



QUEL AVENIR POUR LE SMART CONTRACT EN FRANCE ? *OSER LA VITESSE SANS LA PRÉCIPITATION*





Ce livre blanc est produit sous l'égide de l'association « Paris, Place de Droit » dans le cadre de sa commission « numérique et justice ».

LES AUTEURS

Fabrice Lorvo, Avocat associé, FTPA.

Timothée Charmeil, étudiant, Harvard Law School.

Avec la contribution de *Bruno Deffains* (Professeur à l'Université Paris Panthéon Assas, Avocat Of Counsel, De Gaulle Fleurance & Associés) et la coordination de *Denis Musson* (Administrateur de Paris Place de Droit et Président d'honneur du Cercle Montesquieu, VP d'Equanim International), en tant que responsables de la commission « numérique et justice ».

REMERCIEMENTS

Paris Place de Droit et les auteurs du présent Livre Blanc entendent exprimer leur reconnaissance aux personnes ayant accepté d'être auditionnées. Leurs propos se sont révélés essentiels.

Il s'agit, par ordre alphabétique, de :

- **Federico Ast** (Président fondateur de Kleros et Docteur en management) ;
- **Michel Khazzaka** (Fondateur de Valuechain et responsable du groupe de travail Cryptopaiements de France Payments Forum) ;
- **Matthieu Lucchesi** (Avocat et Conseil en transformation numérique au sein de Gide 255) ;
- **Fabrice Mauléon** (Enseignant à l'ESSEC, Professeur associé à l'IFP School, consultant et expert en *business transformation*) ;
- **Pierre Person** (Ancien député et auteur du rapport parlementaire « Monnaies, banques et finance : vers une nouvelle ère crypto ») ;
- **Thibault Schrepel** (Professeur de droit à l'université VU d'Amsterdam, Professeur affilié au CodeX Center de l'université de Stanford et auteur du rapport de la Commission européenne « *Smart contracts and the Digital Single Market through the lens of a « Law + Technology » Approach* »).

PLAN

INTRODUCTION

PARTIE I – BILAN ET ENJEUX

A/ BILAN : LE SMART CONTRACT ET SON ENVIRONNEMENT

A.1/ Le fonctionnement de l'outil

A.2/ La pièce dans son environnement

B/ LES ENJEUX

B.1 / Avantages & inconvénients du smart contract

B.2/ le droit applicable au smart contract est un enjeu de souveraineté

PARTIE II – LES DROITS FRANÇAIS ET EUROPÉEN SONT L'AVENIR DU SMART CONTRACT

A/ LES ATOUTS DES DROITS FRANÇAIS ET EUROPÉEN

A.1 Approche globale

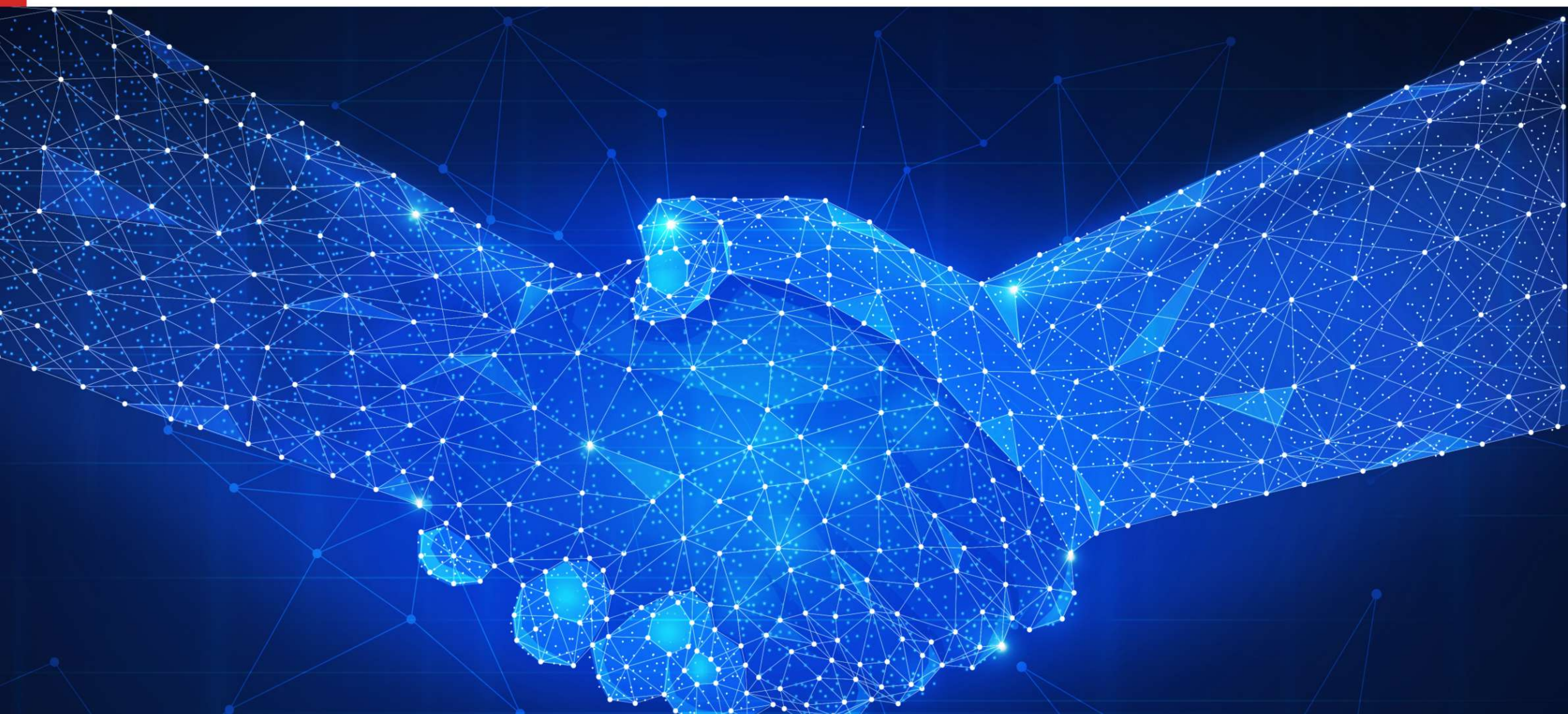
A.2 Approche sectorielle

B/ NOS RECOMMANDATIONS

B.1 : Les recommandations relatives aux sujets du smart contract

B.2 : Les recommandations relatives à l'objet du smart contract

CONCLUSION



INTRODUCTION

La révolution numérique poursuit son œuvre de digitalisation, notamment de l'économie. Son développement ultime aboutira d'abord à la dématérialisation des actifs (à savoir les produits, les services et la monnaie qui permet de les échanger) puis à l'automatisation de leurs échanges.

L'outil qui permettra l'automatisation des échanges d'actifs dématérialisés est connu sous l'appellation anglo-saxonne de « *smart contract* »¹. Comprendre et maîtriser cet outil est essentiel dès lors que, comme le souligne M. Lucchesi, « **le smart contract est une des réalités de demain** » et même « **déjà une réalité quotidienne** ».

Section I : Définition du smart contract

La promesse d'un « *smart contract* » a été formulée pour la première fois au siècle dernier par N. Szabo (1996). Le *smart contract* apparaissait alors comme « un protocole de transaction automatisé qui exécute automatique les termes d'un contrat », dont l'objectif est de « minimiser les erreurs tant malveillantes qu'accidentelles et de minimiser le besoin d'intermédiaires fiables »². Longtemps resté à l'état de promesse, le *smart contract* est devenu une réalité avec l'avènement de la technologie Blockchain (Cf. Glossaire).

Le *smart contract*, tel qu'utilisé aujourd'hui, peut alors être défini comme **le protocole informatique organisant l'échange automatique d'actifs dématérialisés enregistré sur une blockchain**.

Cette définition laisse apparaître les 4 caractéristiques du *smart contract*:

1. **Un protocole informatique** : L'architecture du smart contract ne repose pas sur des normes légales (qui identifient les comportements possibles eu égard aux valeurs d'une société), mais sur des normes technologiques (qui identifient les comportements possibles eu égard à l'état de développement technologique). Le *smart contract* permet, en cas de réalisation d'une hypothèse, d'obtenir automatiquement un résultat. Le *smart contract* est donc généralement codé sur le modèle suivant : « IF x, THEN y »³.
2. **Une Automaticité** : Après la conclusion du *smart contract*, son exécution n'est plus subordonnée à aucune action des parties. Le smart contract est une « **entité vivante** » (P. Person). L'exécution est subordonnée à la réunion d'éléments objectifs déterminée préalablement par les parties. Le *smart contract* exclut donc tout comportement subjectif des parties de toute nature (opportuniste ou involontaire).
3. **Des actifs dématérialisés** : lorsqu'il s'exécute, le *smart contract* opère un transfert d'actifs dématérialisés. La dématérialisation doit porter sur la chose (un produit ou un service) mais aussi sur le prix (exprimé en cryptomonnaie).
4. L'enregistrement sur une blockchain : le *smart contract* tire sa force de son enregistrement sur une blockchain. En effet, c'est la blockchain qui lui confère son immutabilité, sa traçabilité et son automaticité.

Dans ces conditions, le *smart contract* permet de :

- **Fusionner en un seul acte la conclusion du contrat et son exécution** (même si la réalisation de l'exécution est parfois différée).

¹ La traduction française en est « contrat intelligent ». Les rédacteurs ont considéré que la traduction française était trompeuse et ont opté pour l'utilisation de la terminologie anglo-saxonne.

² N. SZABO, "Smart contracts: Building Blocks for Digital Free Markets", In Extropy Journal of Transhuman Thought, 16.

³ Une expérimentation concrète du smart contract menée par AXA permet de mieux comprendre le fonctionnement du smart contract fondé sur le modèle « IF ..., THEN ... ». En septembre 2017, AXA a annoncé le lancement d'un service d'assurance entièrement automatisé au moyen d'un smart contract Ethereum. Ce service, baptisé « Fizzy », permettait l'indemnisation des passagers d'un vol ayant subi un retard supérieur à deux heures dès lors que les passagers avaient souscrit a priori à l'assurance Fizzy. Parce que le mécanisme assurantiel Fizzy était connecté au trafic aérien mondial, aucune intervention humaine n'était nécessaire afin d'indemniser les passagers en cas de retard. En effet, dès lors que le smart contract constatait un retard supérieur à deux heures sur un vol, les passagers étaient automatiquement indemnisés. Pour de plus amples développements sur l'usage du smart contract dans l'opération d'assurance : L. MAYAUX, « La blockchain et le smart contract : entre autonomie et automaticité », In Responsabilité civile et assurances n° 3, Mars 2023, dossier 12.

- **Supprimer l'intervention des intermédiaires avant l'exécution du contrat** (notamment le banquier ou l'huissier de Justice)⁴.
- **Rendre inéluctable la phase d'exécution du contrat lorsque les conditions sont objectivement réalisées.** En effet, nul ne peut empêcher l'exécution du *smart contract* dans les conditions prévues par le code enregistré dans la Blockchain.

L'intelligence du *smart contract* résiderait donc dans son aptitude à garantir la réalisation matérielle d'une condition préalablement prévue. Cette aptitude aurait pour effet de rendre l'exécution irréversible (et ce quoi qu'il en coûte).

En bon français, le *smart contract* ne serait donc qu'un « **contrat à exécution automatique conditionnelle** », ce qui conduit à relativiser très fortement sa prétendue intelligence (« smart »). En effet, si le *smart contract* est programmé pour réagir à certains faits, il ne dispose d'aucune aptitude pour comprendre la nature des choses⁵. Rendu immuable par son inscription sur la blockchain, le smart contract ne peut plus être modifié. Or, comme l'affirme une célèbre formule, « il n'y a que les imbéciles qui ne changent pas d'avis ». Dans ces conditions, on pourrait même se demander si ce protocole informatique ne constituerait pas plutôt un « **dumb contract** » (« contrat stupide »).

Section II : Appréhension du smart contract dans la pratique

Le *smart contract* est une réalité difficile à appréhender :

1. **Une Réalité** : Le *smart contract* est aujourd'hui omniprésent, comme en attestent les millions de transactions (permettant la conversion entre la monnaie fiat et la cryptomonnaie) opérées quotidiennement sur la Blockchain. Pourtant, avec le *smart contract*, le fait précède la règle de droit, en ce sens que les inventions technologiques précèdent, pour le moment sans cesse, la description notamment légale de leurs conditions de fonctionnement et d'utilisation. À l'heure actuelle, les droits français et européen sont muets quant au *smart contract*. Cette situation est cependant en train d'évoluer, notamment au niveau européen⁶, même si pour certains experts, cela ne va pas toujours dans le bon sens⁷.
2. **Difficile à appréhender** : le smart contract est une sorte d'**OJNI**, un objet juridique non-identifié. Cela d'autant plus qu'il ne constitue qu'une **partie d'un univers numérique plus complexe encore**. Ainsi, appréhender le smart contract nécessite tout à la fois de comprendre cette technique informatique nouvelle, mais également plus largement l'environnement numérique nouveau dans lequel cette technique s'insère. En effet, l'utilisation d'un *smart contract* suppose la réunion de plusieurs conditions préalables :
 - Chaque partie (personne physique ou morale) au *smart contract* doit être titulaire d'un portefeuille électronique (un wallet) ;
 - L'objet du contrat doit porter sur des actifs électroniques ; le vendeur doit donc fournir un produit ou un service sous forme numérique et l'acheteur doit pouvoir payer avec de la cryptomonnaie
 - L'opération doit s'inscrire sur une blockchain ;
 - Les parties reconnaissent l'existence d'un certain nombre d'implicites et notamment la fiabilité du système des wallets, les caractéristiques de la blockchain (immutabilité, infalsifiabilité, etc.), la pérennité des cryptomonnaies...

⁶ Le Parlement européen a récemment voté en faveur d'une proposition de règlement, baptisé Data Act, visant les smart contracts (l'article 30 de ce projet de règlement proposant de remodeler les smart contracts afin qu'ils puissent être « interrompus » ou « réinitialisés »).

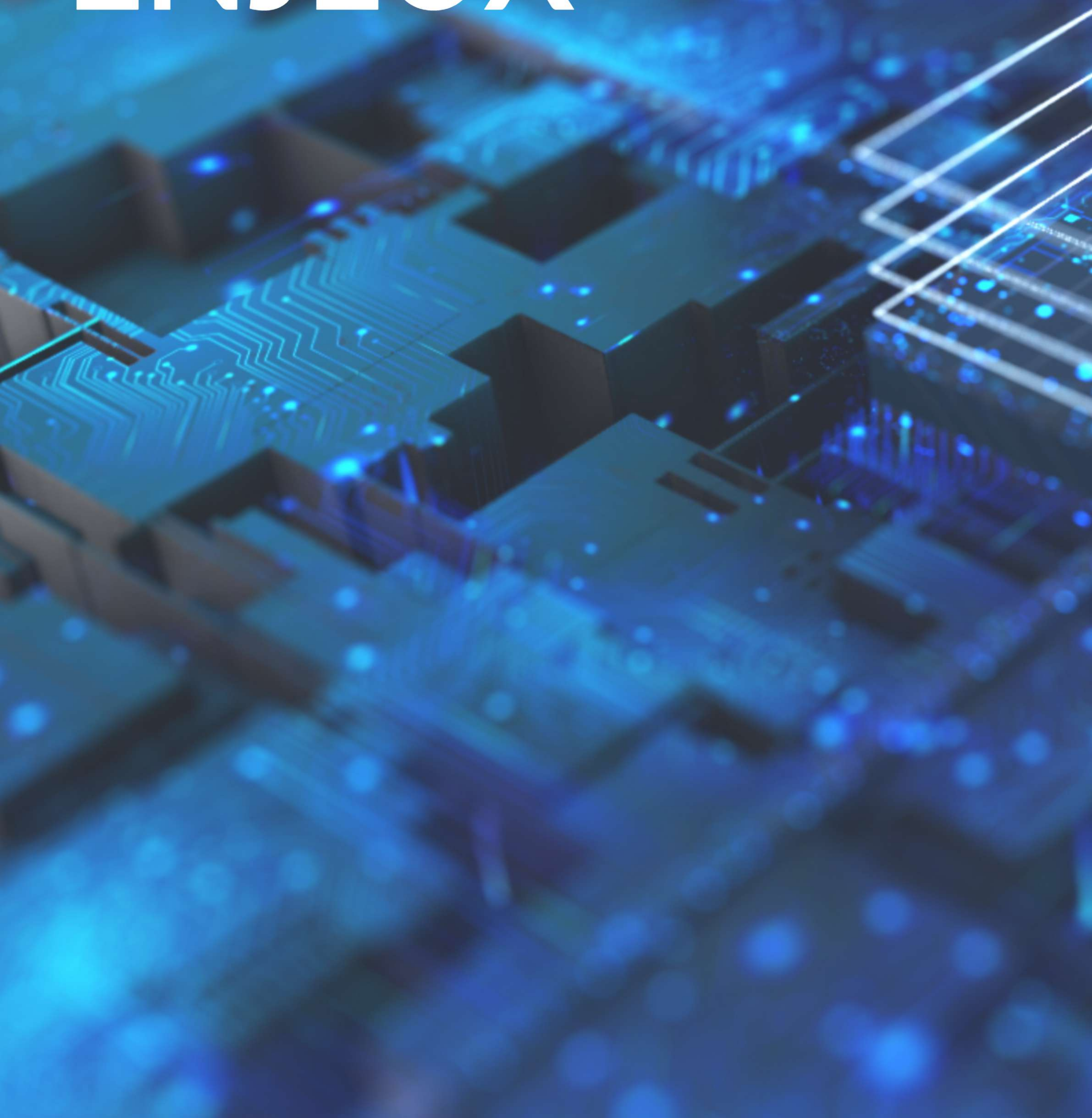
⁷ Pour certains experts comme Thibault Schrepel, le fait que le smart contract puisse être « arrêté » ou « réinitialisé » serait de nature à mettre en péril le smart contracts dans la DeFi et/ou ne limite l'innovation dans le secteur de la blockchain.

À ce jour, le *smart contract* est largement employé⁸ pour des transactions particulièrement simples d'achat ou de vente de cryptomonnaies. Force est d'ailleurs de constater que cet outil informatique se révèle particulièrement performant pour de telles transactions. Toutefois, les virtualités du *smart contract* sont bien plus larges. Théoriquement, tous les contrats d'affaires pourraient prendre la forme de *smart contract*.

