée aux particuliers cocontractants, dans la mesure où elle sera indissociable du contrat proposé. Comme en matière d'arbitrage, il ne serait donc pas inutile de réfléchir aux conditions qui permettent d'éviter l'imposition d'un mécanisme d'appel dont les caractéristiques – en particulier l'identité de l'arbitre, le choix des sources d'informations utilisées, et les procédés de décision – seront prédéterminées et potentiellement abusives. Il serait en ce sens cohérent avec les limites posées en matière d'arbitrage (“ arbitrabilité objective ”et“ arbitrabilité subjective ”) de prévoir des cas d'interdiction dans les cas relevant de l'ordre public, des lois de police ou de droits indisponibles. Là encore, une exigence d'information sur les droits et obligations des différentes parties pourrait s'avérer judicieuse.

Une troisième préoccupation tient à l'encadrement et au statut de l'information utilisée cette fois-ci au sein du mécanisme d'appel ou d'arbitrage. Lors du contrôle de l'exécution de l'obligation contractuelle, l'information fournie par l'oracle est primordiale. Pour le juriste, le constat que les faits sont parfois prépondérants dans l'application de la règle de droit n'est pas une découverte. C'est tout l'enjeu de l'appréciation des faits, puis de leur qualification juridique. Il faut donc s'interroger sur la nécessité et la possibilité de garantir la neutralité de l'information

utilisée au stade du contrôle de l'exécution, c'est-à-dire l'objectivité des données transmises.

Quatrièmement, le droit devrait s'intéresser *a fortiori* au statut de l'arbitre. D'abord et évidemment, il s'agit comme pour l'oracle de s'intéresser à son objectivité et à son indépendance vis-à-vis des parties. A nouveau, comme en matière de clauses compromissoires prévoyant le recours à l'arbitrage, la loi devrait interdire les clauses abusives, susceptibles par exemple le fait de confier l'examen de l'appel à une partie prenante au contrat.

Cette préoccupation peut d'ailleurs rejoindre la précédente. Ainsi, dans le cas d'un billet de train vendu par l'EPCI SNCF, l'État en tant qu'actionnaire unique n'aurait-il pas intérêt à ce que l'EPA Météo France soit généreux avec ses deniers quand il faudra déterminer si la non-exécution de l'obligation d'acheminement peut être justifiée par le caractère exceptionnel des conditions météorologiques ? Comme en matière d'information préalable à l'engagement contractuel, le recours à des autorités administratives indépendantes pourrait offrir des perspectives intéressantes, à moins de se satisfaire d'un contrôle ex-post, de nature judiciaire, en cas de contentieux persistant après l'inscription dans la blockchain de l'opération contractuelle.

Ensuite, il n'est pas inutile de se demander si l'arbitre ne doit pas être soumis à un certain nombre d'obligations déontologiques. Là aussi, la réglementation juridique existante en fournit des illustrations. Ainsi, dans le cas d'un contrat d'assurance vie, l'arbitre serait amené à manipuler des données personnelles couvertes en France par le secret médical, il faudrait donc en assurer le respect, ce qui peut être facilement obtenu en imposant le recours à un médecin-conseil comme c'est le cas pour l'assurance traditionnelle.

En aval

Si l'intervention ex ante de la règle de droit est de nature à éviter un certain nombre de complications, il n'empêche que l'exécution du Smart Contract, toute automatique qu'elle soit, peut être source de contestations. La question qui convient alors nécessairement d'envisager, en particulier dans le cas de contrats dotés de procédure d'arbitrage, c'est celle de leur force exécutoire (en cas d'une exécution impossible – par exemple, si le débiteur n'a plus de crédits disponibles sur la blockchain) ou de la contestation de cette dernière (en cas de contestation de l'exécution automatique et/ou de la décision prise sur appel par l'arbitre).

L'une des solutions avancées par les auteurs qui se sont penchés sur ce point, consiste à adosser au Smart Contract un contrat existant dans le monde réel, afin de lui appliquer en cas de besoin les voies légales prévues en matière d'exécution. A l'analyse, ce détour paraît tout à fait inutile et même contre-productif. Il revient à subordonner l'efficacité accrue du Smart Contract, en raison de l'automaticité de l'exécution, à l'absence de contentieux, alors que celle-ci a justement vocation à éviter celui-ci. Ensuite, cette proposition présuppose que le Smart Contract n'est pas susceptible d'être légalement reconnu comme un engagement contractuel, en raison de sa forme électronique notamment ; or un tel raisonnement repose sur une conception du droit laissant une part tout à fait excessive au formalisme (Raskin 2016) p321. Cela étant, l'analyse du Smart Contract comme un engagement contractuel ne résout pas toute difficulté que peut soulever la question de son exécution.

