L'émergence de la blockchain dans les relations contractuelles : Vers une nouvelle forme de confiance algorithmique ?

Alison Blondeau

L’émergence de la *blockchain* dans les relations contractuelles :

Vers une nouvelle forme de confiance algorithmique ?

Alison Blondeau

L’émergence de la *blockchain* dans les relations contractuelles :

Vers une nouvelle forme de confiance algorithmique ?

Alison Blondeau

2 avril 2021

À propos de l'auteure

Titulaire d'un Master en Droit de l'entreprise, Alison Blondeau est doctorante contractuelle depuis octobre 2018 sur le thème de la responsabilité en intelligence artificielle, sous la direction de Nathalie Nevejans, à l'Université d'Artois. Elle est également membre du Centre Droit, Éthique et Procédures (UR 2471) et membre de la Chaire IA Responsable (Université d'Artois).

Mail : blondeau.alison@gmail.com

Twitter : @AlisonBlondeau

LinkedIn : linkedin.com/in/alison-blondeau-a0a599165

Remerciements

À ma famille, mes amis, et mes collègues du Centre de recherche Droit, Éthique et Procédures et de l'Université d'Artois, à l'ensemble du personnel de la Bibliothèque universitaire de Douai, à tous ceux qui m'ont soutenue et qui ont cru en moi, je leur dis merci. Une pensée particulière à Sarah et Frédéric, pour leur soutien et leurs conseils.

À Monsieur Jean-Paul Delahaye, Professeur émérite d'informatique et de mathématiques, pour son extrême bienveillance et sa disponibilité. Une rencontre que je ne pourrai jamais oublier.

À Marielle pour sa patience et ces heures de corrections minutieuses, ainsi qu'à Cassandra pour sa lecture attentive, ses nombreux et précieux conseils, et sa bienveillance. Merci à toutes les deux pour leur soutien.

À Caroline, pour sa patience, sa présence et son soutien sans faille, jusqu'au bout et au-delà. Et à Alice, pour sa sagesse, sa positivité et sa confiance depuis le début. Merci à toutes les deux pour leur amitié inaltérable.

À ma professeure, directrice de mémoire et désormais directrice de thèse, Madame Nathalie Nevejans, une Grande Dame comme il est rarement permis d'en rencontrer et sans laquelle ma dernière année de Master, et sans aucun doute le restant de ma vie professionnelle, auraient été bien fades. Grâce à elle je vis une merveilleuse aventure. Merci pour sa disponibilité, ses encouragements et ses inestimables conseils tout au long de ce projet, mais également pour ces discussions sans fin plus enrichissantes et passionnantes les unes que les autres. Merci d'avoir cru en moi.

À mes parents, pour leur patience, leur confiance absolue, et pour m'avoir toujours permis de donner le meilleur de moi-même. Particulièrement à ma mère, pour son soutien indéfectible. Enfin, à mon petit frère qui, en toute situation, réussit toujours à me faire rire. Merci.

Sommaire

(Une Table des matières détaillée et un Index alphabétique figurent à la fin de l'étude)

À propos de l'auteure 3
Remerciements 4
Sommaire 5
Liste des abréviations 7

INTRODUCTION **14**

PARTIE 1

LES APPORTS DE LA* BLOCKCHAIN *EN TANT QUE

SYSTÈME INCUBATEUR DE CONFIANCE :

UNE VOLONTÉ DE SIMPLIFICATION DES RELATIONS CONTRACTUELLES

TITRE 1. Les *smart contracts* : programmation d'une modalité technique d'exécution inédite **53**

Chapitre 1. Renforcer l'efficacité de la force contractuelle : l'automatisation comme aide et suivi à l'exécution **54**

Chapitre 2. Amplifier l'efficacité de la force contractuelle : l'interconnectivité comme mise à exécution instantanée **110**

TITRE 2. La *blockchain* : promesse d'une sécurité juridique accrue **143**

Chapitre 1. Une variété de signature électronique existante **144**

Chapitre 2. Une variété de preuve algorithmique naissante **195**

PARTIE 2

LES SPÉCIFICITÉS DE LA* BLOCKCHAIN *EN TANT QUE

POTENTIELS FREINS À L'INSTITUTION D'UNE CONFIANCE ALGORITHMIQUE :

DES RÉSISTANCES COMPLIQUANT L'APPLICATION DES EXIGENCES JURIDIQUES ACTUELLES

TITRE 1. Incohérences entre *blockchain* et droit : un besoin d'adaptation . **243**

Chapitre 1. L'immuabilité, une difficile maîtrise des parties **244**

Chapitre 2. La décentralisation, une délicate intervention du juge étatique **300**

TITRE 2. Problèmes créés de l'utilisation faite de la *blockchain* : un manque de fiabilité 348

Chapitre 1. Les enjeux de la gouvernance 349

Chapitre 2. Les vulnérabilités fonctionnelles 384

CONCLUSION GÉNÉRALE 426

Annexes 431

Table des annexes 432

Bibliographie 444

Index alphabétique 476

Table des matières 488

Liste des abréviations

Abréviations	Libellés
aff.	*Affaire*
AFNOR	Association française de normalisation
AJ contrat	*Actualité juridique contrat*
AJ fam.	*Actualité Juridique Famille*
AJCA	*Actualité juridique contrats d'affaires*
AJDA	*Actualité juridique de droit administratif*
al.	alinéa
ANSSI	Agence nationale de la sécurité des systèmes d'information
ap. J.-C.	après Jésus-Christ
Arch. Phil. dr.	Archives de philosophie du droit
art.	article
art. cit.	article cité
ass. plén.	Assemblée plénière
av. J.-C.	avant Jésus-Christ
B2B	*Business-to-Business*
B2C	*Business-to-Consumer*
BOSP	Bulletin officiel du service des prix
BTC	*bitcoin(s)*
Bull. civ.	*Bulletin des arrêts de Chambres civiles de la Cour de cassation*
C.	Code
C. assur.	Code des assurances
C. civ.	Code civil
C. com.	Code de commerce
C. consom.	Code de consommation
C. énergie	Code de l'énergie
C. envir.	Code de l'environnement
C. mon. et fin.	Code monétaire et financier
C. patr.	Code du patrimoine