⁸ A ce jour, il n'existe pas de données quant au nombre total de smart contracts en « circulation » sur l'ensemble des blockchains. Il faut dès lors se contenter de données propres à certaines blockchains. Ainsi, une étude menée sur la blockchain Binance Smart Chain en mai 2021 a révélé que près de 20 000 smart contracts étaient créés chaque jour, en moyenne, sur cette blockchain. Si le nombre de smart contracts créés quotidiennement se mesure en milliers, le nombre d'utilisations quotidiennes de smart contract atteint des millions. En effet, certains smart contracts sont utilisés jusqu'à un million de fois par jour (source : T. SCHREPEL, « Smart contracts and the Digital Single Market through the lens of a « Law + Technology » Approach », Commission européenne, 2021, p. 18).

Partie I

BILAN ET ENJEUX



PARTIE I – BILAN ET ENJEUX

A/ BILAN : LE SMART CONTRACT ET SON ENVIRONNEMENT

A.1/ Le fonctionnement de l'outil

L'appréhension du *smart contract* est difficile. Cette difficulté trouve sa source dans plusieurs causes.

Elle tient d'abord au fait que le *smart contract* est une étape supplémentaire dans la dématérialisation du monde et qu'il a une nature duale : c'est tout à la fois **un outil** et **une pièce d'un environnement numérique**.

En d'autres termes, il faut se représenter, d'une part, un Monde nouveau dans lequel la dématérialisation est la nouvelle norme et, d'autre part, un outil qui va intégrer dans un même programme, par une codification informatique, la conclusion d'un contrat et les conditions de son exécution automatique. Enfin, parce que le *smart contract* n'est qu'une pièce, son fonctionnement suppose de recourir à d'autres outils numériques.

Le contexte de la dématérialisation numérique constitue une rupture importante car elle implique de s'affranchir à la fois de support physique signé manuellement et de la possession matérielle. C'est bien cette dématérialisation qui constitue le cœur de la révolution numérique. Dans cette révolution, *le smart contract* va probablement constituer une étape décisive pour systématiser, accélérer et sécuriser le transfert des biens dématérialisés sur le marché numérique.

A.1.1 / Le smart contract est un outil

Le smart contract n'est ni bon, ni mauvais par nature : il sera ce que l'on en fera.

Pour paraphraser Jean-Philippe Desbiolles⁹, le *smart contract* sera ce que l'on en fera. En effet, à l'état brut, le *smart contract* n'est qu'un logiciel c'est-à-dire un fidèle exécutant dépourvu de tout sentiment et de toutes capacités d'appréciation contextuelle (hors oracle – Cf. Glossaire).

A.1.2 / Le smart contract est une « pièce » du puzzle numérique

Parce que le smart contract n'est qu'une pièce du puzzle numérique, il doit être emboîté avec d'autres pièces pour « faire sens ». Ainsi, en pratique, avant de recourir au smart contract, il convient de choisir une cryptomonnaie à acquérir puis une plateforme sur laquelle procéder à cette acquisition. Cela avant de procéder à une ouverture de compte et de fixer un niveau de support. Ce n'est qu'à ces conditions qu'une transaction pourra être exécutée au moyen d'un smart contract.

Le *smart contract* n'est qu'une composante d'un environnement nouveau et global fondé sur les technologies numériques. Ce faisant, afin de comprendre l'outil et de déterminer ses capacités, il faut être **capable de situer cet outil sur le marché numérique** et de **comprendre les capacités de l'environnement numérique dans lequel cet outil prend place et s'exécute**.

L'utilisation d'un *smart contract* suppose que les utilisateurs disposent de wallets et de cryptomonnaies (pour plus de détails sur comment exister sur le marché numérique, voir Annexe 2). Il suppose ensuite que la **standardisation d'un accord type auquel deux parties vont adhérer** (1). Cet accord, qui est **rédigé en code informatique** par des développeurs (2), contient l'identification des conditions préalables à son exécution ainsi que la constatation de la réalisation de ces conditions. Cela entraîne **l'exécution immédiate et a priori irréversible de la transaction** (3).

Le recours à un *smart contract* suppose donc qu'un certain type de transaction soit identifié comme étant répétitif. Cette répétitivité justifie la création de programmes automatiques préexistants auquel les parties désireuses de l'utiliser n'auront qu'à adhérer. Le *smart contract* a donc pour finalité l'automatisation des échanges entre actifs dématérialisés (avec une recherche permanente de l'amélioration du ratio vitesse - sécurité). Dans cette perspective, l'avenir du smart contract est plutôt basé sur une **approche « prêt-à-porter »** que « haute couture ».

Le code informatique est le cœur du *smart contract*. Les développeurs apparaissent dès lors comme les acteurs centraux du *smart contract*. Nous verrons ci-après que la force du *smart contract* est aussi sa faiblesse puisque ce code n'est pas immédiatement apparent pour l'utilisateur. On peut même considérer que le secret des affaires incite les codeurs à ne pas rendre immédiatement accessibles ces codes. Dans ce contexte, l'on ne peut qu'appeler de ses vœux une standardisation du langage informatique du smart contract (c'est-à-dire standardisation du code).

Enfin, le fonctionnement optimal d'un *smart contract* suppose l'échange automatique d'un produit ou **d'un service virtuel contre un paiement** en monnaie ou autre actif virtuel (la cryptomonnaie). En conséquence, l'automatisme d'échange entre marchandises (produit / services) d'un côté et paiement de l'autre ne connaîtra son fonctionnement optimal qu'en présence de cryptomonnaie. L'échange se faisant simultanément de wallet à wallet, sous réserve de la réunion des conditions préalables.

A.2/ La pièce du smart contract dans son environnement

Le *smart contract* ne constitue qu'une pièce d'un puzzle numérique global, permettant l'avènement du Web 3.0 (Cf. **Glossaire**). Ce puzzle est constitué d'une pluralité d'autres pièces, comme la Blockchain (1), la cryptomonnaie (2) le wallet (3) et, les nouvelles technologies ayant la Blockchain pour support (4).

A.2.1 / La Blockchain (Cf. Glossaire)

Les parties désireuses de recourir à un smart contract devront choisir une blockchain. En effet, il ne peut exister de smart contract sans blockchain. Le smart contract a besoin d'être sur une blockchain pour exister, pour fonctionner, pour être garanti comme pour être prouvé. La blockchain est à la fois le support et le registre du smart contract. De plus, l'existence comme l'identité du propriétaire des cryptomonnaies sont nécessairement inscrites dans la blockchain.

A.2.2 / Les cryptomonnaies (Cf. Glossaire)

L'utilisation des cryptomonnaies n'est pas indispensable pour le fonctionnement du *smart contract*. Cependant, comme nous l'avons vu, son objectif est l'accélération dans l'automatisation des transactions et cette accélération ne peut être optimale que si les actifs échangés sont tous numériques ¹⁰.

10 M. DOUAOUI-CHAMSEDDINE, « Le paiement en crypto-monnaie ou en jetons de monnaie électronique des créances de somme d'argent antérieures ou postérieures non privilégiées à l'épreuve de l'article L. 622-7, I du Code de commerce », In Revue de droit bancaire et financier n° 2 du 2023, 8.

A.2.3 / Le Wallet (Cf. Glossaire)

Les transactions sont rendues possibles par l'existence de portefeuilles numériques, qualifiés par la pratique de « *wallets* ». Ainsi, l'échange automatique et simultané d'actifs n'est possible que si le transfert électronique se fait d'un wallet à un autre *wallet*.

A.2.4 / L'univers numérique composé d'une pluralité de technologies ayant la Blockchain pour support (Métavers, NFT, DAO, ...)

Pour fonctionner, le *smart contract* a donc besoin de la Blockchain, des cryptoactifs et du wallet. La réunion de ces trois éléments permet l'avènement d'un smart contract, qui peut lui-même donner naissance ou être combiné à de nouvelles technologies numériques. Appréhender les capacités du *smart contract* impose donc d'avoir une certaine connaissance du nouvel univers numérique qu'est le Web 3.0.

Le Web 3.0, tel que nous le connaissons aujourd'hui, a vu l'apparition :

- **Du Métavers** (Cf. Glossaire)
- **Du jeton non-fongible (NFT)** (Cf. Glossaire)
- **De l'organisation autonome décentralisée (DAO)** (Cf. Glossaire)

À cette première difficulté de connaissance s'ajoute une nouvelle difficulté qui est l'évolution permanente de ce nouvel univers. En effet, force est de constater que cet environnement demeure aujourd'hui autant à l'état de projet qu'à l'état virtuel.

S'agissant du projet, sans l'émergence d'un tel monde numérique, le smart contract se trouvera dépourvu d'intérêt et ne connaîtra donc pas l'essor qu'on lui promet. La révolution numérique s'étant affranchie des frontières comme des états, **son développement optimal nécessitera** une uniformisation au niveau mondial.

S'agissant de la virtualité, la révolution numérique est un mouvement permanent (mais peut-être pas perpétuel). En conséquence, seule une petite communauté connaît et comprend les capacités comme les implications de ces nouveaux outils.

En définitive, le *smart contract* apparaît comme le cœur du Web 3.0, en ce qu'il constitue la courroie de **transmission permettant le fonctionnement de l'ensemble du Web 3.0**. Il est cet élément invisible qui assure la marche du système. En cas de dysfonctionnement du *smart contract*, le nouvel univers numérique dans son ensemble s'écroule. Dès lors, les défis résultant du smart contract doivent être appréhendés avec une attention particulière.

B/ LES ENJEUX

Malgré des avantages indéniables, le *smart contract* présente également des inconvénients tout aussi indéniables. Inconvénients qui nécessiteront l'adoption d'une réglementation qui semble ne pouvoir être qu'internationale.

B.1 / Avantages & inconvénients

Parce que le *smart contract* ne peut être envisagé en dehors de l'environnement numérique dans lequel il s'insère, le smart contract partage les avantages et inconvénients de cet environnement. Ainsi, en sus de ses propres avantages et inconvénients (B.1.1), le *smart contract* présente également les avantages et inconvénients de l'univers numérique dans lequel il évolue (B.1.2).

B.1.1 / Avantages & inconvénients du smart contract

Théoriquement, le smart contract porte la promesse d'un contrat inviolable, plus rapide, moins cher et à l'exécution certaine. Il ne fait donc aucun doute que le smart contract est « book smart » (« intello ou rat de bibliothèque »). Il n'est toutefois pas certain que, en l'état, il soit « street-smart » (« qui a appris dans la rue, débrouillard »). En effet, la pratique a révélé une pluralité de lacunes : la persistance des litiges, l'immuabilité d'un mauvais codage, l'inintelligibilité du code informatique pour le consommateur, la fin de crédit implicite, le partage de la valeur,...

1. Les avantages des smart contract

Théoriquement, les avantages du *smart contracts* sont nombreux :

- **La rapidité les transactions** : Le *smart contract* portant sur la conversion des monnaies *Fiat* en cryptomonnaie est utilisé quotidiennement. Cet outil est parfaitement adapté pour la répétition d'opérations similaires. Ainsi, « **le smart contract a vocation à devenir la pierre angulaire du business de la récurrence** » (F. Mauléon).
- **Inviolabilité du smart contract** : Dès lors que le *smart contract* ne peut être modifié une fois enregistré sur la Blockchain, les parties ont a priori l'assurance que l'opération sera exécutée telle qu'elle a été prévue initialement. Les termes de leur accord ne pourront jamais être modifiés. Le *smart contract* a donc pour ambition de « graver les termes du contrat dans le marbre numérique », de sorte que nul ne pourra ultérieurement modifier de façon unilatérale la volonté initiale des parties, et surtout pas par le juge... Les premiers penseurs du *smart contract* voyaient en effet dans le juge un « empêcheur de contracter en rond »¹², ayant tendance à réécrire le contrat.
- **Exécution certaine des obligations** : L'immutabilité du *smart contract* neutralise le risque d'inexécution ou de mauvaise exécution de l'obligation. En effet, dès lors que l'exécution du *smart contract* n'est subordonnée à aucune action supplémentaire des parties (mais uniquement à la survenance de conditions extérieures préalablement définies), le *smart contract* exclut tout comportement opportuniste des parties ou toute violation efficace. En pratique, le *smart contract* élimine donc les risques de retard de paiement ou d'impayés, fréquemment constatés dans le cadre d'un contrat traditionnel. Le smart contract se veut donc être un instrument optimal de gestion du risque par la suppression des risques relatifs à l'exécution. Par là même, le *smart contract* supprime la question de la confiance dans le cocontractant. En effet, le smart contract substitue la confiance dans la Blockchain, souvent qualifiée de « Trust Machine »¹³, à la confiance dans le cocontractant. Par là même, avec le smart contract, l'on passe du « **tiers au confiance** » au « **computer de confiance** » (F. Mauléon).

¹² J.-C. RODA, « Smart contracts, dumb contracts? », In Dalloz IP/IT, p. 54-60, juillet-août 2018.

¹³ The Economist, « The Trust Machine », 31 octobre 2015.

- **Exécution immédiate des obligations** : La vie des affaires est gouvernée par un impératif de célérité et de recherche permanente de réduction du temps. Le *smart contract* intègre à merveille la maxime « Le temps, c'est de l'argent » en ce qu'il apporte une solution définitive au problème de la vitesse des opérations. En effet, le *smart contract* ne se contente pas d'accélérer les transactions, il les rend purement et simplement immédiates. À ce titre, la tentation peut être grande de présenter le *smart contract* comme la dernière étape de l'évolution des contrats d'affaires.
- **Réduction des coûts** : Le *smart contract* constitue la promesse de réduction des coûts dès lors qu'il permet d'éviter l'intervention des tiers de confiance habituelle ainsi que de garantir l'exécution du contrat. En pratique, il supprime donc les coûts relatifs aux suivis et à la passation d'un contrat.

En somme, le smart contract, en sa qualité de « **vecteur d'automatisation des contrats** » (M. Khazzaka), permet d'aller « **plus vite et plus loin** » (F. Mauléon).

2. Les inconvénients pratiques du smart contract

Si les avantages du *smart contract* sont nombreux, ses inconvénients le sont tout autant :

- **La fin du crédit implicite ?** : Dans la vie des affaires, les retards de paiement ou les difficultés de paiement sont le lot commun des contrats, ce qui signifie souvent que le contrat est conclu mais n'est que partiellement exécuté. Cette zone grise contractuelle peut résulter de l'intérêt commun des parties (il peut être préférable pour le vendeur de prouver qu'il a vendu même s'il n'est pas payé). L'acheteur peut parfois accepter des délais de paiement qu'il sait **pertinemment intenable** du fait de la dissociation entre la fourniture du produit du service et le paiement du prix. Avec le *smart contract*, cette nuance, ne peut plus exister. Le transfert simultané des actifs dématérialisés redonne vigueur à l'ancien adage « pas d'argent, pas de Suisses ». Faute de contrepartie financière disponible lors de l'exécution du *smart contract*, ce dernier ne s'exécutera pas.
- **L'incompréhension du code informatique** : Le *smart contract* pose un problème de compréhension du code informatique par le consommateur, et ce d'autant qu'il est fort peu probable que ce code source sera apparent dans la transaction. Même s'il l'était, comment espérer du consommateur qu'il comprenne le code alors qu'il comprend déjà très difficilement le contrat écrit (d'où les dispositions sur la protection des consommateurs) ou la loi ? Surtout, différents travaux ont mis en lumière la méconnaissance du code informatique par le grand public. Ainsi, une étude menée en 2013 a révélé que seule 0,26 % de la population mondiale est à même de comprendre le code informatique. En pratique, le code du *smart contract* est donc incompréhensible pour 99,74 % de la population mondiale ! Dans tous les cas, même si le consommateur avait la connaissance de ce langage, encore faudrait-il qu'ils lisent le code informatique afférent à chaque smart contract, ce qui nous semble encore très peu probable dès lors que personne ne lit les conditions générales que l'on passe notre temps à signer.

- **L'absence de consentement** : on rappellera qu'une des conditions de validité du contrat est que chacune des parties ait un consentement libre et éclairé. En principe, chaque partie doit donc donner son consentement au « contrat mots » comme au « contrat code ». Il sera du reste possible de prévoir dans le « contrat mots » que le consentement est donné au « contrat code » si ce dernier comporte les mêmes termes que le « contrat mots ». La difficulté est qu'en pratique, les plates-formes réduisent dorénavant le « contrat mots » à sa plus simple expression. Simplicité de la transaction (click sur le produit / service convoité) et prédominance du client (retour /échange facile pour conserver la relation client à tout prix) sont les nouveaux principes. Ainsi, la puissance économique des plateformes supplante

aujourd'hui le consentement éclairé. Dans ce contexte, le smart contract est de nature à renforcer la position dominante des géants économiques déjà installés et à faire apparaître de nouvelles formes de pouvoir (notamment au niveau des codeurs ou des mineurs, Cf. Glossaire). En effet, le recul du consentement éclairé du consommateur accroît corrélativement le pouvoir de ceux qui produisent et comprennent les termes des nouvelles formes d'accord.