Si l'hypothèse de l'exécution impossible (pour des raisons techniques ou liées à la disposition des fonds nécessaires sur la blockchain par exemple) se résout sans difficultés particulières devant le juge du contrat, la situation dans laquelle c'est l'exécution qui est source de contentieux est davantage source d'interrogations.

En premier lieu, lorsqu'elle a été automatiquement assurée, l'exécution peut toujours être soumise à une contestation judiciaire (ce contentieux contractuel aurait toutefois pour particularité d'intervenir ex post, alors que le juge du contrat est usuellement saisi pour assurer le respect de l'obligation contractuelle et son exécution en nature, ou pour constater l'existence

d'un titre exécutoire). Tel sera le cas si la cause du contrat est illicite et contraire à l'ordre public, mais aussi en cas de divergence d'interprétation des obligations par les parties, ou entre les expectatives et les résultats produits par le Smart Contract.

Les problèmes juridiques pouvant surgir à ce stade sont nombreux : quel effet faut-il attacher à l'absence d'utilisation par l'une des parties de la possibilité de faire appel à l'arbitre avant inscription de l'opération dans la blockchain ? Faut-il voir, comme en matière d'arbitrage, dans cette passivité une renonciation rendant une saisine ultérieure du juge irrecevable ?

En second lieu, il faut également s'interroger sur l'effet du mécanisme d'appel mis en œuvre préalablement à l'inscription sur la blockchain du résultat du Smart Contract. Faut-il reconnaître à l'arbitrage intégré au Smart Contract l'autorité de chose jugée entre les parties ? Et si oui, quelles sont alors les conditions qui entourent l'hypothèse d'un appel devant l'autorité judiciaire compétente ? Quelle doit être l'étendue de la compétence du juge ? Convient-il de la limiter au respect de l'ordre public, ou de l'étendre aux constatations factuelles tirées de l'oracle ?

Enfin, dans différentes situations envisagées précédemment, au-delà de la reconnaissance par le droit du Smart Contract et de son caractère obligatoire, l'efficacité du mécanisme peut nécessiter la reconnaissance de sa force exécutoire. Ainsi, en cas de besoin et afin de transformer le en titre exécutoire, le droit devra déterminer si le Smart Contract possède en soi, comme l'acte authentique établi par un notaire, une force exécutoire, ou s'il est au contraire nécessaire de recourir à une procédure d'exequatur au préalable ?

Ouverture

Toutes ces questions sont ouvertes, car leurs réponses dépendront du niveau de protection que le droit souhaitera accorder aux utilisateurs des Smart Contracts. Les problèmes posés en aval de l'exécution témoignent en tout cas de l'importance pour les systèmes juridiques de se prononcer sur le régime juridique qui doit accompagner leur développent.

Certes, dans le cadre du commerce électronique international, on a pu observer la naissance spontanée d'une *lex electronica*, constituée de normes informelles et de codes de bonnes pratiques adoptés par les acteurs du secteur, généralement regroupés en organisations transnationales, plutôt que par les autorités étatiques. Cependant la nécessité de protéger le consommateur face à des professionnels a partout fait naître des réglementations spécifiques complémentaires, destinées à accompagner le développement d'internet et à insuffler la confiance nécessaire pour son développement. Le parallèle entre ce précédent et le cas des Smart Contracts n'est pas dépourvu de pertinence. On observe en effet, à travers des initiatives comme celle d'Hyperledger ou de clause.io, une volonté des acteurs du milieu de coopérer pour établir des standards. Cependant, il y a dans ces démarches des mobiles qui, sans être nécessairement incompatibles avec l'objectif de protection des utilisateurs, tiennent davantage d'une stratégie d'occupation. Cela étant, la diffusion, bien souvent en opensource, de standards techniques peut favoriser la sécurité juridique, dans la mesure où leurs promoteurs sont bien souvent soucieux d'intégrer des principes juridiques largement acceptés (Hansen and Reyes 2017). En accompagnant ce mouvement, le droit pourra ainsi éviter qu'il revienne aux seuls acteurs dominants du secteur de déterminer à travers leurs technologies les valeurs qui doivent régir le fonctionnement des Smart Contracts.