C. pén.	Code pénal
C. mut.	Code de la mutualité
C. route	Code de la route
C. tourisme	Code du tourisme
C. trav.	Code du travail
C. urb.	Code de l'urbanisme
c/	contre
C2C	*Consumer-to-consumer*
CA	Cour d'appel
Cass.	Cour de cassation
Cass. Civ.	Cour de cassation, Chambre civile
Cass. Com.	Cour de cassation, Chambre commerciale
Cass. Crim.	Cour de cassation, Chambre criminelle
CCNUCC	Convention-cadre des Nations unies sur les changements climatiques
CDE	*Cahiers de droit de l'entreprise*
CE	Conseil d'État
CERNA	Commission de réflexion sur l'Éthique de la Recherche en sciences et technologies du Numérique d'Allistene
CGI	Code général des impôts
CGU	conditions générales d'utilisation
Ch.	Chambre
CJUE	Cour de justice de l'Union Européenne
CNIL	Commission nationale de l'informatique et des libertés
CNRS	Centre national de la recherche scientifique
CNUDCI	Commission des Nations unies pour le droit commercial international
coll.	collection
collab.	*en collaboration avec*
comm.	commentaire
Comm. com. électr.	*Communication Commerce électronique*
Cons. const	Conseil constitutionnel
Const.	Constitution
Contrats, conc. consom.	*Contrats, concurrence, consommation*
CPC	Code de procédure civile
CPCE	Code des postes et des communications électroniques

CPI	Code de la propriété intellectuelle
CPP	Code de procédure pénale
CRPA	Code des relations entre le public et l'administration
CSE	Certificat de signature électronique
CSN	Conseil supérieur du notariat
CSP	Code de la santé publique
CSS	Code de la sécurité sociale
(dir.)	(sous la direction de)
D.	*Recueil Dalloz*
D. IP/IT	*Recueil Dalloz, droit de la propriété intellectuelle et du numérique*
Dalloz actualité	*Dalloz actualité (en ligne sur dalloz.fr)*
DAO	*Decentralized Autonomous Application* (organisation autonome décentralisée)
déc.	décision
décr.	décret
DEEP	dispositif d'enregistrement électronique partagé
délib.	délibération
dir.	directive
DP	*Dalloz périodique*
Dr. & patr. Mensuel	*Droit & patrimoine l'hebdo*
ECC	*Elliptic Curve Cryptography*
éd./ed.	édition/Edition (en anglais)
EEE	Espace économique européen
et al.	et autres
et s.	et suivants
ETH	*ether*
ETSI	European Telecommunications Standards Institute, c'est-à-dire l'Institut européen des normes de télécommunications
FAI	fournisseur d'accès à Internet
fasc.	fascicule
Gaz. Pal.	*Gazette du Palais*
Go	Giga octets
H.	House (USA)
I2D	*Informations, Données et Documents*
Ibid.	*Ibiden*, au même endroit

Id.	*Idem*
IGC	Infrastructure de gestion de clé (ou PKI en anglais, pour « Public Key Infrastructure »)
infra	ci-dessous
IoT	*Internet of Things* (« Internet des Objets »)
IP (adress)	Adresse IP, *Internet Protocol*
ISO	Organisation internationale de normalisation
JCl.	*Juris-Classeur*
JCl. Civil Code	*JurisClasseur Civil Code*
JCl. Com.	*Juris-Classeur Commerce*
JCl. Contrats-Distribution	*Juris-Classeur Contrats-Distribution*
JCl. Sociétés Traité	*JurisClasseur Sociétés Traité*
JCl. Roulois	*JurisClasseur Roulois*
JCP	*Semaine juridique (appelé aussi Juris-classeur périodique)*
JCP A	*Semaine juridique-Administration et collectivités territoriales*
JCP E	*Semaine juridique Entreprise et affaires*
JCP G	*Semaine juridique, édition générale*
JCP N	*Semaine juridique, édition notariale et immobilière*
JOAN Q	*Journal officiel (Questions réponses) Assemblée nationale*
JORF	*Journal officiel de la République française*
JOUE	*Journal officiel de l'Union européenne*
Juris-Data	*Juris-Data : banque de données juridiques*
JWT	*JSON Web Token*
KYC	*Know Your Customer* (règles de conformité « Connaissance client »)
L.	Loi
L. org.	Loi organique
LGDJ	*Librairie générale de droit et de jurisprudence*
loc. cit.	*loco citato*, passage précité d'un article ou d'un ouvrage
LPA	*Petites affiches (Les)*
M2M	*machine-to-machine*
MARC	modes alternatifs de règlement des conflits
MARL	modes alternatifs de règlement des litiges
Mo	méga octets
n.	note

n° /No.	numéro/Numéro (en anglais)
NF	Norme française
NTIC	Nouvelles Technologies de l'Information et de la Communication
op. cit.	*opere citato*, ouvrage cité précédemment
ord.	ordonnance
p. (pp.)	page (pages)
P2P	*Peer-to-Peer* (de pair à pair)
PME	petites et moyennes entreprises
PoS	*Proof of Stake* (« preuve de participation »)
PoW	*Proof of Work* (« preuve de travail »)
préc.	précité(e)(s)
prot.	protocole
prot. Nations Unies	protocole des Nations Unies
PSCo	prestataire de service de confiance
PUAM	Presses universitaires de l'Université d'Aix-Marseille
PUF	Presses universitaires de France
PUR	Presses universitaires de Rennes
rapp.	rapport
rapp. AN	rapport de l'Assemblée Nationale
rapp. Sénat	rapport du Sénat
RD bancaire et fin.	*Revue de droit bancaire et financier*
RDC	*Revue des contrats*
RDI	*Revue de droit immobilier*
règl.	Règlement
Rép. civ. Dalloz	*Répertoire Dalloz de droit civil*
Rép. com. Dalloz	*Répertoire Dalloz de droit commercial*
rép. min.	réponse ministérielle
Rép. pén. Dalloz	*Répertoire Dalloz de droit pénal et de procédure pénale*
Rép. pr. civ. Dalloz	*Répertoire Dalloz de procédure civile*
req.	requête
résol.	résolution
Rev. crit. DIP	*Revue critique de droit international privé*
Rev. éco. fin.	*Revue d'économie financière*
RID comp.	*Revue internationale de droit comparé*

RLDA	*Revue Lamy Droit des Affaires*
RLDC	*Revue Lamy Droit Civil*
RLDI	*Revue Lamy Droit de l'immatériel*
RSE	Responsabilité sociale et environnementale des entreprises
RTD civ.	*Revue trimestrielle de droit civil*
RTD com.	*Revue trimestrielle de droit commercial*
s.	suivants
S.	Senate (USA)
SAE	systèmes d'archivage électroniques
sect.	section
Sén.	Sénat
SPS	*Science… & pseudo-sciences*
supra	*ci-dessus*
t.	tome
TGI	Tribunal de grande instance
TI	Tribunal d'instance
TJ	Tribunal judiciaire
trad.	traduction, traducteur
UE	Union européenne
UN/CEFACT	Organisme de Facilitation des Procédures Commerciales et le Commerce Électronique des Nations unies
UNECE	Commission économique pour l'Europe des Nations unies
UNIDROIT	Institut international pour l'unification du droit privé
USD	dollar américain
v.	voir
vol./Vol.	volume/Volume (en anglais)

"Imagination is more important than knowledge.
For knowledge is limited, whereas imagination embraces the entire world,
stimulating progress, giving birth to evolution."
Albert EINSTEIN[1].