- Le risque d'un mauvais codage devenu immuable : L'immutabilité, parfois présentée comme une bénédiction, peut se révéler être une malédiction. Tel est notamment le cas dans l'hypothèse où le smart contract peut avoir été mal codé, de sorte que le code du smart contract ne traduit pas l'intention réelle de toutes les parties. Rendu immuable par son inscription sur une blockchain, le smart contract ne pourra être modifié et son exécution ne pourra être interrompue.
- **La persistance des litiges** : Comme l'illustre le risque d'un mauvais codage, il est illusoire de penser que le *smart contract* est synonyme de disparition des litiges et des difficultés d'exécution. En effet, de nombreux problèmes tant juridiques que technologiques peuvent apparaître à l'occasion du *smart contract*. Alors que certains ont cru pouvoir prétendre que l'avènement du *smart contract* allait faire disparaître l'utilité du juge, nous considérons à l'inverse, que le *smart contract* peut être de nature à créer deux fois plus de difficultés puisqu'au contentieux traditionnel du « contrat mots » s'ajoutera celui du « contrat code ». Face à la persistance des litiges, « **les juristes vont devoir rendre possible la défense des parties faibles** » (P. Person).
- **L'anonymat** : si la révolution numérique a mis l'individualité au cœur du système, assez paradoxalement, l'individu aime dissimuler son identité notamment sous des pseudos ou des avatars. Pour le vendeur, cette pratique est une vraie difficulté ! Comment peut-on concilier l'anonymat avec les contraintes croissantes pesant sur les professionnels et résultant des obligations en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT) ? De plus, la difficulté d'identification des parties à un *smart contract* rend particulièrement complexe l'application des règles traditionnelles de compétence et donc la résolution des litiges. Un tel constat est source de difficultés dès lors que nous avons préalablement établi que le *smart contract* ne supprime par le risque de litige.
- **Le partage de la valeur** : L'étude du marché du *smart contract* révèle une asymétrie d'information entre les auteurs de transactions, d'une part, et les mineurs d'autre part. En effet, alors que les transactions sont exposées à la vue de tous, le minage est par définition sous-terrain. De cette asymétrie découle un risque de détournement de la valeur baptisé **Miner Extractable Value (MEV) (Cf. Glossaire)**. Alors que les mineurs de la blockchain sont les gardiens de l'intégrité de la blockchain, il va donc se poser avec beaucoup d'acuité cette question manifestement très ancienne « qui gardera les gardes ? »
- **L'absence de normes internationales sur les algorithmes faisant fonctionner les *smart contracts*** : Dès lors que le code informatique est le cœur du *smart contract*, les développeurs apparaissent comme les acteurs centraux du *smart contract*. On pourrait concevoir que les codes ne soient pas apparents mais ce serait à la condition que lesdits codes puissent se référer à une norme (du style, « le présent *smart contract* est codé selon la norme XYZ »). Dans ce contexte, l'on ne peut qu'appeler de ses vœux une standardisation du *smart contract* et l'adoption de normes internationales sur les algorithmes. Comme ce point sera examiné ci-après, le *smart contract* ne doit pas être le cheval de Troie qui permettra à d'autres continents de nous imposer indirectement et subrepticement une vision du monde qui n'est pas celle de l'Union Européenne.

- **L'Oracle** : Pour que le *smart contract* puisse s'auto-exécuter, il faut que ses conditions, baptisées « Oracle », soient satisfaites, immédiatement ou à terme. La réalisation d'un *smart contract* permettant l'achat de cryptomonnaie nécessite la réalisation de conditions immédiates. Monsieur Dupont a des euros et il veut un ETH et Monsieur Durand a un ETH et il veut des euros. Parfois, la réalisation des conditions se fait avec un décalage temporel, encore faut-il que le *smart contract* soit prévenu de la réalisation postérieure des conditions prévues. Toute défaillance de l'oracle a pour effet d'enrayer le *smart contract* et de bloquer son exécution du *smart contract* ou à l'inverse à le faire s'exécuter alors que la condition n'était pas, en fait, réunie. L'Oracle joue donc un rôle essentiel dans le smart contract. À ce titre, une attention toute particulière doit être accordée par les parties au choix de l'Oracle, à son intégrité (la survenance ou l'absence de survenance de l'Oracle peut-elle être contrôlée par un tiers ?) et à sa transmission (du monde physique dans lequel il se réalise vers le monde virtuel de la blockchain où il va déclencher l'exécution du smart contract). En définitive, comme le souligne T. Schrepel, « **l'essor du smart contract sera limité aussi longtemps que la difficulté de la confiance dans l'oracle n'aura pas été résolue** ».

B.1.2 / Les risques résultant des fondements technologiques du smart contract

Dès lors que, pour fonctionner, le smart contract a besoin d'une blockchain, d'une cryptomonnaie et de wallets, les avantages et inconvénients de ces trois éléments fondamentaux de l'univers numérique ont logiquement une importance déterminante pour le smart contract. Ce faisant, recourir à un smart contract implique d'accepter les avantages et inconvénients de ces composantes de l'univers numérique.

1. La cryptomonnaie

L'avantage essentiel de la cryptomonnaie est de permettre la circulation optimale des actifs dématérialisés notamment par l'intermédiaire d'un *smart contract*. Les risques entourant l'utilisation de cryptomonnaies sont légion, de sorte que les consommateurs désireux de recourir au *smart contract* doivent s'armer de prudence. Surtout, ils ne peuvent méconnaître les deux risques principaux de la cryptomonnaie : **la perte de valeur** et **la disparition d'intermédiaires**.

Le premier risque est évidemment celui de la perte de valeur. Dès lors que les cryptomonnaies sont une manifestation de la décentralisation, leur valeur n'est aucunement stabilisée et /ou aucunement garantie par une banque centrale. Ainsi, le consommateur faisant l'acquisition aujourd'hui de cryptomonnaie n'a aucune assurance quant à la valeur de cette cryptomonnaie le lendemain. Le risque de « tout perdre » existe.

Si la valeur de la cryptomonnaie peut fondre, des intermédiaires impliqués dans le marché de la cryptomonnaie peuvent également disparaître ou cesser leurs activités du jour au lendemain. Le scandale FTX que nous avons évoqué précédemment en est une parfaite illustration. L'on peut encore citer la décision en février 2022 de Local Bitcoins, une bourse d'échange de BTC de particulier à particulier lancée en 2012, de cesser son service au lendemain de l'effondrement du marché des cryptoactifs. De même, en avril 2023, Paxful, un acteur historique des cryptomonnaies aux États-Unis a mis un terme à son activité en raison notamment de la pression réglementaire sur le marché du peer-to-peer. Dans ce contexte, la plateforme a demandé à ses utilisateurs de retirer leurs actifs électroniques.

À ce jour, nous considérons que la cryptomonnaie (à savoir une monnaie dématérialisée) est un outil indispensable pour l'optimisation du fonctionnement des *smart contracts*. Cependant, et à ce jour, la cryptomonnaie semble être le maillon faible du projet.

2. Le wallet

Le wallet est le **talon d'Achille du numérique**. En effet, il constitue la composante la plus vulnérable du Web 3.0.

Le wallet est confronté à deux difficultés majeures :

- **Un problème de gouvernance** : chaque wallet donne lieu à la remise d'une unique clef. Dès lors, celui qui détient la clé entre ses mains possède le contenu du wallet (monnaies NFT etc.). Le détenteur de la clé a donc tout le pouvoir. Cet état de fait pose des difficultés importantes notamment chez les personnes morales. Quid si celui qui connaît la clé est révoqué ou licencié ? On peut bien évidemment spéculer sur l'honnêteté du titulaire, sur le fait qu'il ne serait pas moral qu'il s'en serve comme d'un moyen de pression. À l'inverse, le titulaire de la clé est en principe un simple mortel, on ne peut pas exclure la possibilité d'un décès accidentel. Dans ces conditions la perte de la clé pourrait entraîner l'impossibilité d'accès au wallet. À ce stade, les tiers de confiance (comme les huissiers, les notaires¹⁶, les avocats) qui devenaient obsolètes par l'utilisation des *smart contract* pourraient connaître une utilité nouvelle comme tiers de confiance et dépositaire des clés numériques des wallets spécialement pour les personnes morales.
- **Un problème de sécurité** : l'actualité très récente a tristement rappelé que les wallets n'étaient pas immunisés contre les piratages¹⁷. A ce risque de piratage du wallet s'ajoute les risques d'atteintes à la clef du wallet. Dès lors qu'il n'existe qu'une unique clef par wallet, la perte de cette clef engendre mécaniquement une perte irréversible de la totalité du contenu du wallet. Dans le même sens, il suffit de voler la clef du wallet pour accéder à la totalité des actifs contenus par le wallet.

En définitive, c'est dans la clé du wallet et donc dans le monde physique que réside actuellement le talon d'Achille du nouvel univers numérique.

3. La Blockchain

L'avantage essentiel du « **système d'information** » (P. Person) qu'est la Blockchain est qu'elle est réputée être infalsifiable. Une telle infalsifiabilité, à supposer qu'elle soit réelle aujourd'hui, n'a pas vocation à perdurer pour deux raisons :

- **Le passé** : l'Histoire de l'humanité est marquée par des risques de falsification. Il n'y a aucune raison que cela s'arrête.
- **L'avenir** : S'il fallait supposer que, aujourd'hui, la Blockchain soit effectivement infalsifiable par l'humain, il serait toutefois loisible de penser que, demain, l'IA pourra faire ce que l'humain ne peut faire aujourd'hui. À ce titre, l'infalsifiabilité de la Blockchain pourrait n'être que temporaire.

Si la Blockchain ne peut être falsifiée, elle peut toutefois être modifiée par une partie de la communauté des utilisateurs de cette blockchain. Une telle modification a lieu lors d'un « *fork* » (Cf. **Glossaire**).

Plus encore, la Blockchain et les *smart contract* enregistrés sur la Blockchain peuvent présenter des failles exploitables par des utilisateurs mal intentionnés¹⁸.

Contrairement à ce qui est parfois affirmé, la Blockchain et le *smart contract* ne sont donc pas sans failles (même si l'exploitation de ces failles suppose un niveau de technicité extrêmement élevé). La relativité de l'infalsifiabilité de la blockchain et du smart contract doit donc être conservée à l'esprit.

¹⁶ V. 117e congrès des notaires de France, Le rôle du notaire dans l'encadrement du smart contract : JCP N 2021, 1280.

¹⁷ Le 3 juin 2023, des hackers sont parvenus à pirater de nombreux portefeuilles crypto Atomic Wallet et ont subtilisé à cette occasion plus de 100 millions de dollars en cryptomonnaie aux utilisateurs de ce service de wallet.

¹⁸ De telles failles ont été révélées à l'occasion du « DAO hack » affectant la première DAO, sous le nom de « The DAO ». La particularité de cette organisation résidait dans son objectif, qui était symbolique avant d'être économique. En effet, The DAO a d'abord été créé dans le but de prouver que les DAO ne sont pas un fantasme mais une réalité. Accessoirement, The DAO visait à récolter des fonds destinés à être investis dans des projets validés par les participants à la DAO. The DAO était un succès relayé par la presse internationale jusqu'au 17 juin 2016, date à laquelle un hacker est parvenu à profiter d'une faille dans le code de The DAO afin de détourner l'équivalent de près de 140 millions de dollars.

B.2/ La réglementation du web 3.0 et du smart contract est un enjeu de souveraineté

Le smart contract est d'ores et déjà devenu une ressource stratégique de la « guerre de souveraineté juridique » à laquelle nous assistons aujourd'hui. La France et l'Europe ne sauraient prendre de retard dans cette lutte de souveraineté dans laquelle certains États sont déjà en train de s'engager. Cela d'autant plus que la prime au premier entrant pourrait bien trouver à s'appliquer.

Il est manifeste que le Web 3.0 va prochainement devenir la place de marché numérique majeur, à tout le moins pour la consommation de masse. Si le Web 3.0 était un être vivant, le *smart contract* serait son sang. En effet, le *smart contract* va être l'instrument permettant, en pratique, le bon fonctionnement optimal de tous les organes du Web 3.0, que sont notamment la Blockchain, le Métavers ou encore le NFT. Sans *smart contract*, le Web 3.0 n'est qu'une coquille vide dénuée de vie. Ce faisant, on doit aussi garder à l'esprit que celui qui aura la main le *smart contract* pourra tirer les ficelles de ce nouvel univers qu'est le Web 3.0.

Dans ces conditions, il est évident que le Web 3.0 comme le *smart contract* vont constituer un instrument décisif dans la lutte, qu'elle soit directe ou de fait, entre les différentes visions juridiques du monde. Dès lors, comme l'affirme P. Person, « **le smart contract est un enjeu de souveraineté** » (pour de plus amples développements sur la souveraineté : Cf. annexe 3).

Avec le numérique, les problèmes anciens de souveraineté demeurent mais de nouveaux apparaissent. En sa qualité de nouveau joyau de la révolution numérique, le *smart contract* n'échappe pas à cette guerre de souveraineté qui s'exerce à différents niveaux. Cette guerre froide 3.0 n'est pas anodine : celui qui imposera son droit pour l'utilisation des *smart contracts* imposera aussi sa vision du monde ou, à tout le moins, pourra remettre en cause une vision concurrente d'un autre État. Dans ce contexte, le numérique est une **arme de soft power** dont il ne faut pas méconnaître la portée.

L'on ne saurait prendre du retard dans cette lutte de souveraineté, dès lors qu'il est fort à parier que la règle de la **prime au premier entrant** s'appliquera. Ainsi, celui qui sera à même de proposer la meilleure technologie utilisable pour le développement des smart contracts sera probablement désigné vainqueur de cette guerre silencieuse.

Les premières manifestations de cette « **guerre froide de souveraineté juridique** », opposant les grands systèmes juridiques sont d'ores et déjà visibles (cela est notamment visible entre le monde anglo-saxon du Common Law et les pays de droit européen).

Les premiers *smart contracts* d'échange de cryptomonnaies fonctionnent quotidiennement aux USA. De plus, depuis quelques années, l'environnement Web 3.0 est traversé par une dynamique nouvelle : les principaux systèmes juridiques ont entrepris de démontrer en quoi ils étaient les mieux adaptés à l'essor du *smart contract*. C'est ainsi que, dès 2018, un rapport est paru en Grande-Bretagne pour expliquer que le système juridique britannique était le seul à même d'assurer un essor pérenne du *smart contract* (ex : *UK Jurisdiction Taskforce, Legal statement on crypto assets and smart contract, 2018*). Même si nous rendons hommage au travail réalisé par nos collègues anglais, nous sommes au regret de ne pas partager leurs conclusions (surtout depuis le Brexit.....).

Dans ces conditions, la France se doit d'être le promoteur du droit européen dans le cadre du développement du *smart contract*. En effet ; dans un monde globalisé, raisonner en droit français n'a pas de sens. Cela, d'autant plus que le droit français est aujourd'hui largement composé d'un droit d'origine européenne.

C'est pour participer à cette démarche, qui doit être incessante, que le présent rapport a été rédigé en vue de mettre en lumière les atouts qui font de la place de Paris le lieu idéal pour l'essor des *smart contracts*.

Cette ambition, saine et nécessaire, ne doit pas nous dispenser d'une nécessaire modestie dès lors que l'analyse ci-dessus n'est que l'expression d'un certain ethnocentrisme. La présente étude ne vise que l'Union européenne et sa rivalité avec son interlocuteur principal, le monde anglo-saxon. Toutefois, la même réflexion devrait être entreprise vis-à-vis des marchés numériques émergents que sont la Chine, l'Inde, la Russie, etc. Si la Chine et l'Inde ne sont pas à ce jour des partenaires économiques visibles de l'UE, ces deux pays ont vocation à le devenir rapidement en raison de leur avancée technologique. Il est évident que le constat de l'importance potentielle du smart contract dans le prochain développement économique mondial a aussi été fait dans ces autres pays qui n'attendent pas les initiatives, notamment européennes, pour développer leur propre modèle.

En même temps, on doit se demander si la loi applicable sera le seul facteur de développement du *smart contract*. En effet, au-delà de la norme juridique, le commerce numérique mondial est également gouverné par la satisfaction du consommateur. En conséquence, celui qui saura proposer une application intégrant un *smart contract* satisfaisant le consommateur sur la durée pourrait emporter le marché, et ce, **quels que soient sa langue, son droit ou la technologie qu'il utilise.**

Sous le bénéfice de ces réserves, on doit rappeler ce truisme qu'un combat n'est perdu que s'il a été disputé et que dans ces conditions, il appartient aux forces vives de notre pays de mettre en avant ses atouts, dès lors qu'ils sont nombreux.

Partie II
**LES DROITS FRANÇAIS
ET EUROPÉEN SONT
L'AVENIR DU SMART
CONTRACT**



PARTIE II – LES DROITS FRANÇAIS ET EUROPÉEN SONT L'AVENIR DU SMART CONTRACT

Du fait de ses atouts (A), nous avons la conviction que ce sont les droits européen et français qui détiennent les clefs d'un essor souhaitable du smart contract, c'est-à-dire un essor dans le sens d'une transformation numérique qui « fonctionne pour tous et pas seulement pour quelques-uns »¹⁹ de manière à donner naissance à « une société numérique fondée sur les valeurs et les règles européennes »²⁰. Dans ce contexte, nous formulons quelques recommandations (B) de nature à contribuer, à nos yeux, à la démarche européenne en cours.

A/ LES ATOUTS DES DROITS FRANÇAIS ET EUROPÉEN

Que l'on se place dans une démarche globale ou sectorielle, « les droits français et européen sont pleinement aptes à appréhender le smart contract. À cette aptitude du droit s'ajoute la maturité déjà atteinte par l'écosystème blockchain en France » (M. Lucchesi).

A.1 Approche globale

A.1.1 : Nos postulats

Les auteurs du présent Livre Blanc partent du postulat que le smart contract, qui sera ce que nous en ferons, ne pourra se développer durablement en dehors du droit existant. Il y aura donc bien une régulation du smart contract. Cela d'autant plus que cette régulation par le droit pourrait bien être imposée de facto par le marché.

1/ Le smart contract sera ce que nous en ferons.

Comme précédemment évoqué, le *smart contract* n'est qu'un outil. Or, tout outil notamment numérique dispose d'une aptitude extraordinaire à devenir soit un outil de progrès, soit un outil de spoliation. Une telle aptitude résulte de l'essence même du monde numérique. Pour reprendre une expression du Conseil d'État, la difficulté tient « à l'ambivalence intrinsèque du phénomène numérique : il ouvre de nouveaux espaces de libertés, tout en étant porteur de risques pour ceux-ci. Une intervention trop rigoureuse du législateur destinée à prévenir les aspects négatifs du numérique risque, du même mouvement, d'en entraver le potentiel positif ».²¹

Le *smart contract* n'échappe pas à cette ambivalence. L'on peut même légitimement se demander s'il n'en constitue pas le paroxysme. En effet, à l'état brut, le *smart contract* n'est qu'un protocole informatique, c'est-à-dire un fidèle exécutant dépourvu de tout sentiment et de toutes capacités d'appréciation contextuelle. En conséquence, cet instrument neutre par nature pourrait devenir, entre de mauvaises mains et sans régulation, un instrument de spoliation de l'individu (et spécialement, du consommateur). Une fois de plus, *le smart contract* ne sera que ce que nous en ferons.

19 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 19 février 2020, Façonner l'avenir numérique de l'Europe, COM (2020) 67 final.

20 Ibid.

21 Conseil d'État, « Le numérique et les droits fondamentaux », 2014.

2/ Le smart contract ne pourra se développer durablement en dehors du droit existant tel que nous le connaissons.