Références

Androulaki, Elli, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, et al. 2018. "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains." In *Proceedings of the Thirteenth Eurosys Conference*, 30. ACM.

Atzei, Nicola, Massimo Bartoletti, and Tiziana Cimoli. 2017. "A Survey of Attacks on Ethereum

Smart Contracts (Sok)." In *Principles of Security and Trust*, 164–86. Springer.

Bhargavan, Karthikeyan, Antoine Delignat-Lavaud, Cédric Fournet, Anitha Gollamudi, Georges Gonthier, Nadim Kobeissi, Natalia Kulatova, et al. 2016. "Formal Verification of Smart Contracts: Short Paper." In *Proceedings of the 2016 Acm Workshop on Programming Languages and Analysis for Security*, 91–96. ACM.

Blemus, Stéphane. 2017. "Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide." *Revue Trimestrielle de Droit Financier*.

Bozic, Nikola, Guy Pujolle, and Stefano Secci. 2016. "A Tutorial on Blockchain and Applications to Secure Network Control-Planes." In *Smart Cloud Networks & Systems (Scns)*, 1–8. IEEE.

Breidenbach, Lorenz, IC Cornell Tech, Philip Daian, Florian Tramer, and Ari Juels. 2018. "Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts." In *27th {Usenix} Security Symposium ({Usenix} Security 18)*. USENIX} Association.

Cohen, Travis Parker, Alen West. 2017. "The Enforceability of Smart Contracts." *In Georgetown Law Technology Review* 1 (2).

Dannen, Chris. 2017. *Introducing Ethereum and Solidity*. Springer.

Grzegorczyk, Christophe. 2002. "Ordre Juridique Comme Réalité." *Droits*, no. 1: 103–18.

Hansen, J Dax, and Carla L Reyes. 2017. "Legal Aspects of Smart Contract Applications: Digital Asset Sales and Capital Markets." *Supply Chain Management, Land Registries, Government Records and Smart Cities, and Self-Sovereign Identity/Perkins Coie LLP//*.

Herbaut, Nicolas, and Daniel Négru. 2017. "A Model for Collaborative Blockchain-Based Video Delivery Relying on Advanced Network Services Chains." *IEEE Communications Magazine* 55.

Hirai, Yoichi. 2017. "Defining the Ethereum Virtual Machine for Interactive Theorem Provers." In *International Conference on Financial Cryptography and Data Security*, 520–35. Springer.

Jentzsch, Christoph. 2016. "Decentralized Autonomous Organization to Automate Governance." *White Paper, November*.

Kiayias, Aggelos, Alexander Russell, Bernardo David, and Roman Oliynykov. 2017. "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol." In *Annual International Cryptology Conference*, 357–88. Springer.

Lessig, Lawrence. 1999. "Code Is Law." *The Industry Standard* 18.

Mik, Eliza. 2017. "Smart Contracts: Terminology, Technical Limitations and Real World Complexity." *Law, Innovation and Technology* 9 (2): 269–300.

Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System."

Pailler, Pauline. 2018. "Quel Encadrement Pertinent Pour Les Initial Coin Offerings ?" *In Revue Internationale Des Services Financiers*.

Raskin, Max. 2016. "The Law and Legality of Smart Contracts."

Szabo, Nick. 1997. "The Idea of Smart Contracts." *Nick Szabo's Papers and Concise Tutorials* 6.

Vamparys, Xavier. 2018. "Perspectives Américaines Sur La Régulation Des Crypto-Actifs." *Bulletin Joly Bourse*.

Vauplane, Hubert. 2017. "Blockchain and Conflict of Laws." *Revue Trimestrielle de Droit Financier* 4 (50).

Veronese, Giuliana Santos, Miguel Correia, Alysson Neves Bessani, Lau Cheuk Lung, and Paulo Verissimo. 2013. "Efficient Byzantine Fault-Tolerance." *IEEE Transactions on Computers* 62 (1): 16–30.

Xu, Xiwei, Cesare Pautasso, Liming Zhu, Vincent Gramoli, Alexander Ponomarev, An Binh Tran, and Shiping Chen. 2016. "The Blockchain as a Software Connector." In *Software Architecture (Wicsa), 2016 13th Working Ieee/Ifip Conference on*, 182–91. IEEE.