[1] VIEREK (George Sylvester), « What Life Means to Einstein », The Saturday Evening Post [online], 26 Oct. 1929, p. 17, http://www.saturdayeveningpost.com/wp-content/uploads/satevepost/Einstein.pdf.

Introduction

1. La notion de confiance. En 2007, le film *Live Free or Die Hard* réalisé par Len Wiseman met en scène une cyber-attaque planifiée par un groupe terroriste dont l'objectif final est d'anéantir les principales infrastructures économiques et gouvernementales des États-Unis d'Amérique. Ils cherchent dans un premier temps à s'introduire dans le système informatique du pays gérant à la fois les transports, l'énergie mais également toutes les communications à travers le territoire, et à pirater ses finances. Ils tentent dans un second temps de paralyser le pays en gelant informatiquement toutes les ressources contrôlées par le réseau, à l'instar des satellites, de l'électricité, du gaz, des radars, des marchés boursiers et bancaires, … Finalement, en une fraction de seconde, le chaos s'abat sur le continent. Il s'avère que, dans cette œuvre cinématographique, l'ensemble de ces ressources sont centralisées en un même point. Indubitablement, un constat s'impose : *hackers* et cryptographes sont tant capables de se rendre excessivement riches, que de provoquer la ruine des États-Unis – voire du monde entier. Or, l'état de l'art de ce type de systèmes montre leur vulnérabilité, comme en témoignent les cyber-attaques des grands groupes tels que Netflix[2], Amazon[3], Twitter[4], Google[5], Apple[6], Snapchat[7],

[2] BAYARD (Florian), « Netflix : ses abonnés victimes d'une tentative de piratage ! », *PhonAndroid* [en ligne], 20 sept. 2017, http://www.phonandroid.com/netflix-abonnes-victimes-tentative-piratage.html.
[3] « Une immense cyberattaque a visé des grands sites Web », *Le Figaro* [en ligne], 22 oct. 2016, http://www.lefigaro.fr/secteur/high-tech/2016/10/21/32001-20161021ARTFIG00343-des-grands-sites-web-perturbes-par-une-immense-cyberattaque.php.
[4] « Twitter confirme le piratage de comptes », *Le Figaro* [en ligne], 15 mars 2017, http://www.lefigaro.fr/flash-actu/2017/03/15/97001-20170315FILWWW00113-twitter-confirme-le-piratage-de-comptes.php.
[5] DURIEZ-MISE (Johann), « Les 5 piratages les plus inquiétants de 2014 », *Europe1* [en ligne], 24 nov. 2014, http://www.europe1.fr/high-tech/les-5-piratages-les-plus-inquietants-de-2014-2298585.
[6] *Id.*
[7] « Snapchat va mettre à jour son application après le piratage de millions de données », *20 minutes* [en ligne], 3 janv. 2014, https://www.20minutes.fr/web/1269287-20140103-20140103-snapchat-va-mettre-a-jour-application-apres-piratage-millions-donnees.

Orange[8], Target[9], eBay[10], Spotify[11], Deloitte[12], CNN[13], New York Times[14] ou encore FireEye qui a ensuite permis l'attaque de plusieurs agences gouvernementales des États-Unis d'Amérique[15]. Ces failles de sécurité manifestent la nécessité de s'interroger sur la fiabilité du système centralisé actuel. La technologie se propose d'y remédier afin d'éviter une crise de confiance des usagers.

Des relations d'affaires aux relations sociales, en passant par les relations institutionnelles, la *confiance* en l'autre est le fondement de toute relation humaine[16]. Concept central et naturel de vie en communauté, elle est de surcroît indispensable dans les relations contractuelles dès qu'il s'agit d'échanger un bien ou un service. De la négociation à l'exécution des dispositions contractuelles, sous le vocable « principe de bonne foi », elle apparaît directement ou indirectement à l'origine de diverses obligations liant les parties[17]. Aujourd'hui, que ce soit sur papier ou *via* Internet, la confiance joue le rôle de « contrat psychologique »[18] acceptant plus ou moins l'incertitude et rendant possible le véritable contrat[19]. Conclure un marché avec une personne qui n'inspire pas confiance est aussi difficile que d'accepter de saisir les numéros de sa carte bleue sur un site inconnu[20]. Selon certains auteurs, « la confiance est un état psychologique dans lequel l'intention d'accepter la vulnérabilité [de la situation] est fondée sur une attente positive vis-à-vis des intentions ou du comportement de l'autre »[21]. Il en découle que la relation