À nos yeux, l'usage du *smart contract* ne pourra se généraliser, que si celui-ci permet un essor des relations commerciales équilibrées entre les personnes en toute sécurité juridique. En d'autres termes, *le smart contract* n'aura pas un avenir durable s'il devient l'arme ultime des marchands pour contourner les barrières protectrices érigées par le droit des contrats et de la consommation et ainsi optimiser les transactions. Ne nous leurrions pas : des esprits mal intentionnés verront, dans le smart contract, une arme « nucléaire » **numérique permettant** d'éluder des siècles de construction juridique ayant pour objet ou pour effet d'instaurer un équilibre contractuel, dans le monde physique, entre les parties. Parier de la sorte contre la capacité de notre droit à surmonter le nouveau fait technologique qu'est le smart contract serait une grave erreur. En effet, notre droit, fondé sur la recherche d'un équilibre, va une nouvelle fois faire la démonstration de sa vitalité et de sa résilience, et ce même en présence d'un outil dématérialisé.

La soumission du *smart contract* au droit français/européen existant (sous réserve de son adaptation à une relation totalement dématérialisée) est donc la condition de son essor. « **Le chemin vers la Blockchain n'est donc nécessairement libertarien** » (M. Khazzaka).

Parce que le *smart contract* s'insère dans la nébuleuse numérique dont le propre est d'abolir les frontières, le *smart contract* pourrait techniquement s'affranchir des normes juridiques existantes, qui n'ont vocation à produire des effets que sur un territoire strictement limité. Ainsi, le *smart contract* pourrait s'affranchir du droit européen en étant basé et régi par des lois non européennes. Cette potentialité technologique n'est toutefois ni souhaitable, ni sérieusement envisageable.

Bien sûr, il pourra exister des offres basées sur des *smart contract* générés en dehors de l'Europe et du cadre normatif européen. Toutefois, nous n'hésitons pas à affirmer qu'il ne s'agira que d'expériences éphémères vouées à l'échec.

Une telle affirmation ne relève pas tant de la divination que de l'étude des cycles et du passé. Le marché a historiquement pour caractéristique de vite apprendre des échecs des premiers précurseurs, ou plus prosaïquement des premières victimes. Ainsi, si un marché hétéroclite des *smart contract* de masse, marqué par la coexistence de smart contracts offshore, de *smart contracts* soumis à un droit étranger et smart contracts soumis au droit français venait à voir le jour, ce marché devrait vite apprendre des premiers échecs. Dès lors, à terme, il est plus que probable que **la loi du plus fort cédera devant la loi la plus forte** (c'est-à-dire, la loi la plus protectrice pour les consommateurs). Dans cette perspective, le droit français/européen présente de nombreux atouts.

Outre la prégnance de loi, nous anticipons que le consommateur imposera la soumission du *smart contract* à la loi européenne.

3/ La régulation des smart contracts par le droit pourrait de facto être imposée par le marché

Le *smart contract* ne pourra connaître un essor durable que s'il est proposé par les commerçants et accepté par les consommateurs. Dès lors, les commerçants exerçant dans le marché unique ne pourront pas, sur le long terme, ignorer les lois existantes sans risquer d'engager leur responsabilité ou adopter des comportements prédateurs, sans voir les consommateurs se détourner d'eux.

Ainsi, l'utilisation d'un *smart contract* ne pourra pas conduire les professionnels à méconnaître les obligations qui s'imposent à eux dans le monde non-numérique, et notamment le droit des consommateurs et les obligations en termes de LCB-FT et RSE. Cette dernière contrainte devrait conduire lesdits professionnels à ne pas accepter de conclure des *smart contracts* avec des personnes non-identifiées (ou dont le bénéficiaire économique ultime ne serait pas expressément identifié).

Du côté du cyber-consommateur, les promoteurs de *smart contract* devront compter avec la faculté des individus à se mobiliser - au moyen des réseaux sociaux notamment - pour informer ou dénoncer des comportements considérés comme iniques. Cette faculté (même s'il est très difficile de distinguer entre des « bonnes » et des « mauvaises » campagnes de mobilisation des consommateurs...) sera de nature à permettre de rétablir un certain équilibre entre le professionnel et le consommateur. D'un point de vue marketing, l'intérêt des commerçants sera donc d'utiliser, sur le marché unique, des *smart contracts* en conformité avec le droit européen.

A.1.2 : Le droit français/européen présente tous les atouts

En ce qu'ils placent la personne et non la marchandise en leur centre, les droits français et européen possèdent tous les atouts pour une régulation du smart contract permettant de faire peser la balance du bon côté entre « outil progrès » et « outil spoliation » : le droit des contrats, le droit de la consommation, le droit des données à caractère personnel, la législation LCB-FT et les modes alternatifs de résolution des différends.

1/ Un Droit protecteur et actif

Conscientes que les smart contracts « sont utilisés dans plusieurs domaines et ce, en l'absence de tout cadre juridique approprié »²², les institutions de l'Union européenne ont d'ores et déjà annoncé que réglementer les smart contracts étaient une de leur priorité.²³

C'est ainsi que des premières propositions de normes européennes visant à encadrer l'usage du *smart contract* ont vu le jour. Par exemple, le projet de Data Act²⁴ contient un article dédié au *smart contract* (article 30). Cet article, qui subordonne la validité du smart contract à un « degré très élevé de robustesse », impose notamment que les smart contracts puissent être « arrêtés » ou « réinitialisés ». Même si la rédaction de cet article est critiquée, force est de souligner que le projet de Data Act entérine la volonté du droit européen de façonner la destinée du smart contract.

Cette appréhension du *smart contract* par le droit européen nous paraît d'autant plus bienvenue que les droits français et européens détiennent les clefs d'un essor pérenne du *smart contract*.

2/ Un Droit des contrats français performant :

Rappelons que le droit des contrats français a récemment été structurellement refondu²⁵. L'esprit de cette réforme - et donc du nouveau droit des contrats - est défini dans le Rapport au président de la République²⁶. Ainsi, ce dernier identifie les deux piliers soutenant la réforme : l'efficacité et l'équilibre contractuel.

²² Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission concernant une législation sur les services numériques : adaptation des règles de droit commercial et civil pour les entités commerciales exerçant des activités en ligne, 2020/2019 (INL).

²³ Communication de la Commission du 8 février 2022, Programme de travail annuel de l'Union en matière de normalisation européenne pour 2022 (2022/C 66/01).

²⁴ Proposition de règlement du Parlement européen et du Conseil du 23 février 2022 concernant des règles harmonisées relatives à l'accès équitable aux données et à leur utilisation (Data Act), COM(2022) 68 final. 49

²⁵ Ordonnance du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations.

²⁶ Rapport au Président de la République relatif à l'ordonnance du 10 février 2016.

Si, à l'état de « nature », le *smart contract* atteint déjà indubitablement l'objectif d'efficacité en raison de l'immutabilité de son exécution, il méconnaît largement, en son état naturel, l'objectif d'équilibre contractuel. La soumission du *smart contract* au droit français des contrats permettra de garantir l'équilibre entre toutes les parties au contrat.

Le *smart contract* devra donc se mettre en conformité avec les dispositions impératives du droit des contrats comme notamment le consentement libre et éclairé du consommateur, la force majeure, l'interdiction des clauses abusives etc. Plus encore, le *smart contract* ne saurait écarter le règlement (alternatif ou judiciaire) des possibles litiges. Ce faisant, des modalités d'interventions d'un médiateur ou d'un juge dans le *smart contract* devront être prévues dès l'étape du ce

3/ Un Droit de la consommation et droits des consommateurs (DDC) :

L'essor du *smart contract* de masse ou grand public suppose une compatibilité avec le droit de la consommation au sens large, c'est-à-dire avec les dispositions prohibant un déséquilibre dans les relations contractuelles.

En pratique, deux difficultés devront être résolues : l'obligation de transmission d'informations dans un langage clair et compréhensible et le droit de rétractation des consommateurs dans les relations BtoC.

S'agissant de l'obligation de transmission d'informations dans un langage clair et compréhensible, il est évident qu'outre la compréhension du « contrat mot », le code ne saurait constituer un tel langage clair et compréhensible. En effet, par définition, la notion de code est intrinsèquement liée à celles d'abstraction et de secret. Cette difficulté pourrait être contournée par l'adoption d'une norme internationale à laquelle le *smart contract* déclarera adhérer.

S'agissant du droit de rétractation, un tel droit semble a priori peu compatible avec un *smart contract* dont le propre est l'auto-exécution (lorsque l'exécution est concomitante à la signature) et dans l'impossibilité d'interruption de cette exécution automatique (lorsque l'exécution est prévue postérieurement à la signature). Toutefois, le droit de rétractation devrait pouvoir être prévu, dans un certain délai immédiatement après la signature du *smart contract*.

4/ Le Règlement général sur la protection des données (RGPD)

Dès lors que le *smart contract* a vocation à utiliser des données personnelles, il ne peut espérer se soustraire à la législation européenne sur les données (RGPD).

Les parties à un *smart contract* devront pouvoir continuer à exercer leurs droits garantis par le RGPD tels que le droit à l'effacement, droit à la rectification ou encore le droit de ne pas faire l'objet d'une décision fondée uniquement sur un traitement automatisé. L'exercice de ses droits devra être prévu, en amont, lors de la rédaction du *smart contract*.

Permettre l'exercice des droits des personnes dont les données sont traitées impliquera au préalable d'identifier les responsables du traitement de données générés par le *smart contract*. Dans ce contexte, la CNIL a d'ores et déjà fournis quelques premières pistes²⁷. Ainsi, elle a notamment avancé que le développeur de *smart contracts* et les mineurs²⁸ pourraient être qualifiés de sous-traitants au sens du RGPD. Une telle qualification serait lourde de conséquences dans la mesure où le RGPD met nombre d'obligations à la charge des sous-traitants : obligation de transparence et de traçabilité, *privacy by design* et *by default*, obligation de garantir la sécurité des données traitées, obligation d'assistance, d'alerte et de conseil, etc.

²⁷ CNIL, « Blockchain – Premiers éléments d'analyse de la CNIL », septembre 2018.

²⁸ Dans le domaine des technologies blockchain, un mineur est une personne qui contribue à la sécurité et à l'intégrité du réseau en vérifiant et en traitant les transactions (blocs) émises sur le réseau.

5/ Une législation LCB-FT²⁹ performante :

On rappellera que la LCB-FT est au cœur des priorités européenne et française. En effet, les menaces que font peser le terrorisme et la délinquance économique et financière sur notre société, comme sur le marché européen, justifient cette législation contraignante qui s'impose à tous.

La lutte contre le blanchiment s'inscrit dans un double objectif : d'une part, prévenir les activités criminelles en les privant de fonds et, d'autre part, assurer la solidité, l'intégrité et la stabilité du système économique et financier.

Un développement des *smart contract* de masse en dehors de cette législation est inenvisageable.

6/ Médiation et règlement amiable :

La rapidité des transactions n'a de sens que si elle est couplée à une rapidité de résolution des litiges (commerce et justice doivent impérativement rester au même niveau).

Les droits français et européen privilégient la tentative de résolution amiable des litiges puis la résolution alternative des litiges. C'est dans cet esprit que le Règlement *Platform to Business* impose que les plateformes proposent, dans leurs conditions générales, au moins deux services de médiation en cas de survenance d'un différend (article 12). Dans le même sens, le DSA prévoit que les destinataires d'un service de plateforme en ligne ont le droit de choisir tout organe de règlement extrajudiciaire des litiges en vue de résoudre les litiges relatifs aux décisions du fournisseur de plateformes en lignes (article 21).

Il apparaît alors que numérique et modes alternatifs de règlement des différends (MARD) ont pour partie vocation à se coupler et s'intégrer avec des outils comme les *smart contracts*. Cela semble particulièrement vrai s'agissant des conflits simples et répétitifs.

De surcroît, en matière commerciale, la justice française n'a pas hésité à se saisir du numérique, comme en attestent la numérisation de son greffe et le développement des activités sur la Blockchain (mouvement de titres de sociétés, hypothèques maritimes, etc.). Dès lors, il n'est pas illusoire de penser que la justice française sera en mesure de proposer des solutions à intégrer directement dans le code du *smart contract* en vue de garantir un accès numérique et automatique à la justice commerciale en cas de difficulté d'exécution.

Dans ces conditions, le droit français dispose de tous les atouts pour que soient intégrées dès la conception du smart contract les modalités du règlement des potentiels litiges.

Conclusion :

Les droits français et européen ne doivent pas être vus comme des obstacles, mais comme des boussoles pour le *smart contract*. Dès lors, selon M. Lucchesi, « **la France a vocation à devenir une terre d'accueil pour le smart contract** ».

Les droits français et européens sont des outils de nature à éviter que le *smart contract* se transforme en outil d'oppression de la partie faible par la partie forte. Dès lors, **il faut organiser la coexistence entre ces droits et le smart contract**. L'essentiel reste à faire, car à ce jour, il n'existe pas de réglementation globale du *smart contract*. Ce dernier étant régulé indirectement au travers de la technologie blockchain.

A.2 Approche sectorielle

Une des particularités actuelles des règles qui encadrent les *smart contracts* réside dans le fait qu'elles relèvent de règles sectorielles traduisant des degrés d'adaptation et de développement relativement variés – pour ne pas dire contrastés – selon les secteurs d'activités concernés.

Cette régulation sectorielle fait essentiellement référence aux mesures réglementaires et de conformité qui sont appliquées à l'utilisation de la technologie blockchain dans différents secteurs économiques à l'image de la finance, de la santé ou encore de l'immobilier pour se limiter à quelques domaines significatifs.

A.2.1 : Régulation dans le domaine financier

Si, à ce jour, il n'existe pas de cadre réglementaire spécifique aux smart contracts, des lois et réglementations existantes peuvent s'appliquer à leur utilisation dans le domaine financier. On peut notamment citer la directive sur les marchés d'instruments financiers (MiFID II), le règlement général sur la protection des données (RGPD) ou encore la directive sur les services de paiement (DSP2). À ces réglementations existantes s'ajoute un cadre normatif en gestation : le Data Act.

En Europe, la régulation des *smart contracts* dans le domaine financier est un domaine en évolution et en développement constant. Cette régulation des *smart contracts* - essentielle dès lors que « **les comportements voraces de la finance traditionnelle se répéteront sur la Blockchain** » (P. Person) - dépend en grande partie des réglementations existantes dans le domaine financier et des initiatives spécifiques prises par les organismes de réglementation. Actuellement, il n'existe pas de cadre réglementaire spécifique aux *smart contracts*, mais les lois et réglementations existantes peuvent s'appliquer à leur utilisation dans le domaine financier.

En pratique, le cadre réglementaire applicable aux *smart contracts* financiers est déterminé par différentes directives et règlements, tels que la directive sur les marchés d'instruments financiers (MiFID II), le règlement général sur la protection des données (RGPD) et la directive sur les services de paiement (DSP2), le règlement sur la lutte contre le blanchiment et le financement du terrorisme (LCBFT). Ces réglementations ont des implications pour l'utilisation des *smart contracts* dans des domaines tels que les marchés financiers, les services d'investissement, les paiements et la protection des données personnelles.

Par ailleurs, certains pays de l'UE ont pris des mesures spécifiques pour réglementer les *smart contracts* dans le domaine financier. Par exemple, la France a adopté une loi en 2019 qui reconnaît la valeur juridique des « registres distribués » (**Cf. Glossaire**), y compris les *smart contracts*, et définit un cadre juridique pour leur utilisation.

De fait, la régulation des *smart contracts* financiers est un domaine complexe et en constante évolution. L'ensemble des acteurs cherche à évaluer les implications et les risques potentiels associés à l'utilisation des *smart contracts*, tout en cherchant à promouvoir l'innovation et le développement de la technologie blockchain.

On se rend compte de ce processus de « tâtonnement » législatif dans le cadre de la proposition de règlement sur l'harmonisation des règles d'accès et d'utilisation équitable des données (dit "Data Act") publiée par la Commission européenne, le 23 février 2022. Au titre des nombreuses dispositions proposées, certaines traitent spécifiquement des *smart contracts*, notion usitée dans le cadre des blockchains.

L'article 2 (16) de la proposition Data Act définit le *smart contract* comme "a computer program stored in an electronic ledger system wherein the outcome of the execution of the program is recorded on the electronic ledger". Cette définition fait ainsi des smart contracts des outils techniques intégrés dans un registre électronique, c'est-à-dire dans "un enregistrement électronique inviolable de données assurant l'authenticité et l'intégrité des données qu'il contient, l'exactitude de la date et de l'heure de ces données ainsi que de leur classement chronologique" au sens du projet d'article (53) du règlement eIDAS tel que modifié par la proposition de modification de Règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique. En pratique, le registre électronique est notamment connu grâce aux technologies de blockchain.

Désormais, le lien entre *smart contract* et registre électronique devrait donc reposer sur un texte juridique de portée générale mais on perçoit la difficulté s'agissant de l'application (ou pas) de certains dispositifs au secteur financiers. L'article 11 de la proposition de Data Act reconnaît les *smart contracts* au titre des mesures techniques appropriées que le détenteur des données peut appliquer pour empêcher tout accès non autorisé aux données et pour garantir le respect des conditions contractuelles convenues pour la mise à disposition des données. Le texte européen précise que ces mesures ne doivent pas entraver l'exercice des droits reconnus aux utilisateurs conformément aux dispositions adoptées par ailleurs dans le Data Act (notamment à des fins d'interopérabilité et de portabilité des données).

En conséquence, l'élaboration des *smart contracts* doit tenir compte des contraintes d'accès et de mise à disposition des données, contraintes qui résulteront des accords contractuels entre les détenteurs de données et les utilisateurs, et des dispositions du Data Act applicables. De fait, d'autres principes juridiques peuvent trouver à s'appliquer, dont la réglementation relative à la protection des données personnelles, ou en cas d'application plus sectorielle, la réglementation applicable en matière bancaire ou assurantielle par exemple.

Mais au-delà de ce constat, on mesure aussi les difficultés qui subsistent encore afin d'optimiser la répartition de la valeur des mêmes données entre les différents acteurs économiques concernés, et plus particulièrement celles liées à l'utilisation des objets connectés et au développement de l'internet des objets.

L'article 30 du Data Act stipule que les *smart contracts* devraient inclure des mécanismes de contrôle d'accès rigoureux³⁰, ainsi que la possibilité de résilier ou d'interrompre toute transaction relative auxdits contrats. Possiblement adapté au domaine de l'internet des objets, pour lequel ce texte a initialement été pensé, il apparaît qu'une telle contrainte pose question dans le domaine de la Finance Décentralisée (DeFi). Surtout, T. Schrepel soulève une question essentielle : « **un smart contract dont l'exécution peut être interrompue constitue-t-il encore un smart contract dès lors que, en théorie, la caractéristique première de ce dernier est d'être immuable ?** ».