[8] BACHELERIE (Jean), « Orange : la sécurité de la messagerie oubliée », *Mediapart* [en ligne], 12 oct. 2017, https://blogs.mediapart.fr/jean-bachelerie/blog/121017/orange-la-securite-de-la-messagerie-oubliee.
[9] BOHIC (Clément), « Piratage : Wendy's rejoint Target et Home Depot sur la liste », *ITespresso* [online], 11 juill. 2016, https://www.itespresso.fr/piratage-wendys-target-home-depot-134310.html.
[10] « Piratage d'eBay : 145 millions de victimes potentielles », *Le Figaro* [en ligne], 23 mai 2014, http://www.lefigaro.fr/secteur/high-tech/2014/05/21/32001-20140521ARTFIG00249-victime-d-une-cyberattaque-ebay-recommande-de-changer-de-mot-de-passe.php.
[11] GRONDIN (Anaëlle), « Cyberattaques: Que peuvent faire les pirates avec vos données? », *20 minutes* [en ligne], 2 juin 2014, https://www.20minutes.fr/high-tech/1391121-20140602-cyberattaques-peuvent-faire-pirates-donnees.
[12] UTERSINGER (Martin), « Le géant du conseil Deloitte victime d'un piratage », *Le Monde* [en ligne], 25 sept. 2017, https://www.lemonde.fr/pixels/article/2017/09/25/le-geant-du-conseil-deloitte-victime-d-un-piratage_5191163_4408996.html.
[13] « Une immense cyberattaque a visé des grands sites Web », art. cit.
[14] *Id.*
[15] SANGER (David E.), « Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect », *New York Times* [online], 13 Dec. 2020, https://nyti.ms/2Kn2ZDo.
[16] GOSSA (Julien), « Les blockchains et smart contracts pour les juristes », *D. IP/IT* 2018, n° 7-8, p. 393.
[17] Notamment, C. civ., art. 1104, 1112 (négociations précontractuelles), 1112-1 (devoir d'information, erreur), 1123 (violation du pacte de préférence), 1130 (vices du consentement).
[18] MANGEMATIN (Vincent), *Des mondes de confiance : Un concept à l'épreuve de la réalité sociale*, CNRS Éditions via OpenEdition, 2016, pp. 63-64.
[19] *Ibid.*, p. 7.
[20] GOSSA (Julien), art. cit., *loc. cit.*
[21] « *Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another* » [notre trad.], ROUSSEAU (Denise M.), SITKIN (Sim B.), BURT (Ronald S.), CAMERER (Colin), « Not So Different After All: A Cross-Discipline View of Trust »,

nécessite un certain degré de confiance mutuelle pour que, psychologiquement, le contrat soit accepté. Cette « théorie de la confiance » mobilise en cela les notions propres au contrat hobbien[22]. En effet, chez Thomas Hobbes, l'état de nature n'est pas un état viable, mais un état de « guerre de tous contre tous », régi par des sentiments de défiance, de rivalité et de gloire, où chacun cherche l'auto-conservation au risque de céder à la bestialité. L'Homme peut pourtant quitter cet état primitif et sauvage s'il fait usage d'un contrat. Cependant, le penseur observe que s'il n'y a pas de garantie à la bonne exécution de cet engagement, les Hommes ne le respecteront que dans la mesure où cela servira leurs intérêts. Finalement, les Hommes n'ont qu'une solution pour garantir ce contrat, ils doivent faire confiance au « Léviathan » qui est un pouvoir coercitif créé lui-même contractuellement. En effet, l'objet du contrat d'association entre les Hommes est la garantie que l'adhésion au contrat instituant la paix sera respectée. Chacun passe une convention avec chacun, personne n'a confiance en l'autre mais tout le monde a confiance dans le Léviathan. De fait, le Léviathan n'est lié par rien puisqu'il *est* le contrat. Celui qui instituera donc la paix, sortira l'Homme de son état de nature et de domination, et le protègera dans cet environnement hostile, est un tiers appelé « tiers de confiance »[23].

Aujourd'hui, toute relation de confiance est protégée par un corps de Léviathan. Il en découle que le tiers de confiance est multiple et englobe un ensemble de professions, telles que les juges, les notaires, les plateformes d'intermédiation sur Internet, … Le contrat social actuel est imposé par un système d'abord étatique puis, progressivement, économique. En effet, les entreprises qui gèrent la communication par Internet assument de plus en plus des responsabilités auparavant exercées par les gouvernements. Seulement, depuis l'émergence de ce pouvoir économique et de l'univers du cyberespace, les choses se compliquent, et il s'avère de plus en plus difficile d'inspirer confiance aux Hommes. Entre cyberattaques, collectes et transferts illégaux de données[24], l'insécurité sévit. La question se pose alors de savoir si le contrat social de Thomas Hobbes, tel qu'il a été mis en place ces derniers siècles, est capable de lui résister[25]. Rebecca MacKinnon

Academy of Management Review [online], 1998, Vol. 23, No. 3, pp. 393-404, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.470.8322&rep=rep1&type=pdf.

[22] HOBBES OF MALMESBURY (Thomas), *Leviathan or the Matter, Forme, & Power of a Common-wealth Ecclesiasticall and Civill*, London. Printed for Andrew Crooke, 1651.

[23] GUILHAUDIS (Élise), « Comprendre la blockchain à travers l'étude d'un cas pratique : le covoiturage "Blockcar" », *RLDI* 2017/12, nº 143, p. 1.

[24] V. par exemple, « États-Unis : Google poursuivi en justice pour le suivi abusif des données de géolocalisation », *France TV Info* [en ligne], 21 août 2018, https://www.francetvinfo.fr/monde/usa/etats-unis-google-poursuivi-en-justice-pour-le-suivi-abusif-des-donnees-de-geo-localisation_2904719.html ; « Un gang vendait les données personnelles de clients d'Apple en Chine », *L'Express* [en ligne], 9 juin 2017, https://www.lexpress.fr/tendances/produit-high-tech/un-gang-vendait-les-donnees-personnelles-de-clients-d-apple-en-chine_1916393.html.

[25] GUILHAUDIS (Élise), art. cit., p. 1.

théorise une nouvelle entrée de l'Homme dans l'état de nature lorsqu'elle évoque l'âge hobbien du cyberespace[26]. Selon elle, depuis la révolution numérique, les « netziens », c'est-à-dire les citoyens du Net, sont en proie à la défiance et seraient à la recherche d'une nouvelle entité de confiance qui pourrait les protéger autant que les guider[27]. C'est la raison d'être de l'apparition de la technologie *blockchain*. En effet, nombre d'auteurs pensent qu'elle serait à même de prendre en charge en toute autonomie cette « défiance qui existe naturellement entre les Hommes », tout en leur laissant le soin de fixer en amont les règles de vie en société[28].

2. Définir le « tiers de confiance ». Conscients qu'ils ne peuvent réussir à se faire confiance mutuellement, les Hommes ont établi un système faisant intervenir des tiers réputés neutres et intègres pour sceller leurs engagements réciproques et s'assurer de leur respect[29] ; un système centralisé, un corps de Léviathan. La notion de « tiers de confiance », distincte de la notion européenne des tiers de confiance numériques[30], est en réalité assez vague[31]. Communément, un tiers de confiance est une personne qui, en principe, du fait de ses compétences, sa mission ou son statut, dégage une aura de fiabilité et d'intégrité[32]. La doctrine considère le tiers de confiance comme « un acteur qui facilite la transaction entre deux parties en les rassurant »[33]. Il est donc possible d'y entrevoir, d'une part, les tiers de confiance historiques et, d'autre part, la génération de tiers de confiance apparue à la suite d'Internet.