³⁰ L'article 30, §1 de la proposition de Data Act exige que les smart contracts relatifs au partage de données respectent les exigences suivantes : robustesse (a), garantie de suspension et de terme de l'exécution des transactions (b), archivage des données permettant la traçabilité des opérations passées (c), contrôle des accès (d). Le respect de ces exigences essentielles par le smart contract pourra faire l'objet d'une attestation de conformité (article 30, §2 et §3).

A.2.2 : Régulation dans le domaine de la santé

En matière de santé, plusieurs corpus juridiques trouveront à s'appliquer aux smart contracts. Ainsi, les smart contracts seront notamment appréhendés par le Règlement général sur la protection des données (RGPD) et la Loi informatique et libertés (LIL) à travers le prisme des données de santé. La loi française sur la télémédecine et la téléconsultation pourrait également s'appliquer aux smart contracts utilisés dans le cadre de consultations médicales à distance.

Dans le domaine de la santé, les *smart contracts* sont encadrés juridiquement par diverses réglementations et lois existantes. Nous nous bornerons à examiner la situation en France de manière à décrire la diversité et la difficulté de gérer l'ensemble des contraintes légales et réglementaires.

En premier lieu, la protection des données personnelles est une préoccupation majeure dans le domaine de la santé. Le Règlement général sur la protection des données (RGPD), qui est applicable dans toute l'Union européenne, établit les règles relatives à la collecte, au traitement et au stockage des données personnelles, y compris les données de santé. Les *smart contracts* utilisés dans le domaine de la santé doivent donc se conformer aux exigences du RGPD, notamment en ce qui concerne le consentement du patient, la confidentialité des données et la sécurité des informations personnelles.

En second lieu, la loi relative à l'informatique, aux fichiers et aux libertés (loi Informatique et Libertés) régit également la collecte et le traitement des données personnelles, y compris les données de santé. Elle impose des obligations en matière de sécurité et de confidentialité des données, ainsi que des conditions strictes pour leur traitement. Les *smart contracts* qui traitent des données de santé doivent être conçus de manière à garantir la confidentialité et la sécurité des informations médicales.

En troisième lieu, la loi française prévoit des règles spécifiques pour la télémédecine et la téléconsultation, qui peuvent être liées à l'utilisation de *smart contracts*. Par exemple, la loi du 24 juillet 2019 encadre la pratique de la télémédecine en France et définit les conditions de réalisation des consultations médicales à distance. Les *smart contracts* peuvent être utilisés pour faciliter les paiements, la gestion des dossiers médicaux ou la coordination des soins, mais ils doivent être conformes aux exigences légales de la télémédecine.

Enfin, il est essentiel de souligner que l'utilisation des *smart contracts* dans le domaine de la santé soulève des enjeux éthiques et de responsabilité. Les professionnels de la santé doivent notamment veiller à ce que les décisions prises par les smart contracts soient conformes aux normes médicales et légales, et à ce qu'ils conservent le contrôle sur les actions automatisées. Les questions liées à la responsabilité en cas d'erreurs ou de dommages causés par les smart contracts doivent également être prises en compte.

A.2.3 : Régulation dans le domaine immobilier

La régulation des smart contracts dans le domaine immobilier est au moins tout aussi fournie. Ainsi, les smart contracts pourraient se voir appliquer des dispositions du Code civil, du Code de la construction et de l'habitation, de la Loi Alur ou encore plus largement des réglementations spécifiques.

À l'image de ce que nous avons observé dans le domaine de la santé, les *smart contracts* dans le domaine immobilier sont encadrés juridiquement par divers dispositifs légaux et réglementaires.

Tout d'abord, les *smart contracts* relèvent des dispositions du Code civil, à commencer par les règles relatives à la formation des contrats, à la capacité des parties, à la validité des contrats, à l'obligation de fournir des informations claires et précises ainsi qu'à l'exécution des contrats.

Ensuite ils relèvent du Code de la construction et de l'habitation qui régit les transactions immobilières, les règles de construction, les droits et obligations des parties, les garanties...

À cela nous pouvons ajouter, s'agissant de l'accès au logement et à un urbanisme rénové, la Loi Alur qui comprend des dispositions spécifiques concernant les contrats de location et de vente de biens immobiliers. Cette loi impose notamment des obligations d'information, de transparence et de protection des locataires et des acquéreurs.

D'autres dispositifs spécifiques doivent également être mentionnés dès lors que certaines transactions immobilières peuvent être soumises à des réglementations spécifiques, telles que la vente en l'état futur d'achèvement (VEFA) ou le bail commercial. Les *smart contracts* utilisés dans ces transactions devront donc se conformer aux réglementations spécifiques qui leur sont applicables.

Enfin, il ne faut pas négliger les conditions d'enregistrement et de recours au notaire dans les transactions immobilières. Si les *smart contracts* peuvent être utilisés pour automatiser certaines parties du processus, la présence d'un notaire reste requise pour valider et authentifier la transaction et donc l'ensemble des contraintes légales doivent être respectées dans ce cadre.

Même si les *smart contracts* ne sont pas encore largement utilisés dans le domaine immobilier il peut donc y avoir des incertitudes quant à l'application pratique des réglementations existantes même si les principes fondamentaux du droit des contrats, du droit immobilier et des réglementations spécifiques restent pertinents s'agissant de la mise en œuvre des smart contracts dans le domaine immobilier.

Au total, on constate que dans le domaine financier, la régulation de la blockchain vise à protéger les investisseurs et les consommateurs contre les fraudes et les abus, tout en favorisant l'innovation et la concurrence. Les régulateurs financiers cherchent à s'assurer que les entreprises utilisant la blockchain respectent les normes en matière de lutte contre le blanchiment d'argent, de financement du terrorisme, de protection de la vie privée et de sécurité des données...

Dans le domaine de la santé, la régulation vise à protéger les données des patients et à garantir leur confidentialité, tout en permettant un accès plus facile aux données médicales pour les patients et les professionnels de la santé. Les régulateurs dans ce domaine cherchent également à s'assurer que les entreprises utilisant la blockchain respectent les normes de sécurité des données et les réglementations en matière de protection de la vie privée des patients.

Dans le domaine immobilier, la régulation a plutôt pour ambition de faciliter les transactions immobilières et d'accroître la transparence du marché. L'objectif est de s'assurer que les entreprises utilisant la blockchain respectent les normes en matière de protection des consommateurs et de conformité réglementaire.

En considérant l'état actuel des dispositifs légaux et réglementaires, on peut estimer que la régulation sectorielle de la blockchain vise à la fois à favoriser l'innovation et à protéger les intérêts des investisseurs, des consommateurs et des parties prenantes, tout en garantissant la conformité réglementaire et le respect des normes en matière de protection des données et de la vie privée mais cela se fait dans un cadre hétérogène et rendu complexe par l'empilement des règles.

B/ NOS RECOMMANDATIONS

Les droits français et européen constituent donc un terreau extrêmement favorable au développement du *smart contract*. S'il venait à se développer, sur le marché unique, dans un climat de compréhension et de sécurité, le *smart contract* pourrait devenir l'outil de référence des relations commerciales dans un avenir très proche (2 à 5 ans). Pour ce faire, encore faut-il qu'un accompagnement soit mis en place, ou à tout le moins qu'une impulsion soit donnée.

Dans ce contexte, nous distinguerons nos recommandations relatives aux sujets du *smart contract* (B.1) et celles relatives à l'objet du *smart contract* (B.2).

B.1 : Les recommandations relatives aux sujets du smart contract

Le *smart contract* dispose de nombreux atouts pour obtenir les faveurs du grand public de manière durable. Afin que la transition vers le smart contract se fasse et pour réduire les risques tenant à son utilisation, « **il faut accompagner les différents acteurs** » (M. Khazzaka). La transition vers cet outil technologique doit être collective.

Recommandation n° 1 : Éduquer les consommateurs

Le développement durable du smart contract suppose la confiance du consommateur et du professionnel. Parce qu'une telle confiance ne peut être construite sur une méconnaissance des risques induits par le recours au smart contract, il est indispensable d'éduquer les consommateurs et de forger leur esprit critique pour leur permettre de déjouer d'éventuels pièges.

On ne peut proposer de nouveaux outils sans expliquer comment ils fonctionnent !

On ne peut lutter contre des outils potentiellement toxiques sans développer l'esprit critique des consommateurs !

a. Le consommateur doit comprendre comment fonctionne le *smart contract*

L'avenir du *smart contract* suppose qu'il ne soit perçu par le consommateur que comme un outil. Le *smart contract* ne doit donc pas devenir une idole numérique à laquelle il conviendrait de se soumettre aveuglément.

Il faut enseigner dès le plus jeune âge les rudiments de l'environnement numérique (comme la Blockchain, les cryptos, etc.) dans lequel évoluent les smart contracts. Il nous semble en effet totalement utopique de prétendre confier à un consommateur l'appréciation de la qualité d'un *smart contract* si, dès le départ, ce consommateur ne comprend pas l'environnement numérique dans lequel le *smart contract* s'inscrit.

Il faut ensuite enseigner dès le plus jeune âge les rudiments du *smart contract* et notamment sa caractéristique essentielle qu'est l'exécution automatique. En effet, de la même manière qu'il est nécessaire d'initier les jeunes générations aux dangers physiques de la route, il n'est pas inconcevable de les initier aux conséquences de ce nouvel outil.

b. Le consommateur doit développer son esprit critique vis-à-vis des *smart contracts*

Nous sommes tous quotidiennement confrontés à des arnaques par courriels, SMS, faux sites Internet et cela à toutes les étapes de notre quotidien (amende, renouvellement de carte vitale, délai de livraison d'un colis). La délinquance plus ou moins astucieuse s'est emparée de ces nouveaux outils pour tenter de bernier les plus naïfs comme les moins vigilants. Il serait irresponsable de considérer que les *smart contracts*, de la même manière, ne seront pas instrumentalisés par cette délinquance astucieuse.

Recommandation n° 2 : Éduquer les professionnels vendeurs

En parallèle de l'éducation des consommateurs, il est au moins aussi essentiel d'éduquer les professionnels vendeurs. En effet, ces derniers devront apprendre à recourir au smart contract afin de répondre à la demande de simplification du processus contractuel émanant des consommateurs.

Le règne du clic comme expression de la volonté du consommateur ne fait que commencer et le *smart contract* va probablement en constituer l'aboutissement ultime. Concrètement, la généralisation du recours au *smart contract* permettra, lors d'une transaction depuis son téléphone, de simplifier la transaction notamment en supprimant la phase de validation de paiement puisqu'elle se trouvera, de fait, intégrée dans le *smart contract*.

Les professionnels de demain ne peuvent sérieusement envisager de ne pas suivre leurs consommateurs dans leur volonté de simplification du processus contractuel par le recours au numérique. Cela d'autant plus que l'avenir semble être à la convergence numérique c'est-à-dire au regroupement des outils numériques anciennement indépendants. Dans un tel contexte d'accélération et de facilitation des échanges commerciaux, le smart contract est appelé à jouer un rôle essentiel.

Il appartiendra donc à chaque professionnel de réfléchir à la création d'un modèle économique permettant la commercialisation de son produit et/ou service au moyen d'un *smart contract*. Cela d'autant plus que le *smart contract* ouvre de nouveaux horizons au professionnel vendeur : « **le smart contract constitue tout à la fois une promesse d'automatisation des marchés existants et une perspective d'accès à de nouveaux marchés** » (F. Mauléon).

Dès lors, les professionnels, soit directement, soit par l'intermédiaire de leurs syndicats professionnels, doivent s'interroger dès à présent sur la manière de traduire en code informatique leur processus contractuel en déterminant notamment les conditions permettant de déclencher le processus de vente.

Enfin, il ne suffira pas pour les professionnels vendeurs de développer un tel savoir-faire. Encore faudra-t-il faire savoir au public par des opérations marketing qu'un tel savoir-faire existe.

Recommandation n° 3 : Développer les développeurs

Disposer, d'une part, de consommateurs désireux d'avoir recours à la technologie pour se simplifier leur quotidien et, d'autre part, de professionnels susceptibles d'offrir leurs produits et leurs services ne suffira pas pour permettre l'essor des smart contracts. Encore faudra-t-il que des développeurs puissent coder des smart contracts conformes aux attentes des parties.

Le développeur informatique ou codeur est celui qui transforme le « contrat mot » en « contrat code ». Il rédige un cahier des charges fixant les objectifs (et les besoins) des utilisateurs et décrivant les solutions techniques envisagées. Pour écrire le programme informatique, il utilise des logiciels prêts à l'emploi (progiciels) qu'il adapte aux besoins spécifiques du projet.

Il fera aussi partie des « auditeurs ». En effet, la confiance dans le *smart contract* et l'administration des potentiels différends ne pourra émerger qu'en présence de personnes susceptibles d'éclairer (a priori comme a posteriori) les parties ou le juge sur les qualités techniques du *smart contracts*.

Là encore, il faut continuer à développer l'écosystème technologique français et l'excellence des écoles françaises (l'école est toujours l'avenir de la nation). Plusieurs dimensions sont à conserver à l'esprit :

- Développer les développeurs **en France**. En pratique, cela ne devrait pas poser de difficultés majeures dès lors que la France est un haut lieu de la technologie informatique.
- Développer les compétences **pédagogiques des développeurs**. **Il appartient aux développeurs d'aider les professionnels à opérer une transition vers des modèles de distribution basée sur les smart contracts**. Le travail de vulgarisation entrepris par le présent livre blanc devra dès lors être le quotidien des développeurs.
- Développer les **compétences techniques** des développeurs. En pratique, cela implique d'accroître les efforts tenant à l'essor de l'IA ; cette dernière ayant le pouvoir de doper le potentiel des développeurs. En effet, grâce à l'IA, il ne s'agit plus pour les développeurs de créer le code de toutes pièces, mais uniquement de vérifier et compléter le code généré automatiquement par l'IA.
- **Conserver en France** les développeurs qui y ont été développés. Il est essentiel de lutter contre le débauchage des meilleurs développeurs français par les grandes puissances technologiques (notamment les États-Unis). En pratique, cela implique d'encourager et de faciliter le développement des start-ups, afin de ne pas contraindre les ingénieurs formés dans les écoles françaises à s'expatrier pour exercer leurs talents.

Développer les développeurs est d'autant plus indispensable qu'« **à ce jour, nous manquons de bras humains pour auditer les smart contracts et vérifier leur conformité technique** » (M. Khazzaka).

Recommandation n° 4 : Impliquer les juridictions et créer une juridiction spécialisée

Dès lors que le juge ne saurait être écarté du smart contract, il est indispensable d'impliquer les juridictions dès aujourd'hui dans la régulation du smart contract. Cette implication devra toutefois être pensée avec attention, notamment quant au moment d'intervention du juge dans les litiges impliquant des smart contracts.

Dernier intervenant - et non des moindres - *au smart contract* : le juge, qui doit rester l'ultime tiers de confiance en cas de litige concernant un *smart contract*.

Celui-ci doit impérativement être au fait du développement des smart contracts, et ce, même si nous avons précédemment recommandé qu'il n'intervienne qu'à la fin du processus, c'est-à-dire après épuisement d'un mode de règlement alternatif des litiges.

L'implication des juridictions recouvre deux dimensions :

- La sensibilisation et la formation des juridictions sur les enjeux du *smart contract* ;
- Le passage de « l'épreuve du jugement » par le smart contract : le *smart contract* devra nécessairement être validé par le juge à un moment ou un autre lorsque les premiers litiges arriveront devant les juridictions.

Parmi les bonnes fées qui devront se pencher sur le berceau du *smart contract*, le juge figure en bonne place. Surtout, le juge ne doit pas attendre d'être confronté au *smart contract* pour s'interroger à son sujet, au risque d'y jeter un mauvais sort lorsque ce jour viendra. Ainsi, les juges doivent dès à présent commencer à se demander si le *smart contract* est un contrat ou pas.

Les rédacteurs du présent livre blanc considèrent que si le juge aura un rôle important à jouer, ce rôle sera toutefois limité à ce qui suppose une évaluation, une appréciation, une estimation. En d'autres termes, le juge connaîtra de tout ce qui relève de la subjectivité (subjectivité qui est totalement inconnue du *smart contract*). En effet, à la différence du cerveau humain, le système d'exploitation du *smart contract* ne comprend que les conditions objectives construites sur le modèle « IF x, THEN y ». Dès lors, si le principe, la structure et l'exécution du smart contract devraient échapper au contrôle du juge (à l'exception néanmoins d'une possible différence entre le « contrat mot » et le « contrat code »), l'existence et la validité du consentement ainsi que la réalisation - ou pas - des conditions seront au cœur du contrôle du juge.

Il semble difficile de demander que les juges soient tous familiers du codage informatique. Dans ces conditions, dès lors qu'ils seront saisis de litige concernant la face technique des *smart contract*, les juges vont devoir s'appuyer sur des experts. La question du développement d'un pool d'experts judiciaires pour consulter/auditer l'algorithme est également ouverte.

Dans ces conditions, une sensibilisation des juridictions à ce nouveau phénomène commercial est indispensable. Pour ce faire, il semblerait opportun que soit créé un pôle de magistrats (de formation civile, commerciale, administrative et pénale) qui deviendrait les référents sur ces sujets. Il conviendrait aussi d'y associer éventuellement les autorités de police.

Recommandation n° 5 : Impliquer les autorités répressives

Dès lors que des smart contracts frauduleux pourraient voir le jour, il convient d'envisager une implication des autorités répressives afin de permettre notamment une éradication sans délais de tels smart contracts qui auraient été signalés par des consommateurs.

Même avec un consommateur éduqué et des professionnels de bonne foi, il existera toujours sur le marché des *smart contracts* proposés par des escrocs. De la même manière que la part des anges est un phénomène indissociable à la fabrication ou au transport d'un produit, la part du diable sera indissociable de l'essor du commerce électronique par l'intermédiaire des *smart contracts*. Cela d'autant plus que, comme le souligne T. Schrepel, « **l'une des difficultés majeures de la matière numérique et notamment de la Blockchain est que celui qui ambitionne de contourner une régulation peut parvenir à ses fins au moyen de la technologie** ».

À titre d'exemple, la valeur des fraudes à la carte bancaire en France de 2009 à 2021 est passée de 266 millions à 464 millions d'euros. Si l'on peut espérer qu'il n'en sera pas de même avec le *smart contract*, il serait toutefois plus prudent d'adopter une vision réaliste et donc de se préparer à la vigilance pour pouvoir les identifier.

Une fois ces *smart contract* délictuels identifiés, le vrai défi sera d'instaurer une procédure permettant de les signaler et de les faire éradiquer sans délais par les autorités compétentes. À l'immédiateté de l'exécution des *smart contracts* lorsque les conditions sont satisfaites, il convient de répondre par l'immédiateté de l'éradication.

Il appartiendra aussi de sensibiliser « les gendarmes » sur le rôle qu'ils auront à jouer pour lutter contre la délinquance dite astucieuse, dès lors que ce type de délinquant ne manquera pas de trouver formidable les capacités offertes par le *smart contract*.

B.2 : Les recommandations relatives à l'objet du smart contract

Recommandation n° 6 : Encourager et accélérer l'essor des MNBC

L'essor de l'euro numérique constituerait un remède à l'instabilité de la valeur des cryptomonnaies, qui est de nature à entraver le développement des smart contracts. Dans ce contexte, il faudra non seulement que l'euro numérique soit mis en circulation dans l'UE, mais encore que la pratique se saisisse de cette monnaie.

Le *smart contract* ne pourra exprimer son plein potentiel que dans un environnement où les cryptomonnaies sont utilisées. Or, l'utilisation à grande échelle des cryptomonnaies imposera une certaine stabilité de la valeur de celles-ci. Comment les consommateurs pourraient-ils en effet durablement avoir confiance et donc utiliser les *smart contracts*, si la valeur des cryptomonnaies utilisées pour l'exécution du *smart contract* peut disparaître (ou être substantiellement amputée) du jour au lendemain ?

On ne peut raisonnablement ajouter à l'incertitude inhérente au passage à l'économie numérique total un autre aléa sur la valeur de la contrepartie financière utilisée (pour plus de détails, voir annexe 4). Afin de pallier la problématique de la sécurité de la cryptomonnaie privée, la seule réponse qui nous semble présenter, à court terme, les garanties de sécurité les plus importantes est la monnaie numérique de banque centrale (MNBC) (**Cf. Glossaire**).

Cette réalité est bien comprise de la Chine, qui expérimente actuellement un projet de MNBC, (le *e-yuan*) dans les grandes municipalités chinoises. Si la Chine est en donc déjà au stade de l'expérimentation pratique, l'Union européenne en est encore à l'étape de la théorie.

Ainsi, le 28 juin 2023, la Commission européenne a présenté une proposition de cadre juridique pour la mise en circulation d'un « possible euro numérique ». Le chemin est toutefois encore très long avant la mise en circulation d'un euro numérique. En effet, l'adoption de cette proposition de la Commission par le Parlement européen et le Conseil sera insuffisante : la Banque centrale européenne (BCE) décidera seule s'il y a lieu d'émettre un euro numérique, et à quel moment.

En tout état de cause, l'euro numérique ne verra pas le jour avant plusieurs années. En effet, le gouverneur de la Banque de France anticipe un lancement « potentiel et progressif à partir de 2027 ou 2028 »³².

³² <https://www.latribune.fr/entreprises-finance/banques-finance/euro-numerique-la-banque-de-france-precise-les-contours-967153.html>

Dans ce contexte, une accélération du calendrier de lancement de l'euro numérique paraît indispensable pour garantir un essor du smart contract sur le marché européen. Cela d'autant plus qu'il faudra non seulement que les **MNBC soient mises en circulation dans l'UE**, mais encore que la **pratique se saisisse de cette monnaie** (ce qui implique que la MNBC soit librement accessible).

À défaut, toute situation possible du smart contract sera probablement à risque :

- le *smart contract* pourra se développer en utilisant une cryptomonnaie qui, si elle s'effondre, portera un coup fatal à la crédibilité de cet outil ;
- le *smart contract* se développera sans utilisation de cryptomonnaie, ce qui amputera de manière importante ses capacités ;
- le *smart contract* se développera avec l'utilisation d'une MNBC étrangère, ce qui pourra poser rapidement des questions de souveraineté économique.

Recommandation n° 7 : Encourager la standardisation sous conditions du smart contract

L'établissement de standards de smart contracts suppose deux volets : les conditions d'établissement de tels standards (dans la transparence) et leur contenu. Il pourrait notamment être envisagé que ces standards contiennent, d'une part, une liste des instruments à mobiliser lors du recours à un smart contract et, d'autre part, un tronc commun assimilable à des conditions générales (auquel pourraient s'ajouter des modalités de personnalisation).

Si réglementer la structure du smart contract est essentiel, cela ne sera guère aisé. En effet, comme le souligne T. Schrepel, « **le risque de la standardisation est de conduire à une uniformisation des smart contracts et ce faisant de freiner l'innovation** ».

Cette exigence de réglementation de la structure du *smart contract* recouvre plusieurs dimensions :

1. **Existence de standards de smart contracts** : la fixation d'une norme internationale ou ISO de *smart contracts* permettrait de faciliter l'accès à ce nouveau produit tant au niveau des consommateurs qu'au niveau des professionnels appelés à les utiliser. Cela permettrait aussi de réduire les risques de contestation judiciaire.
2. **Transparence des standards de smart contracts** : la transparence est une condition essentielle de la confiance des consommateurs. Cette transparence est d'autant plus indispensable que « **des standards de *smart contracts* particulièrement opaques ont déjà vu le jour et sont déjà utilisés en pratique** » (P. Person).
3. **Protection des innovations technologiques par le biais du secret des affaires** : la transparence a pour seule limite la protection de l'innovation technologique. En effet, le prix de la transparence ne peut être le sacrifice de la protection des innovations technologiques. Ainsi, si un professionnel concerné devra certifier que son *smart contract* a intégré ledit standard cela ne l'empêchera pas d'assortir, notamment pour les conditions particulières, chaque *smart contract* d'innovation technologique qui devront rester protégées par le secret des affaires. Cela, pour garantir audit professionnel l'avantage concurrentiel conféré par ses investissements technologiques

Une fois établie la nécessité d'un standard de *smart contract* se pose la question du contenu d'un tel standard.

À nos yeux, un tel standard devra comporter une présentation tant des outils à utiliser lors du recours à un *smart contract* que d'un tronc commun (assimilable aux conditions générales d'un contrat) répliquable pour tous les smart contracts. Il va de soi que ce tronc commun devra être accessible en open source gratuitement.

Parce que les *smart contracts* n'ont pas vocation à être identiques, il serait pertinent d'ajouter dans cette norme des modalités de personnalisation du *smart contract*, variables en fonction des caractéristiques du produit ou du service vendu (assimilable aux conditions particulières d'un contrat).

Ainsi, ce standard pourrait d'abord consister en l'énumération des instruments à mobiliser lors du recours à un *smart contract* :

- une blockchain
- une crypto monnaie
- un wallet
- les conditions auxquelles le smart contract s'auto-exécute
- l'oracle chargé d'inscrire la réalisation des conditions dans la blockchain
- un procédé de signature.

Il semble difficile d'aller plus loin et donc de proposer nominativement tel ou tel prestataire. En effet, cela reviendrait à privilégier un prestataire et donc porter atteinte aux règles de concurrence. Dans ces conditions, afin de ne pas laisser les **consommateurs et professionnels livrés à eux-mêmes dans la jungle numérique, nous recommandons l'établissement d'un tiers impartial chargé de la notation de la fiabilité des différents prestataires de *smart contract*.**

Ce tiers impartial serait notamment chargé de comptabiliser et d'informer le public quant au :

- nombre de *smart contracts* utilisant telle blockchain
- nombre de *smart contracts* utilisant telle cryptomonnaie
- nombre de *smart contracts* avec telle blockchain et telle cryptomonnaie ayant abouti
- nombre de *smart contracts* avec telle blockchain et telle cryptomonnaie ayant conduit à un litige.

Recommandation n° 8 : anticiper une nouvelle approche du règlement des litiges liés à l'utilisation des smart contracts

Dès lors que les smart contracts n'engendreront pas une disparition des litiges, il serait opportun d'anticiper une nouvelle conception du règlement des litiges les concernant. Dans cette optique, il pourrait notamment être envisagé d'opérer un traitement différent des litiges tenant aux conditions objectives du smart contract et des litiges tenant à ses conditions subjectives. L'on pourrait favoriser le développement de modes de règlement alternatifs.

Le smart contract est présenté comme la solution anti-litige, dès lors que l'exécution est automatique et ne nécessite donc aucune action des parties. Le smart contract ne laisserait donc aucune place aux faiblesses humaines que seraient la versatilité (le refus d'honorer l'engagement), la chicane, l'interprétation, l'incertitude ou l'hésitation. Il ne faut pas s'y tromper : cette prétendue sécurité juridique « absolue » est illusoire. Le smart contract ne va donc pas supprimer les litiges. Plus encore, le smart contract pourrait bien démultiplier les litiges.

Comprendre cette réalité impose de redevenir à la définition du smart contract : celui-ci est un protocole informatique qui exécute un accord préalable entre les parties si les conditions sont réunies. Il se décompose donc en deux étapes. D'abord, un accord traditionnel conclu entre plusieurs personnes avec des mots (le « contrat mots »), qui est, ensuite, transcrit en un code informatique (le « contrat code »). Tout le contentieux traditionnel du « contrat mots » va donc continuer à s'appliquer. À cela va s'ajouter le nouveau contentieux du « contrat code ». Les litiges ne vont pas disparaître, mais se démultiplier.

Cette démultiplication des litiges ne doit pas être vue comme une fatalité. Il convient au contraire de s'interroger dès aujourd'hui sur des approches innovantes qui pourraient être adoptées.

8.1 : Distinguer les litiges tenant aux conditions objectives du smart contract et ceux tenant aux conditions subjectives

Il nous semble falloir distinguer les litiges tenant aux conditions objectives du *smart contract* et les litiges tenant aux conditions subjectives du *smart contract*.

Par « litige tenant aux conditions objectives du smart contract », nous entendons les litiges relatifs à l'application mécanique du logiciel.

Si le professionnel utilise un logiciel conforme à un standard établi dans les conditions précédemment mentionnées, il conviendrait de prévoir une sorte de présomption de conformité. Cela opérerait un renversement de la charge de la preuve, de sorte qu'il appartiendrait au consommateur de prouver en quoi le smart contract qu'il a utilisé n'est pas conforme à ce standard. **À défaut de preuve contraire, ces critères objectifs du smart contract ne pourraient pas être remis en cause dans le cadre d'un contentieux**

À l'inverse, si le professionnel utilise un logiciel non conforme à un standard et/ou qu'il prétend conserver secret la structure de son smart contract au titre de la protection du secret des affaires, il appartiendrait au professionnel de prouver en quoi le smart contract qu'il a utilisé est conforme tant au standard qu'à l'engagement contractuel pris. Afin qu'un contentieux ne soit pas le prétexte, pour des concurrents, pour espionner les innovations technologiques d'un professionnel, il conviendrait - pour cette matière uniquement - de faire évoluer le Code de procédure civile et de **permettre que ce type de preuve ne soit plus soumis au principe du contradictoire et qu'il ne puisse être exposé qu'auprès du juge sans la présence de l'adversaire consommateur** (cette pratique existe notamment dans les pays anglo-saxons).

Les litiges tenant aux conditions subjectives du *smart contract* désignent les litiges relatifs au consentement des parties, à la réalisation matérielle des conditions ou encore à l'inscription des bonnes informations sur la Blockchain par l'Oracle.

8.2 : Prévoir systématiquement un mode de règlement alternatif des litiges.

Le standard précité devrait rendre obligatoire la possibilité de saisir, un système de règlement alternatif des litiges après l'exécution du smart contract, lorsqu'une des parties au smart contract considérerait ne pas avoir reçu satisfaction. En d'autres termes, après son auto-exécution (c'est-à-dire en cas de réalisation des conditions), **le smart contract serait programmé pour questionner chaque partie et leur demander si l'une d'elles n'a pas reçu satisfaction si elle souhaite demander une médiation**

L'on pourrait ainsi imaginer que le juge ne connaisse des litiges impliquant des smart contract que dans l'hypothèse où une solution alternative de règlement des différends (type Kleros ou équivalent) n'aurait pas abouti. **C'est en ce sens que F. Ast a développé un standard (baptisé « ERC 792 » Cf. Glossaire), permettant de connecter tout smart contract à Kleros de manière à rendre ledit smart contract arbitral par Kleros en cas de survenance d'un litige.**

L'intervention du juge ne serait limitée qu'aux hypothèses dans lesquelles une solution alternative n'aura pas pu être trouvée rapidement.

Synthèse des recommandations :

Le *smart contract* ne pourra connaître un essor pérenne que si toutes les parties prenantes sont impliquées dès aujourd'hui. Dès lors, il paraît nécessaire d'éduquer les parties au *smart contract* (consommateurs et professionnels vendeurs), les tiers au *smart contract* (les développeurs) et les autorités amenées à être confrontées au *smart contract* (juridictions et autorités répressives).

Les acteurs du *smart contract* ne sont les seuls à devoir évoluer : tel est encore le cas du *smart contract* en lui-même. Une telle évolution pourrait voir le jour au moyen d'un essor des MNBC, d'une standardisation du smart contract et de l'émergence d'une nouvelle conception du règlement des litiges liés à l'utilisation des *smart contracts*.

CONCLUSION

La révolution numérique va connaître une nouvelle vague, aussi puissante que celle d'internet, avec l'avènement du Web 3.0, et personne ne pourra l'arrêter. La prochaine figure destinée à prendre la tête de cette révolution est déjà connue : *le smart contract*.

S'il faut faire preuve d'une « peur prudence » face à ce nouvel élu numérique, il n'est nul besoin d'éprouver une « peur paralysante ». En effet, le *smart contract* n'est qu'un outil. Outil qui devra être manié avec précaution car, s'il peut permettre d'améliorer sensiblement les affaires humaines, il pourrait aussi devenir un auxiliaire d'oppression des populations les plus faibles.

Le smart contract ne doit pas être le nouvel outil qui permettra au renard de s'appropriier le fromage du consommateur – corbeau –.

Pour éviter cela, il est impératif d'étudier, de comprendre et autant que possible d'accompagner le *smart contract*. C'est le meilleur moyen pour ne pas subir un modèle imposé par un autre continent (comme les États-Unis, la Chine, l'Inde, ...) et incompatible avec nos valeurs européennes.

Accueillir avec bienveillance la modernité de l'outil et ses vertus (rapidité et sécurité des transactions) ne saurait en aucun cas conduire à un renoncement aux différentes protections progressivement érigées par le droit de l'UE.

Dans ces conditions, il faut que le *smart contract* soit européen... ou qu'il ne soit pas.

Pour connaître un essor pérenne sur le marché unique, le *smart contract* doit être accompagné. Si le « comment accompagner » a été largement évoqué dans le présent Livre Blanc, le « qui doit accompagner » demeure indécis.

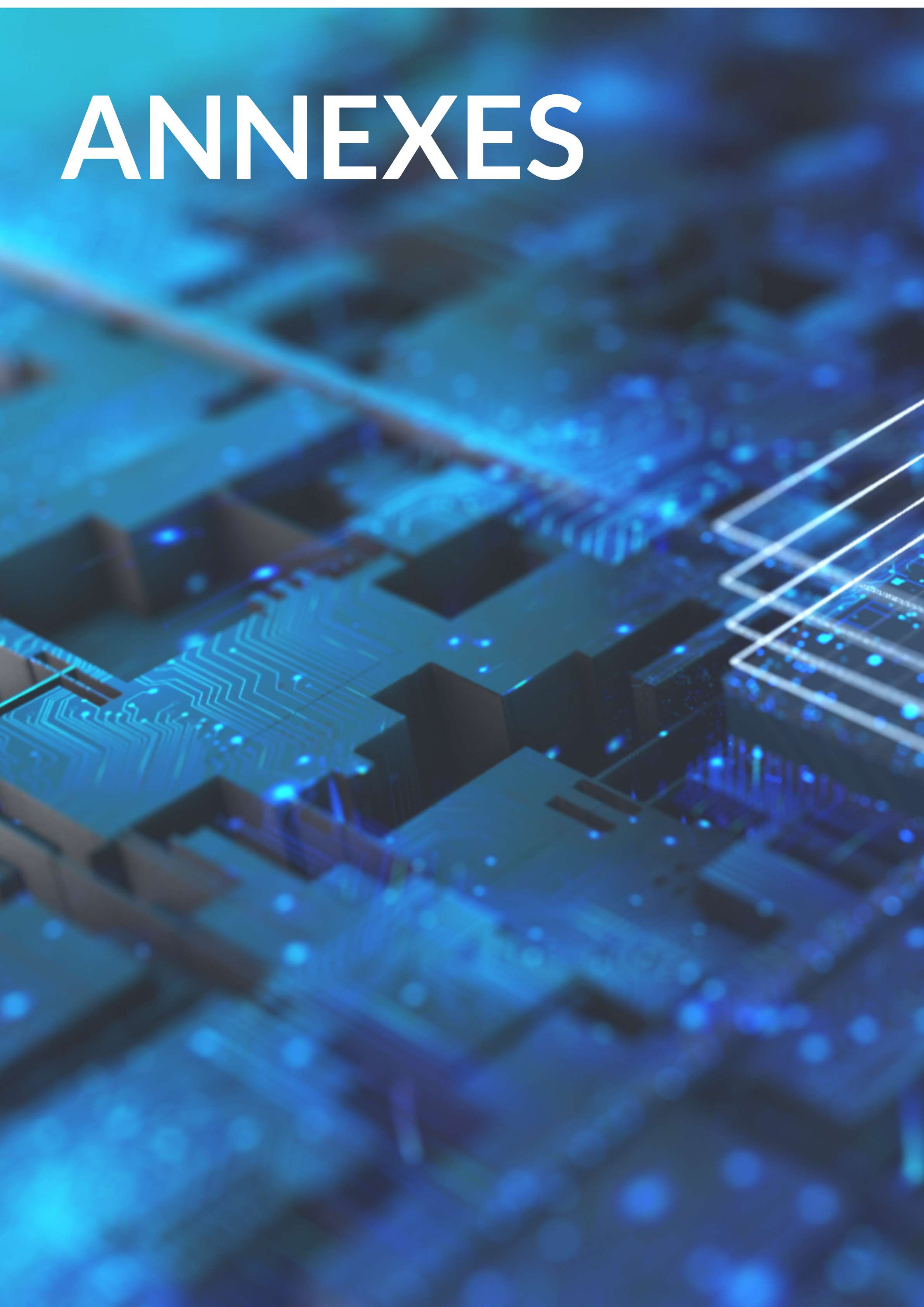
Bien évidemment, dans une démarche idéaliste, l'on ne pourrait qu'appeler de ses vœux une intervention au niveau de l'UE. Cependant, il est fort à parier que le délai de gestation particulièrement court des *smart contracts* ne soit pas compatible avec le délai de réflexion - particulièrement long - de l'UE. Si l'idéaliste appellera donc de ses vœux une intervention européenne, le réaliste tournera quant à lui son regard vers la France. **La France doit assumer son rôle de locomotive de l'Europe sur le terrain numérique et donner l'exemple.**

Si l'impulsion doit venir de la France, qui doit donner la donner ? Le secteur public ? le secteur privé ? Les deux ? Dans quelle proportion ? Avec quel budget ? Avec quels bénéfices ? avec quelles responsabilités ? Autant de questions dont la légitimité n'a pour équivalence que la complexité de la réponse à y apporter.