Les tiers de confiance historiques consistent en des entités étatiques telles que les professions réglementées ou les services d'administration publique. C'est à partir de la fin du XV^e^-début XVI^e^ siècle que la fonction publique prend réellement forme[34]. Après s'être employés à construire l'État monarchique en tant qu'agents du Roi sous Philippe Le Bel, ils deviennent officiers ou commissaires sur ordre du Roi François I^er^ pour les besoins de

[26] MACKINNON (Rebecca), *Consent of the Networked: The Worldwide Struggle for Internet Freedom*, ed. Basic Books, 2012, cité dans : GUILHAUDIS (Élise), art. cit., *loc. cit*.
[27] Pour plus de détails sur le sujet, v., MACKINNON (Rebecca), *Consent of the Networked: The Worldwide Struggle for Internet Freedom*, *op. cit*.
[28] GUILHAUDIS (Élise), art. cit., *loc. cit*.
[29] BERBAIN (Côme), « La blockchain : concept, technologies, acteurs et usages », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 6.
[30] Pour plus d'informations sur les tiers de confiance numériques, v., le site officiel de la Fédération des tiers de confiance numériques, https://fntc-numerique.com/fr/accueil.html.
[31] DOUVILLE (Thibault), VERBIEST (Thibault), « Blockchain et tiers de confiance : incompatibilité ou complémentarité ? », *D.* 2018, pp. 1144 et s.
[32] *Id.*
[33] BOUDÈS (Thierry), « La blockchain déchaîne les questions ! », *Annales des Mines – Gérer et comprendre* 2018/1 (mars 2018), n° 131, p. 83.
[34] Ordonnance de Louis XI du 21 oct. 1467.

ses finances lors de l'instauration de la vénalité des offices[35]. Aujourd'hui, les descendants de ces officiers et commissaires sont les notaires, huissiers de justice, avocats au Conseil d'État et à la Cour de cassation[36], nommés par arrêté du Garde des sceaux[37]. En revanche, les métiers d'experts-comptables, d'avocats et même de commissaires aux comptes[38], de commissaires-priseurs[39] ou encore de courtiers[40] se perpétuent, bien qu'ils ne disposent plus du statut d'offices. Leur qualité ou ancienne qualité d'officier leur confère une légitimité dans leur domaine. Dans la pratique, un registre est tenu par l'officier ou le tiers de confiance désigné par les parties. Celui-ci a pour mission de le maintenir à jour afin, d'une part, d'assurer les droits et obligations de chaque partie et, d'autre part, d'éviter tout risque de falsification frauduleuse[41]. Le juge a également le rôle d'un tiers de confiance car, en tant que magistrat du siège rendant la justice et veillant à l'application des lois institutionnelles, il participe au fonctionnement du service public de la justice[42]. De plus, lorsqu'il est saisi plus spécifiquement par les parties à un contrat en vue de son exécution, le juge a pour mission de veiller en toute impartialité à ce que les dispositions contractuelles soient correctement observées par chacune des parties[43]. À côté des entités étatiques, les tiers de confiance historiques recouvrent également les autorités spécialisées, notamment les banques et les compagnies d'assurance.

Avec l'avènement d'Internet, une nouvelle forme de confiance est apparue et entraîna une transformation profonde de l'institution des tiers de confiance[44]. Ces nouveaux tiers, portés par la notion d'économie collaborative, consistent en des « plateformes d'intermédiation », c'est-à-dire des plateformes en ligne mettant directement en relation les utilisateurs entre eux en vue d'échanger des biens ou des

---

[35] Évènement ayant profondément marqué l'Histoire du pouvoir monarchique, pour plus de précisions sur le sujet, v., Direction de l'information légale et administrative, « L'Histoire de la fonction publique », *Vie publique* [en ligne], 12 oct. 2012, http://www.vie-publique.fr/decouverte-institutions/institutions/approfondissements/histoire-fonction-publique.html.

[36] ORDONNEAU (Pascal), *Monnaies cryptées et blockchain : La confiance est-elle un algorithme ?*, éd. Arnaud Franel, 2017, p. 191.

[37] Direction de l'information légale et administrative, préc.

[38] ORDONNEAU (Pascal), *op. cit.*, p. 191.

[39] Ministère de la Justice et des Libertés, « Les officiers ministériels », [en ligne], juin 2010, Secrétariat général > Service de l'administration centrale > Département des archives, de la documentation et du patrimoine, http://www.archives-judiciaires.justice.gouv.fr/index.php?article=14875&rubrique=10774&ssrubrique=10827.

[40] Le métier de courtier est devenu un office par un Édit de Charles IX de juin 1572, puis commença à se libéraliser avec la loi du 18 juillet 1866 portant sur la liberté d'exercer la profession de courtier (L., 18 juill. 1866, sur les courtiers de marchandise, *in Recueil Duvergier*, p. 390). Désormais le courtage « en ligne » est régi par la L. n° 2000-642, 10 juillet 2000, portant réglementation des ventes volontaires de meubles aux enchères publiques, *JORF* n° 159, 11 juill. 2000, texte n° 2.

[41] BERBAIN (Côme), « La blockchain : concept, technologies, acteurs et usages », art. cit., *op. cit.*

[42] L. org. n° 2001-539, 25 juin 2001, relative au statut des magistrats et au Conseil supérieur de la magistrature, *JORF* n° 0146, 26 juin 2001, texte n° 1.

[43] LE BARS (Thierry), HÉRON (Jacques), *Droit judiciaire privé*, éd. LGDJ, coll. Domat privé, 7e édition, 2019, nos 280 et s.