Reste la démarche collaborative, permise par le numérique, et qui conduirait à réunir les bonnes volontés autour d'un projet qui consisterait à créer le standard français du *smart contract* ainsi qu'un recueil des meilleures pratiques pour assurer la transition d'un contrat traditionnel dans une économie réelle vers le *smart contract* dans une économie numérique. Cette démarche est possible, notre livre blanc en est la preuve. Il faut cependant aller plus loin !

La prochaine étape pourrait consister à partir d'un cas d'école d'utilisation du *smart contract* (du type « comment passer de la vente du ticket de métro carton à un *smart contract* ? ») et à communiquer sur ses résultats, un tel groupe de travail pourrait conduire chaque professionnel français, à son niveau, à engager une transition vers le *smart contract*.

ANNEXES



Annexe 1 : Glossaire

Blockchain

Pour reprendre la définition de la CNIL³⁴, « la blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle. Elle constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création, sécurisée et distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne ».

Derrière l'unité de la notion de Blockchain se cachent deux réalités bien distinctes : les blockchains privées et les blockchains publiques.

Dans une blockchain privée, l'accès à la blockchain et son utilisation sont encadrés par un ou plusieurs acteurs centralisateurs. Par exemple, les Notaires du Grand Paris ont lancé une « blockchain notariale » en 2020. L'accès est donc privé.

A contrario, les blockchains publiques sont ouvertes à tous et donc librement accessibles. À ce titre, cette forme de blockchain peut être assimilée à « un très grand cahier, que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire, mais qui est impossible à effacer et indestructible » (J.-P. Delahaye). Les blockchains les plus célèbres sont des blockchains publiques. Ce faisant, lorsque la notion de blockchain est utilisée dans le débat public, c'est quasiment toujours afin de désigner une blockchain publique.

S'il existe une technologie Blockchain, il existe de très nombreuses applications de cette technologie. En d'autres termes, il n'existe pas une unique blockchain, mais de très nombreuses blockchains fonctionnant selon des règles différentes et permettant l'échange de cryptomonnaies différentes. Ainsi, chaque blockchain a sa propre cryptomonnaie.

À titre d'illustration, les blockchains les plus utilisées à ce jour sont les suivantes :

- **Bitcoin**, qui est la première blockchain créée, est incontestablement la plus populaire. Cependant, cette blockchain présente nombre d'inconvénients en ce que les frais de transaction sont élevés et qu'elle est réputée pour sa lenteur.
- **Ethereum** est la deuxième blockchain la plus importante à ce jour en termes d'utilisation. Sa particularité réside dans le fait qu'il s'agit d'une blockchain à code source ouvert. En pratique, cela permet à tout un chacun de créer des smart contracts. Ethereum a donc vocation à gagner en importance avec l'essor du smart contract. Cela d'autant plus qu'Ethereum présente des frais de transaction moins élevés que Bitcoin et est également réputée plus rapide.
- L'on peut encore citer la blockchain **Cardano**, qui est une nouvelle venue ayant le vent en poupe et dont l'ambition est de concurrencer Ethereum. L'avantage de Cardano réside incontestablement dans ses frais de transactions minimales et dans sa plus grande efficacité énergétique ainsi que dans son engagement environnemental.

Cryptomonnaies

Selon l'AMF³⁵, les « cryptomonnaies », plutôt appelées « cryptoactifs », sont des actifs numériques virtuels qui reposent sur la technologie de la blockchain, à travers un registre décentralisé et un protocole informatique crypté.

L'appellation de « cryptomonnaie » ne doit pas induire en erreur : **un cryptoactif n'est pas une monnaie** ! Ainsi, l'article L. 111-1 du Code monétaire et financier énonce que « la monnaie de la France est l'euro », excluant ainsi manifestement les cryptoactifs.

Cette réalité juridique connaît des fondements économiques. En effet, la littérature en économie attribue trois fonctions principales à la monnaie : une monnaie constitue tout à la fois un **moyen de paiement**, une **unité de compte** et une **réserve de valeur**.

Malgré l'essor des cryptoactifs, il demeure que ces derniers ne sont pas acceptés par tous comme un moyen de paiement. Ainsi, seule une certaine communauté accepte de voir une obligation monétaire éteinte au moyen de cryptoactifs. À ce titre, contrairement à une monnaie, les cryptoactifs ne constituent pas un produit universellement accepté comme moyen de paiement. Les cryptos ne remplissent donc que partiellement la fonction de moyen de paiement.

La notion d'unité de compte renvoie à l'aptitude d'une monnaie à exprimer la valeur d'échange d'un bien ou service sur un marché. Force est de constater que cette condition est satisfaite par les cryptoactifs. En effet, l'on peut aisément évaluer la valeur de n'importe quel bien en cryptoactifs.

Enfin, une monnaie doit pouvoir jouer le rôle de réserve de valeur. En d'autres termes, la monnaie doit conserver son pouvoir d'achat dans le temps. Ainsi, celui qui acquiert de la monnaie doit avoir la certitude qu'il peut la conserver pendant un certain temps sans qu'elle perde une part trop importante de sa valeur. C'est ce critère de réserve de valeur qui écarte définitivement la qualification de monnaie pour les cryptoactifs, dont les cours sont pour le moins chaotiques. À titre d'exemple, entre novembre 2021 et mai 2022 (soit 6 mois), le Bitcoin a perdu près de 55 % de sa valeur !

La justification de la fluctuation permanente de la valeur des cryptoactifs réside dans l'absence de tiers de confiance. Alors que la valeur d'une monnaie est, en principe, contrôlée par une Banque centrale, la valeur des cryptoactifs est uniquement déterminée par la loi de l'offre et de la demande.

Chaque cryptoactif a une valeur différente. Celui qui souhaite entrer dans le monde des cryptos est donc confronté à un choix particulièrement ardu. Cela d'autant plus qu'il existe à ce jour plus de 1 300 cryptoactifs (les plus connus étant le bitcoin, le ripple, l'ether, le litecoin, le nem et le dash).

Decentralized Autonomous Organisation (DAO)

Une *Decentralized Autonomous Organisation* (DAO) est « un regroupement de *smart contracts* écrits dans la blockchain choisie »³⁶, permettant à une pluralité d'individus de coopérer afin d'atteindre un objectif déterminé.

La particularité de la DAO réside dans son fonctionnement : d'une part, elle est dénuée d'autorité centrale et de toute idée de hiérarchie et, d'autre part, elle est parfaitement transparente dans la mesure où ses règles de fonctionnement sont inscrites dans le code enregistré sur la blockchain.

Les DAO constituent donc un nouveau type d'organisations sociales, dont le *smart contract* est la principale source de gouvernance. En pratique, la gestion collective de la DAO est opérée par le vote en ligne de ses participants. En plus de faciliter l'exécution des contrats, le *smart contract* apparaît donc également comme le vecteur de la création de sociétés numériques.

DeFi

Acronyme pour Decentralized Finance (finance décentralisée), qui désigne les services financiers de pair à pair (P2P) sur les blockchains publiques.

ERC 792

Kleros est un « service d'arbitrage décentralisé pour les litiges de la nouvelle économie » créé en 2017 sur la blockchain Ethereum et reposant sur les concepts de théorie des jeux développés par T. Schelling. En pratique, la solution Kleros s'articule autour d'un token appelé « Pinakion » (PNK). Pour espérer devenir juré sur Kleros, il faut d'abord faire l'acquisition de ces jetons et les déposer ensuite sur la plateforme. Les jurés sélectionnés ne connaissent pas l'identité des autres jurés, de sorte qu'ils ne peuvent pas communiquer entre eux. La solution Kleros repose donc sur le recours à des jurés présentés comme anonymes, impartiaux et incapables de communiquer entre eux.

Fork

Un fork désigne une mise à jour du réseau blockchain. Deux modèles de fork doivent être distingués : le soft fork et le hard fork.

Dans le cadre d'un soft fork, les nœuds nouvellement mis à jour sont compatibles avec les autres nœuds. Dès lors, aucune division de la blockchain n'est nécessaire.

Dans le cadre d'un hard fork, les nœuds mis à jour sont incompatibles avec les autres nœuds. Ce faisant, une division en deux de la blockchain est nécessaire entre les partisans des anciens nœuds d'une part, et les partisans des nœuds mis à jour d'autre part. La survenance d'un hard fork permet donc de revenir en arrière, de manière à effacer une partie de l'histoire de la blockchain.

Jeton non fongible (NFT)

Un non-fongible token (NFT) est un actif numérique unique associé à un support électronique parfois extrêmement banal (JPG, vidéo, etc.). L'unicité comme la traçabilité de cet actif unique sont certifiées par un dépôt dans la blockchain. En pratique, un NFT est généré par un smart contract.

Métavers

Le Métavers est « un monde virtuel immersif et constant en 3D où les utilisateurs interagissent par l'intermédiaire d'un avatar pour profiter de divertissements, faire des achats et effectuer des transactions avec des cryptoactifs, ou travailler sans quitter leur siège »³⁷.

Les virtualités des métavers sont potentiellement illimitées. En effet, théoriquement, tout ce qui est fait aujourd'hui dans le monde physique pourrait être fait demain dans un métavers. Ainsi, les différents métavers (Decentraland, The Sandbox, Roblox, etc.) comportent d'ores et déjà des magasins virtuels offrant à la vente des biens virtuels ou des NFT. Chaque transaction nécessite l'intervention d'un *smart contract*.

Miner Extractable Value (MEV)

La MEV désigne la valeur qui peut être directement extraite des *smart contracts* par les mineurs en qualité de rémunération liée à la cryptomonnaie.

En pratique, les mineurs reçoivent des centaines de transactions à intégrer dans la Blockchain et sont libres de sélectionner les transactions qu'ils souhaitent traiter. Dans ce contexte, les mineurs peuvent introduire leurs propres transactions avant les transactions des autres utilisateurs pour profiter d'un changement de prix ou encore pour revendre les actifs à un prix plus élevé à ces mêmes utilisateurs.

Les montants ainsi détournés par les mineurs s'avèrent colossaux. Ainsi, selon un rapport de la Banque des règlements internationaux³⁸, les mineurs auraient indûment détourné entre 550 et 650 millions de dollars sur la blockchain Ethereum depuis 2020.

Mineur

Personne qui est chargée de valider la transaction sur la blockchain.

Monnaie numérique de banque centrale (MNBC)

La monnaie numérique de banque centrale (MNBC) désigne un **élément de la base monétaire** qui s'échange au pair contre la monnaie fiduciaire et les réserves, que la banque centrale peut seule créer ou détruire, qui est **accessible 24/24h tous les jours de l'année**, et qui **circule sur une infrastructure numérique différente** de celle actuellement utilisée par la monnaie centrale pour un public donné³⁹.

Diverses applications potentielles de la combinaison entre MNBC et *smart contract* ont déjà pu être envisagées⁴⁰ :

- Collecte des impôts : les smart contracts pourraient permettre de collecter automatiquement la TVA lors de la vente de biens ou services.
- Prélèvement à la source : l'automatisation du prélèvement de l'impôt sur le revenu permettrait de réduire/supprimer le coût administratif supporté par les employeurs et faciliterait la lutte contre la fraude fiscale.
- Mise en œuvre d'une politique de monnaie hélicoptère : au sens strict de M. Friedman (1969), la politique de monnaie hélicoptère est la politique par laquelle une autorité monétaire donne directement de l'argent aux consommateurs sans passer par le crédit bancaire.

³⁷ Service de recherche du Conseil de l'Union européenne, « Metaverse – virtual world, real challenges », 29 juin 2022.

³⁸ <https://www.bis.org/publ/bisbull58.pdf>

³⁹ C. Pfister, « Paiements, monnaie et finance à l'ère numérique (1). Etat des lieux et perspectives à court-moyen terme », Fondation pour l'innovation politique, p. 45.

⁴⁰ P. Person, « Monnaies, banque et finance : vers une nouvelle ère crypto. Un enjeu de souveraineté et de compétitivité économique, financière et monétaire », Rapport parlementaire.

Neutralité du net

La neutralité du net constitue le principe fondateur d'Internet selon lequel toutes les données circulant sur Internet sont traitées à égalité, avec la même vitesse de transmission et la même accessibilité pour tous. En d'autres termes, la neutralité du web a pour objectif d'empêcher que certains flux d'information soient favorisés au détriment d'autres.

La neutralité du web constitue donc une forme de principe de non-discrimination propre à Internet.

Oracle

Pour que le *smart contract* puisse s'auto-exécuter dès lors que des conditions sont satisfaites, encore faut-il que celui-ci ait connaissance de la satisfaction de ces conditions dans la vie réelle. Ce faisant, la corrélation **entre monde virtuel de la blockchain et monde physique** est assurée par un tiers de confiance baptisé « Oracle ».

La fonction de ce dernier est de nourrir la blockchain d'informations récoltées dans le monde physique.

Registre distribué

Selon M. Khazzaka, un registre distribué peut être défini comme un « registre électronique simultanément consulté, enregistré et synchronisé par des acteurs autorisés et qui évolue par l'addition chronologique de nouvelles informations préalablement validées par la totalité des acteurs. Ces informations sont immuables (destinées à ne jamais être modifiées ou supprimées) »⁴¹.

Wallet

Un wallet ou portefeuille numérique, également connu sous le nom de portefeuille électronique, est un « appareil électronique, un service en ligne ou un logiciel qui permet à une partie d'effectuer des transactions électroniques avec une autre partie en échangeant des unités monétaires numériques contre des biens et des services »⁴².

Un wallet est d'abord une solution de paiement qui permet de payer ses achats en ligne, d'effectuer et de recevoir des virements, depuis un ordinateur, un smartphone ou une tablette. Il peut donc être souscrit auprès de banques qui les associent avec une carte bancaire classique. Ce type de wallet bancaire ne donne pas accès directement à la cryptomonnaie. Pour ce faire, il faut créer son wallet auprès d'un prestataire numérique.

Il existe de nombreux types de portefeuilles de cryptomonnaies, les plus populaires étant **le portefeuille de garde, le portefeuille non-dépositaire et le portefeuille physique**.

i. Le portefeuille de garde

Le portefeuille de garde (ou hébergé) est le portefeuille de cryptomonnaie le plus répandu. Il est dit hébergé car il se trouve détenu par le prestataire par lequel on passe pour acheter de la cryptomonnaie. Le tiers détient la cryptomonnaie et les clés privées dans l'intérêt de l'acheteur, de la même façon qu'une banque détient l'argent d'un client dans un compte chèque ou un compte-épargne. L'accès au compte suppose l'identification du titulaire. Ce type de portefeuille permet essentiellement l'achat, la vente, l'envoi et la réception de cryptomonnaies.

⁴¹ France Payments Forum, Glossaire des cryptopaiements, 2020, p. 10.

⁴² <https://www.inc-conso.fr/content/banque/le-portefeuille-electronique-ou-numerique>

ii. Le portefeuille non-dépositaire

Le portefeuille non-dépositaire (ou dépositaire autonome) est le portefeuille de cryptomonnaie pour lequel le prestataire fournit uniquement le logiciel nécessaire pour stocker les cryptomonnaies achetées. Le prestataire n'a donc pas accès aux fonds. L'accès n'est permis qu'à la personne titulaire du mot de passe (souvent appelé « clé privée » ou « seed phrase »). Ce type de portefeuille permet également des activités de cryptomonnaie plus avancées telles que le yield farming (génération de rendement), le staking, les prêts, les emprunts.

En conséquence, certains prestataires offrent la possibilité de disposer de plusieurs sortes de portefeuille dès lors qu'avec un portefeuille non-dépositaire, il n'est pas toujours possible d'acheter des cryptomonnaies avec de la monnaie *fiat* (comme des euros ou des dollars américains). Il est donc parfois nécessaire d'utiliser un portefeuille de garde pour convertir des monnaies fiat en cryptomonnaie puis de transférer la cryptomonnaie de son portefeuille de garde vers son portefeuille non-dépositaire.

iii. Le portefeuille physique

Enfin, il est possible d'utiliser un portefeuille physique qui est un appareil physique, de la taille d'une clé USB, qui stocke les clés privées de vos cryptomonnaies hors ligne. L'avantage essentiel est, une fois de plus, sécuritaire, dès lors qu'il réduit le risque de piratage informatique. Son utilisation reste cependant beaucoup plus complexe. De plus, ce système est plus coûteux en ce qu'il nécessite l'acquisition d'un appareil.

En définitive, il existe de nombreuses façons de stocker des actifs numériques dont la cryptomonnaie. Un tel stockage rend possible l'utilisation de la cryptomonnaie pour divers usages dans l'environnement numérique émergent qu'est le Web 3.0.

Web3 ou Web 3.0

Ce terme désigne un web décentralisé exploitant la technologie des chaînes de blocs (blockchain). C'est le nouvel environnement numérique global, dans lequel le *smart contract* a vocation à s'insérer. Le Web 3.0 se veut être l'héritier du Web 2.0 – la version actuelle de l'Internet ayant permis l'essor du commerce électronique et des réseaux sociaux –, lui-même héritier du Web 1.0, uniquement constitué de pages Web reliées par des hyperliens.

Annexe 2 : Comment faire pour exister sur le marché numérique ?