[44] GUILHAUDIS (Élise), art. cit., p. 54.

services[45]. Il s'agit par exemple de faciliter les transactions entre utilisateurs en fournissant des références pertinentes lors de recherches d'informations (moteurs de recherche), de connecter les utilisateurs dans leur environnement (réseaux sociaux), ou même de les associer pour leur permettre d'utiliser les mêmes itinéraires (co-voiturage)[46]. L'économie collaborative de pair à pair, née de cette évolution, ne s'émancipe cependant pas de toute forme d'autorité. Les « netziens » font appel à un réseau hiérarchisé, non plus seulement fondé sur les institutions étatiques, mais désormais également basé sur les entreprises, qui, à terme, a réussi à édifier un comité fermé de sociétés multinationales à pratiques monopolistiques[47]. Il en va ainsi de Facebook, Apple, Amazon, Uber et Airbnb, ou encore Google. D'ailleurs, « googliser » tend à devenir un verbe à part entière, puisqu'il signifie « faire une recherche sur Internet »[48]. En effet, en l'espace de quelques années cette petite entreprise éphémère, installée dans une chambre étudiante de l'Université de Stanford par Serguey Brin et Larry Page[49], a fini par s'imposer au sein du « *Big Four* »[50]. Comptant plus de 60 000 employés originaires de pays différents et comptabilisant 182,527 milliards de dollars de chiffre d'affaires sur l'année écoulée[51], aujourd'hui Google est omniprésente en matière d'innovation[52]. Au centre d'un monde en interconnexion continue, elle est désormais capable de modeler les agissements de ses millions d'utilisateurs à travers ses nombreux produits usuels et leurs diverses « suggestions ». Par ailleurs, le cas de Google peut être rapproché de celui des plateformes ayant fait fortune dans le domaine. Elles ont, chacune à leur niveau, réussi l'exploit de déplacer la valeur marchande du produit ou service directement vers la fonction d'intermédiaire-tiers de confiance[53]. Dans l'état de l'art, ce rôle est bâti sur l'aptitude à valider les informations essentielles à leurs réseaux respectifs[54]. Toutefois, ces capacités se heurtent à l'insatisfaction croissante des consommateurs vis-à-vis des prestations de

[45] GRUMBACH (Stéphane), « Intermediation Platforms, an Economic Revolution », *ERCIM News* [online], 24 Sept. 2014, https://ercim-news.ercim.eu/en99/challenges-for-icst/intermediation-platforms-an-economic-révolution.
[46] *Id.*
[47] BARRAUD (Boris), « Les blockchains et le droit », *RLDI* 2018/4, nº 147, p. 8.
[48] Dictionnaire en ligne Larousse, v° Googliser [français] : « googliser (verbe transitif) – Rechercher des informations (en particulier sur quelqu'un) sur Internet en utilisant le moteur de recherche Google. (On dit aussi *googler*.) » – Oxford Dictionary, v° Google [english] : « *google, verb [with object] – Search for information about (someone or something) on the Internet using the search engine Google. Ex. 'on Sunday she googled an ex-boyfriend'; no object 'I googled for a cheap hotel/flight deal'.* »
[49] « Du garage au Googleplex », *Google* [en ligne], https://www.google.com/about/our-story/.
[50] Aussi appelés « GAFA », il s'agit de Google, Apple, Facebook, et Amazon, les quatre plus grandes multinationales spécialisées dans les communications et Internet.
[51] Chiffres pour l'année 2019, v., « Annual revenue of Alphabet from 2011 to 2020 », *Statista* [online], 8 Feb. 2021, Statistics > Internet > Search Engines & SEO, https://www.statista.com/statistics/507742/alphabet-annual-global-revenue/.
[52] « Du garage au Googleplex », préc.
[53] BARRAUD (Boris), « Les blockchains et le droit », art. cit., *loc. cit*.
[54] *Id.*

services rendues, notamment en matière de sécurité. Le 17 août 2018, l'intégrité de Google est mise en cause car son système de géolocalisation, même désactivé par le propriétaire du smartphone, est utilisé par des services de la société[55]. Il apparaît qu'à de nombreuses reprises Google a réussi, par le biais d'applications presque superflues telle la « lampe-torche », à accéder à la position de l'utilisateur à travers les données GPS générées par son smartphone[56]. Il s'agit d'un marché important pour la société puisqu'il est à l'origine notamment du commerce des publicités ciblées, dont les bénéfices économiques annuels sont estimés à plus de 100 milliards de dollars[57]. Les répercussions attachées au développement des plateformes d'intermédiation posent en filigrane la question du sort de la confiance et, *a fortiori*, de la précarité d'un système *centralisé*.

3. De la crise de confiance au remplacement par l'outil informatique. Depuis des années, la confiance dans la fiabilité d'un système ou d'une organisation découlait de la technique, de l'organisation et du droit, rassemblés dans une seule et unique entité. Lorsque le conservatisme, l'efficacité et la rapidité des tiers de confiance historiques, ainsi que l'insécurité des nouveaux intermédiaires de confiance du web, ont commencé à être vivement critiqués, certains ont évoqué un véritable « divorce entre les citoyens-consommateurs et les institutions »[58]. Une crise de confiance s'est enracinée au sein de la société moderne. L'aspect parfois trop centralisé de ces institutions étatiques et entités économiques est fréquemment mentionné. Cette centralisation du monde économique et financier fut d'ailleurs à l'origine de la crise des *subprimes*[59], provoquée par une succession de prises de risques durant l'automne 2008, commençant par la Fed – Réserve Fédérale des États-Unis – puis, gagnant les banques, et progressivement l'intégralité du marché financier. Les établissements bancaires aux États-Unis, notamment Freddie Mac, Fanny Mae, Deutsche Postbank et Lehman Brothers, se sont déclarés tour à tour en

[55] « États-Unis : Google poursuivi en justice pour le suivi abusif des données de géolocalisation », préc.
[56] AFP, « La géolocalisation, omniprésente à l'ère du smartphone », *Libération* [en ligne], 21 août 2018, http://www.liberation.fr/futurs/2018/08/21/la-geolocalisation-omnipresente-a-l-ere-du-smartphone_1673787 : « L'entreprise américaine n'a pas fait de commentaires. Depuis la publication de l'article la semaine dernière, Google a modifié sa page d'assistance. On y lit désormais que le fait de désactiver l'historique de localisation "n'affecte pas les autres services de localisation sur votre appareil". Les données peuvent également être récoltées lors de l'utilisation d'autres services tels que les cartes, selon la page d'assistance. La page indiquait auparavant que la désactivation de l'historique des lieux signifiait que les lieux visités n'étaient pas stockés par Google. »
[57] « Alphabet : La valeur du jour à Wall Street - GOOGLE affiche un nouveau record en Bourse », *Zone Bourse* [en ligne], 24 juill. 2018, https://www.zonebourse.com/ALPHABET-24203373/actualite/Alphabet-La-valeur-du-jour-a-Wall-Street-GOOGLE-affiche-un-nouveau-record-en-Bourse-26984596/.
[58] MANAS (Arnaud), BOSC-HADDAD (Yoram), « La (ou les) blockchain(s), une réponse technologique à la crise de confiance », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 102.
[59] DELHOMMAIS (Pierre-Antoine), « Alan Greenspan fait part de son "grand désarroi" », *Le Monde* [en ligne], 25 oct. 2018, https://www.lemonde.fr/la-crise-financiere/article/2008/10/25/alan-greenspan-fait-part-de-son-grand-desarroi_1111060_1101386.html.