Nous prendrons l'exemple de M. Dupont lorsqu'il décide de se lancer dans l'univers numérique en achetant une cryptomonnaie, et ce quelle qu'en soit la raison

1/ L'existence sur le marché numérique comme préalable à l'utilisation d'un smart contract

La première difficulté à laquelle M. Dupont est confronté réside dans le choix de la cryptomonnaie à acquérir. Il existe en effet plusieurs milliers de cryptomonnaies. De plus, chaque jour, de nouvelles apparaissent et d'autres disparaissent. Le point commun de ces cryptomonnaies est qu'il n'y a ni garant ni contrepartie financière physique, Il n'existe donc aucune garantie lors de l'achat de cette monnaie électronique, sur sa valeur à moyen et long terme... voire même à court terme. Pour faire simple, la valeur d'une cryptomonnaie dépend uniquement du nombre de personnes qui souhaitent l'acheter. La cryptomonnaie est un bien virtuel comme un autre, soumis à la loi de l'offre et de la demande. Le sous-jacent est inexistant. Sa valeur est donc uniquement fonction du désir de l'autre de l'obtenir. La cryptomonnaie se distingue donc de la monnaie fiduciaire, pour laquelle la confiance accordée par l'utilisateur repose sur le principe de garantie assuré par une institution centralisatrice.

M. Dupont étant un homme prudent, il choisit entre les deux cryptomonnaies les plus connues et les plus établies : le Bitcoin (BTC) et l'Ether (ETH). Au moment de son choix (7 mai 2023 à 19 heures heure de Paris), 1 BTC valait 25 325 € et 1 ETH €1 718.70 €. Souhaitant symboliquement acheter une unité de cryptomonnaie et ayant des moyens limités, M. Dupont fait le choix d'acheter 1 ETH.

La seconde difficulté pour M. Dupont est de choisir la plateforme sur laquelle il va procéder à cette **acquisition**. Là encore, il existe à ce jour, de très nombreuses plateformes de prestataires offrant des services d'achat et de vente de cryptomonnaie entre particuliers. Là encore, il n'existe aucune garantie sur l'honnêteté et la viabilité financière de ses prestataires. En homme avisé, M. Dupont choisit une plateforme qui, d'une part fonctionne depuis quelques années et pratique des frais raisonnables, et, d'autre part, est enregistrée auprès de l'Autorité des marchés financiers (AMF).

Son choix ayant été fait, il lui faut suivre le processus d'ouverture de compte auprès de ce prestataire. Il va devoir ouvrir un compte chez le prestataire en communiquant sa pièce d'identité et un moyen de communication (comme un numéro de téléphone ou une adresse électronique). Une fois les vérifications d'usage accomplies, le compte sera ouvert. Ce compte constitue à la fois un compte sur une plate-forme et un compte bancaire qui, si la plate-forme est située à l'étranger devra faire l'objet d'une déclaration lors de la déclaration annuelle des revenus. Monsieur Dupont devra alors alimenter son compte en monnaies fiat. Il décide donc de transférer 2 000 € sur son compte personnel ouvert chez le prestataire.

M. Dupont va ensuite devoir ensuite déterminer un niveau de support et le type de support de conservation de la cryptomonnaie qu'il souhaite acheter. Le niveau de support constitue un niveau de prix que les participants à un marché estiment être un niveau d'achat acceptable pour un actif financier. Le support de conservation des cryptomonnaies (appelé WALLET) est le portefeuille numérique sur lequel la cryptomonnaie (qui est rappelons-le virtuelle) sera stockée. Le prestataire d'achat des cryptomonnaies peut proposer à Monsieur Dupont de lui fournir une prestation de stockage. M. Dupont peut aussi opter pour la création d'un Wallet auprès d'un prestataire spécialisé et indépendant du prestataire d'achat.

Maintenant que M. Dupont est présent sur le marché numérique, il va enfin pouvoir effectuer sa transaction en utilisant un smart contract.

2/ La réalisation de la transaction par le recours à un smart contract

Pour ce faire, Monsieur Dupont va se connecter sur sa plateforme d'échange et fixer son niveau de support. En d'autres termes, il va informer les potentiels vendeurs d'ETH qu'il est prêt à acheter 1 ETH à la valeur (hors frais de transaction) de 1 700 € par exemple. En cas de vendeur à ce prix-là (nous imaginerons ici qu'un certain Monsieur Durand est vendeur), l'opération va s'exécuter automatiquement par l'intermédiaire d'un smart contract.

En résumé, le smart contract consiste en un programme informatique auquel l'acheteur comme le vendeur a adhéré. Ce contrat est programmé pour s'exécuter si certaines conditions sont réunies :

- Monsieur Dupont est acheteur de 1 ETH ;
- Monsieur Dupont est acheteur à un prix en euro de 1 700 euros ;
- Monsieur Dupont a accepté de payer les frais (ou une partie) de transaction ;
- Monsieur Dupont dispose d'un portefeuille électronique sur lequel figure la somme nécessaire en euro ;
- Monsieur Durand est vendeur de 1 ETH ;
- Monsieur Durand est vendeur à un prix en euro de 1 700 euros ;
- Monsieur Durand à accepter de payer les frais (ou une partie) de la transaction ;
- Monsieur Durand dispose d'un portefeuille électronique sur lequel figure la somme nécessaire en Ether.

Une fois les parties ayant manifesté leur intention d'adhérer à cette transaction, le programme va vérifier que toutes les conditions sont réunies. Dans l'affirmative, ayant constaté la réunion des conditions, le smart contract va exécuter la transaction, d'une part, en débitant 1 700 € plus **les frais dans** le wallet de Monsieur Dupont et en lui créditant 1 ether, et d'autre part en créditant dans le wallet de Monsieur Durand 1 700 € moins les frais et en lui débitant 1 ether.

Annexe 3 : Quelques réflexions sur la souveraineté

En droit, la souveraineté peut être définie comme « la qualité en vertu de laquelle la forme d'organisation humaine la plus élevée, l'État, possède, à l'extérieur, l'indépendance vis-à-vis de tout autre État, à l'intérieur le pouvoir de constater le droit avec une direction dominante, pour lui-même comme pour ses sujets, et celui de leur imposer, en tant qu'ils coopèrent à la réalisation de buts sociaux, le devoir de se conformer à son but collectif suprême, cette qualité se manifeste extérieurement par le droit de l'État, dans ses rapports avec les collectivités qui le composent, de fixer librement sa propre compétence, dans les limites du principe supérieur du droit ; ou d'une manière plus brève, : la souveraineté est la qualité de l'État de n'être obligé ou déterminé que par sa propre volonté, dans les limites du principe supérieur du droit, et conformément au but collectif qu'il est appelé à réaliser ».

Si la souveraineté peut apparaître comme une notion conceptuelle difficile à appréhender, les formes d'atteintes à la souveraineté sont quant à elles aisément identifiables et compréhensibles. Ainsi, il est indiscutable que l'atteinte à la souveraineté peut d'abord se concevoir en termes militaires. En effet, c'est parce qu'un pays est attaqué qu'il voit sa souveraineté menacée. Toutefois, force est aujourd'hui de constater que l'attaque – et donc l'atteinte à la souveraineté – s'est souvent déplacée du champ de bataille au marché et à l'économie. Cette forme empiétement de la souveraineté est à géométrie variable, tant dans son intensité que dans son apparence.

La forme la plus anodine d'atteinte économique à la souveraineté française résulte du commerce international et prend la forme de l'anglicisme. Cela, notamment par onomastisme, comme en atteste la marque frigidaire, créée par General Motors et devenue synonyme de réfrigérateur. Plus prégnant encore, l'atteinte à la souveraineté peut résulter de ce qui est parfois qualifié de « pouvoir des tuyaux »⁴⁴.

L'idée derrière le « pouvoir des tuyaux » est aisément compréhensible : celui qui possède les tuyaux contrôle le monde. La meilleure illustration de cette réalité est fournie par Rockefeller, devenu l'homme le plus riche de son temps, en investissant dans les pipelines qui transportaient le pétrole sur le territoire américain. Le propriétaire du tuyau est donc étroitement associé à la valeur du produit transporté. Outre sa valeur économique, il dispose d'un pouvoir politique important, notamment lorsqu'il décide « de fermer le robinet ». Cela nous a d'ailleurs été rappelé très récemment lors du conflit ukrainien et de la fourniture de gaz russe.

Le pouvoir des tuyaux a pris une importance considérable au cours des dernières années dans le contexte de la révolution numérique. Il apparaît aujourd'hui clairement que le responsable du transport de la *data*, c'est-à-dire de l'information, détient entre ses mains un pouvoir d'influence considérable. On peut citer comme exemple le domaine audiovisuel. Les investissements chinois en Afrique dans le domaine de la TNT (à compte d'auteur !) permettent ainsi aux exploitants chinois de diffuser régulièrement des dessins animés en chinois, et ce pour favoriser l'apprentissage de la langue chinoise par la jeunesse africaine. Ces investissements privés (qui dans un premier temps sont favorables à l'État en ce qu'il le dispense d'investir dans des infrastructures) peuvent, dans un second temps porter atteinte à sa souveraineté.

La révolution numérique a accentué les risques d'atteinte à la souveraineté des États.

A. Les tuyaux changent mais le pouvoir demeure

Aujourd'hui, des atteintes à la souveraineté émergent sur de nouveaux terrains, autrefois jugées impraticables. Ainsi, autrefois confrontés uniquement à des atteintes par la terre, sur la mer et dans les airs, les États sont aujourd'hui confrontés à une menace située 20 000 lieues sous les mers. En effet, la quasi-totalité des flux numériques (99 %) transite par des câbles posés sur les planchers océaniques⁴⁵. Or, les GAFAM, désireux d'acquérir leur indépendance, ont des vues sur les câbles.

Dès lors que toute l'information circule à travers ces tuyaux, des risques considérables apparaissent quant à la sécurité des communications (espionnage) et à la « neutralité du net » (Cf. Glossaire).

Cette neutralité pourra-t-elle continuer d'être garantie si les câbles océaniques transportant la *data* sont détenus par un très petit nombre d'opérateurs ?

B. Nouveaux acteurs et nouveaux dangers

i. Les nouveaux acteurs

Traditionnellement, l'atteinte à la souveraineté était commise par un état concurrent. La révolution numérique a pour singularité qu'elle a vu des acteurs privés déposséder les états de leurs fonctions de régulation des nouvelles technologies.

Prenons pour exemple le cas de l'aviation commerciale (nouvelle technologie du siècle passé). Il s'agit d'une invention privée française (l'aéropostale) qui s'est développée internationalement. Face à son succès commercial, les États ont décidé que cette activité s'exerçait dans un espace aérien dont ils avaient la souveraineté, et l'on soumit à ce titre à une réglementation tant nationale qu'internationale.

Il en est allé différemment du monde du numérique et de l'Internet, dès lors que les précurseurs utopistes, ainsi que les premiers exploitants commerciaux, ont refusé l'intervention étatique au nom de la liberté... Ce refus était possible dès lors qu'Internet n'avait plus de frontières et en conséquence, les états n'étaient plus des interlocuteurs obligés. En résultat, il ne reste plus à ce jour que les GAFAM⁴⁶, qui comptent parmi les plus grosses valorisations boursières du monde (ces 5 sociétés américaines pèsent plus lourd que l'ensemble des entreprises du CAC 40) et disposent d'une puissance financière supérieure à celles de nombreux États.

Cette substitution n'est pas sans risque car la dépossession des États de la régulation des technologies numériques laisse sans contrepoids les nouveaux géants du numérique. Cela peut avoir pour effet d'effacer aujourd'hui les principes protecteurs érigés hier et garantis par les États. En effet, hier, ces technologies, comme ces principes protecteurs, étaient définis, appliqués et contrôlés par des États, au moyen notamment de conventions internationales.

Si cette guerre de souveraineté juridique n'est pas nouvelle, les acteurs de ce conflit ont donc changé. En effet, aujourd'hui, **les belligérants ne sont plus uniquement les États mais aussi les grandes plateformes (GAFAM)**. Ces GAFAM sont en capacité directement ou indirectement, de remettre en cause, en fait, les principes existants en droit en contrôlant tout simplement l'accès aux tuyaux⁴⁷. Il apparaît alors que, à défaut de principes protecteurs garantis par les états, les technologies numériques peuvent très rapidement passer d'outils d'émancipation individuelle à outils d'oppression collective.

⁴⁵ <https://medium.com/caium/vingt-mille-liens-sous-les-mers-g%C3%A9opolitique-des-c%C3%A2bles-internet-824a22ddfe59> 46 Google (Alphabet), Apple, Facebook (Meta), Amazon et Microsoft.

⁴⁷ La désactivation sur Facebook (pour non-respect des règles d'utilisation du réseau social) d'un compte ayant affiché le tableau de Gustave Courbet - « L'origine du monde » - en est la parfaite illustration.

ii. Les nouveaux dangers : le numérique permet d'influencer la décision collective

Notre démocratie repose sur le postulat que le citoyen est capable, c'est-à-dire qu'il sait ce qu'il fait. Cependant, cette capacité peut être fortement altérée par le numérique.

Au niveau international, il existe dans l'histoire récente au moins deux cas qui semblent le suggérer : la tentative du gouvernement russe d'influencer le résultat des élections présidentielles américaines⁴⁸ et le scandale Cambridge *Analytica*⁴⁹.

Ces deux événements ont, d'une manière différente, participé à influencer la décision collective dans le choix d'un président par le recours au numérique. La première a consisté à intervenir auprès de l'opinion publique pour discréditer un candidat par l'information, la seconde a permis d'identifier et de solliciter des électeurs qui auraient pu être passifs et ce uniquement en les ciblant à l'aide de leur data.

Certes, les tentatives d'influence de l'opinion ne sont pas nouvelles. La propagande a largement précédé l'apparition du numérique. Il a donc toujours existé un lien intime entre opinion publique et décision collective.

Cependant ces manipulations ont, avec le numérique, une efficacité nouvelle incommensurable du fait de l'immédiateté de la diffusion, de sa mondialité et de son caractère potentiellement viral. **En d'autres termes, les outils de propagande devaient, par le passé⁵⁰, être fabriqués, mais leurs sources permettaient de les identifier. Aujourd'hui, Internet et les réseaux sociaux constituent un espace existant, gratuit et souvent anonyme au niveau de la source.**

Que ce soit par les infox⁵¹ ou par le profilage avec des data, le numérique rend possible une sollicitation individuelle nouvelle qui permet d'agir sur le comportement des citoyens. Ces démarches semblent permettre l'activation des comportements individuels. Dans son dernier livre, Yuval Noah Harari parle de possibilité de « pirater les êtres humains » .

48 En 2016, des autorités américaines ainsi que le FBI ont dénoncé des interventions du gouvernement russe pour influencer les élections américaines (notamment par les révélations sur les courriels d'Hillary Clinton publiés sur les sites DCLeaks.com and WikiLeaks).

49 Toujours en 2016, il est prétendu que l'élection de Donald Trump a pu être favorisée par le recours au Big Data. Le candidat Trump a fait appel à la société Cambridge Analytica, dont l'activité consiste à fournir, aux entreprises et aux mouvements politiques, des stratégies et opérations de communication clés en main basées sur l'analyse des données à grande échelle. Ainsi, Cambridge Analytica annonce « utiliser les données pour changer le comportement du public ». Comme l'a reconnu Facebook, cette société aurait siphonné les données de 87 millions de ses utilisateurs pour identifier et solliciter dans la société américaine le très fort courant anti-élites qui pouvait favoriser l'émergence d'un candidat atypique.

50 Charlotte Lepri, « De l'usage des médias à des fins de propagande pendant la guerre froide », Revue internationale et stratégique 2010/2 (n° 78), p. 111-118.

51 Ex-fake news.

Annexe 4 : Illustrations de l'aléa sur la cryptomonnaie

Imaginons que Monsieur Dupont, achète des cryptomonnaies en prévision de l'exécution d'un *smart contract* qu'il entend conclure avec un vendeur professionnel (Société ALPHA), mais que la valeur de la cryptomonnaie se volatilise avant l'exécution du smart contract. Dans une telle hypothèse, il est fort à parier que Monsieur Dupont ne renouvellera pas l'expérience du *smart contract* en général.

De plus, il ne serait pas étonnant que Monsieur Dupont se retourne contre son vendeur, la société ALPHA pour tenter de rechercher sa responsabilité. Cela, en prétendant que c'est ce professionnel qui l'a contraint à acquérir des cryptomonnaies pour pouvoir réaliser la transaction espérée (sans l'avoir préalablement informé des risques) par l'intermédiaire d'un *smart contract*.

Imaginons maintenant que le *smart contract* ait parfaitement fonctionné et que la transaction se soit parfaitement déroulée entre Monsieur Dupont et la société ALPHA. C'est le vendeur professionnel qui pourrait se retrouver, à son tour, avec des cryptomonnaies ayant perdu une part substantielle de leur valeur après la transaction.

Les deux cas, l'opération serait une catastrophe économique, même si pour le second, ce serait un succès juridique.

L'objectif de ce livre blanc est d'une part de vulgariser une matière éminemment disruptive, technique et évolutive et d'autre part de s'interroger sur l'avenir possible du *smart contract*.

Le smart contract a-t-il un avenir au-delà de la cryptomonnaie ? Est-il transposable dans la vie des affaires ?

Dans l'affirmative, dans quelles conditions (quels sont les enjeux / risques) et par qui ?

Les rédacteurs partent du postulat que cet outil a un très bel avenir et qu'il rencontrera la faveur des consommateurs (en raison de son apparence de facilité et de rapidité). Dans ces conditions, les professionnels français et européens doivent contribuer à la détermination des standards de *smart contracts* et/ou des sujets sur lesquels une vigilance particulière sera nécessaire.

Cette nécessité s'impose, d'une part, dans une démarche de souveraineté européenne (ne pas contribuer à la détermination des standards reviendra de fait à la soumission au standard adopté par d'autres), et d'autre part afin que le *smart contract* ne devienne pas un outil de spoliation au service d'une minorité.

Enfin, même si le *smart contract* semble actuellement s'affranchir significativement des lois existantes, c'est uniquement parce que lesdites lois ne sont pas (encore) adaptées aux situations nouvelles créées par le *smart contract*. Le *smart contract* ne pourra pas durablement se développer, sur le territoire français, dans l'ignorance des règles juridiques européennes, qui sont le fruit de la lente recherche d'un équilibre entre les deux parties au contrat. C'est cet équilibre ancien qui va devoir être adapté à la situation nouvelle du smart contract. En effet, comme l'indique la Commission européenne, « la transformation numérique ne peut réussir que si elle fonctionne pour tous et pas seulement pour quelques-uns. Il s'agira d'un projet véritablement européen, une société numérique fondée sur les valeurs et les règles européennes ».

La publication de ce livre blanc a été réalisée avec le soutien de  LexisNexis®