difficultés ou en faillite[60]. Effet indirect d'une méfiance paralysant les relations interbancaires, la crise s'est propagée à travers le monde, transformant la crise financière en une crise économique. Or, l'impossibilité pour le système bancaire mondial, considéré comme tiers de confiance ancestral, à mettre en place une politique de gestion du risque capable d'endiguer la crise, a laissé s'installer une défiance généralisée, tant parmi les professionnels de la finance qu'auprès des clients. L'idée est alors apparue de remplacer ce tiers, désormais perçu comme étant indigne de confiance, par la neutralité présupposée de l'outil informatique. C'est ainsi qu'est né le projet d'une monnaie virtuelle, volontairement indépendante du système bancaire actuel et de la monnaie traditionnelle. L'intégrité financière passerait donc par une suite de 0 et de 1, logique binaire propre aux systèmes de traitement de l'information.

Cependant, cette image de vulnérabilité des systèmes centralisés n'a pas cessé d'exister après la création des monnaies cryptographiques (ou crypto-monnaies, notamment *bitcoin*). Cette méfiance s'est au contraire propagée au-delà du secteur économique et financier, impactant la majeure partie des tiers de confiance actuels, et *a fortiori* la crédibilité et la sûreté de leur activité. Il en va ainsi des notaires, des assureurs, des huissiers de justice, des avocats, des plateformes d'intermédiation, et même de l'État. L'affaire Edward Snowden de 2013[61] a d'ailleurs singulièrement étoffé cette crise[62]. L'enjeu a été d'ériger un écosystème entièrement sécurisé, infalsifiable et avant tout décentralisé. La volonté de bâtir une nouvelle démocratie ne tend pas à ériger une organisation politique mais davantage à réaffirmer les principes d'égalité et de liberté semblant faire défaut[63]. Le but devient alors de réinventer les rapports de confiance et ce, sans attache sociale, économique ni même juridique[64].

4. L'histoire de la cryptographie. Selon certains auteurs, « la longue route du progrès technique a toujours été pavée d'éléments symboliques de transition »[65]. Depuis l'Antiquité aussi bien grecque que romaine, et même antérieurement dans l'Égypte Ancienne (-1900 av. J.-C.) puis en Mésopotamie (-1600 av. J.-C.), le monde scientifique

[60] SAGNES (Nicolas), « Économie mondiale – 2008 : De la crise financière à la crise économique », *Encyclopaedia Universalis* [en ligne], 2008, https://www.universalis.fr/encyclopedie/economie-mondiale-2008-de-la-crise-financiere-a-la-crise-economique/.
[61] Pour plus d'informations sur le sujet, v., LEFEBURE (Antoine), *L'affaire Snowden : Comment les États-Unis espionnent le monde*, éd. La découverte, coll. Cahiers Libres, 2014.
[62] MANAS (Arnaud), BOSC-HADDAD (Yoram), art. cit., p. 103.
[63] DE TOCQUEVILLE (Alexis), *De la démocratie en Amérique*, éd. C. Gosselin, 1835 et 1840.
[64] *Ibid.*, p. 102.
[65] DOARÉ (Ronan), DANET (Didier), DE BOISBOISSEL (Gérard) (dir.), *Drones et killer robots : Faut-il les interdire ?*, éd. Presses universitaires de Rennes (PUR), coll. L'Univers des normes, 2015, p. 7.

explore cette science des messages cachés[66]. La cryptographie – ou cryptanalyse – est classiquement définie comme un moyen de communication entre deux personnes qui permet de garder secrète l'information échangée dans le cas où une tierce personne l'intercepterait[67]. De nombreuses études ont été menées sur la cryptographie entre 800 et 1400 au sein de l'Empire arabe[68]. Dans son *Manuscrit*, Al-Kindi, ou Abū Yūsuf Yaʿqūb ibn Isḥāq al-Kindī, a d'ailleurs été le premier à travailler sur la technique d'analyse fréquentielle des lettres, c'est-à-dire la fréquence d'utilisation des lettres, dans les textes chiffrés[69]. Par la suite, nombre d'inventeurs et de cryptanalystes s'en inspirèrent. François Viète, cryptanalyste du roi Henri IV, déjoua ainsi les plans de l'Espagne et de l'Italie en déchiffrant les lettres échangées entre les Cours et leurs armées grâce à une méthode fondée notamment sur l'analyse fréquentielle[70]. De même, furent basés sur cette

[66] ANTOINE (Charles), *Introduction à la physique quantique*, éd. Dunod, 2017, p. 107.
[67] *Id*.
[68] *Id*.
[69] Il s'agit du *Manuscrit sur le déchiffrement des messages codés*, qui fut d'ailleurs récemment retrouvé dans les archives ottomanes d'İstanbul en 1987. Pour plus de précisions, v., BOS (Gerritt), BURNETT (Charles), *Scientific weather forecasting in the middle ages: the writings of Al-Kindī: studies, editions, and translations*, ed. Kegan Paul, 2000. – LEHNING (Hervé), *L'univers des codes secrets : De l'Antiquité à Internet*, éd. Ixelles, 2012.
[70] Tel fut le cas d'une lettre chiffrée envoyée par le Commandeur Juan Moreo au Roi d'Espagne Philippe II le 28 octobre 1589, déchiffrée et publiée par François Viète le 28 mars 1590 [VIÈTE (François), *Deschiffrement d'une lettre escrite par le commandeur Moreo au roy d'Espagne, son maistre, du 28 octobre 1589*, Tours, Mettayer, 1590). – Dans son manuscrit, perdu mais retranscrit par Frédéric Ritter [RITTER (Frédéric), *Étude sur la vie du mathématicien François Viète (1540-1603), son temps et son œuvre, par Frédéric Ritter, polytechnicien et ingénieur des Ponts et Chaussées*, t. I, disponible sous forme de microfilms (87Mi/1) aux Archives nationales (106 AP)], François Viète explique qu' « [i]l faut remarquer toutes les sortes de figures, soit chiffre ou jargon, et nombrer combien elles sont de fois, puis remarquer toutes les sortes de figures qui précèdent ou qui suivent, et conférer les plus fréquentes afin de découvrir les mêmes mots et les mêmes valeurs et n'y épargner ni le labeur ni le papier... et enfin par hypothèses on pourra parvenir à la résolution ». – Pour plus de précisions, v., DELAHAYE (Jean-Paul), « Viète, inventeur de la cryptanalyse mathématique », *Pour la Science*, n° 313, nov. 2003, pp. 90-95 ; PANZA (Marco), « François Viète, between analysis and cryptanalysis », *Studies in History and Philosophy of Sciences*, Vol. 37, Issue 2, Jun. 2006, pp. 269-289.

technique le cadran d'Alberti à la fin du XV^e siècle [71], ou encore le cylindre de Thomas Jefferson en 1793[72].

Mais c'est réellement avec la « Bombe cryptologique », qui est une machine de déchiffrement créée durant la Seconde Guerre Mondiale dans le but de décoder les nombreux télégrammes cryptés envoyés par l'armée allemande à ses troupes[73], que la cryptographie moderne est apparue. Depuis la Première Guerre Mondiale déjà, des équipes polyglottes de cryptanalyses avaient été constituées. Leur efficacité avait été reconnue à de nombreuses reprises, notamment lors de l'affaire du « télégramme Zimmermann » qui proposait secrètement une alliance entre le gouvernement allemand

[71] Il s'agit d'un cadran composé de deux disques concentriques. Le premier disque, prenant place sur le bord extérieur du cadran, est fixe et contient en principe vingt-quatre symboles en lettres capitales, soit vingt provenant de l'alphabet latin et placés dans le bon ordre (J, U, et W ne figurent que sur le second disque, et H, K, et Y figurent ni sur l'un ni sur l'autre car Alberti ne les a pas jugés indispensables à l'émission d'un message) et les quatre chiffres 1, 2, 3, 4, permettant un second chiffrement prédéfini par l'expéditeur et le destinataire. Ce disque correspond au message à coder. Le second disque, prenant place sur le bord intérieur du cadran, est pour sa part mobile, et contient le même nombre de symboles que le premier disque, cette fois en lettres minuscules et en principe dans un ordre quelconque. Y figurent vingt-trois lettres de l'alphabet latin, c'est-à-dire les lettres du premier disque auxquelles les lettres j, u et w se sont adjointes, ainsi que le symbole &. Ce disque correspond au message codé. Les expéditeur et destinataire ont chacun en leur possession la copie conforme du cadran de l'autre, condition *sine qua non* du déchiffrement des messages codés transmis. Pour chiffrer un message, il faut commencer par aligner le A du disque extérieur au a du disque intérieur, puis lire le symbole figurant en minuscule sur le disque intérieur pour chaque symbole en majuscule du message à coder sur le disque extérieur. Alberti conseillait d'ailleurs de modifier périodiquement la correspondance entre les disques, par exemple toutes les quatre lettres, de tourner le disque intérieur d'un cran vers le symbole suivant afin de rendre le déchiffrement plus complexe et plus sûr. Le site *dCode* permet de chiffrer/déchiffrer avec l'alphabet Alberti [v., https://www.dcode.fr/chiffre-alberti] : « Exemple : Les alphabets ABCDEFGHIJKLMNOPQRSTUVWXYZ pour [l'extérieur] et abcdefghijklmnopqrstuvwxyz pour [l'intérieur], A est alignée avec a, B est alignée avec b, etc. Tourner le disque de 2 crans, et alors A est alignée avec c, le décalage initial est de 2. […] Par défaut, tous les 4 caractères (4 = période), le disque intérieur est tourné dans le sens des aiguilles d'une montre de 1 secteur (1 = incrément), ce qui a pour effet de modifier l'alphabet de substitution. […] Chiffrer DCODE avec les alphabets avec un décalage initial de 1, une période de 3 et un incrément de 2. Les alphabets sont donc décalés initialement de 1 ainsi : ABCDEFGHIJKLMNOPQRSTUVWXYZ et bcdefghijklmnopqrstuvwxyza. La période commence, chiffrer D par e, C par d, O par p, la période (de longueur 3) se termine, tourner la roue de 2 lettres. Les alphabets sont décalés ainsi : ABCDEFGHIJKLMNOPQRSTUVWXYZ et defghijklmnopqrstuvwxyzabc, la nouvelle période commence, etc. Le message chiffré est donc edpgh. »

[72] Il s'agit d'un cylindre découpé en vingt-six disques indépendants les uns des autres, représentant les vingt-six lettres de l'alphabet latin. Des lignes sont tracées tout le long des disques, sur la longueur du cylindre, de sorte que chaque disque est divisé en un nombre égal de parties. Sur chaque ligne, l'alphabet y a été inscrit dans le désordre. Ainsi, pour chiffrer, l'expéditeur inscrit son message sur une ligne (par exemple : « JEFFERSON »), puis recopie les lettres figurant sur une autre ligne (par exemple : HIDLJEAMN ») pour les faire parvenir au destinataire. Cette méthode exige que le destinataire dispose d'un cylindre parfaitement identique à celui de l'expéditeur puisque pour déchiffrer le message, il devra inscrire sur son propre cylindre la suite de lettres reçue, puis rechercher sur une autre ligne du cylindre le message en clair. Le site *dCode* permet également de chiffrer/déchiffrer selon la « méthode Jefferson » [v., https://www.dcode.fr/cylindre-jefferson]. – LENHING (Hervé), « Jefferson et les mathématiques », *in* COHEN (Gilles) (dir.), *Mathématiques et politique*, Éditions Pôle Paris, coll. Bibliothèque Tangente, n° 45, 2012, p. 117 : « La clé est l'ordre dans lequel les roues ont été disposées. Il y a donc 26 clés possibles, soit plus de 4x1026. »

[73] LEHNING (Hervé), « Quels étaient les codes secrets de la première guerre mondiale ? », *Futura Sciences* [en ligne], 2017, https://www.futura-sciences.com/sciences/questions-reponses/mathematiques-etaient-codes-secrets-premiere-guerre-mondiale-8067/.

et le gouvernement mexicain contre les États-Unis d'Amérique[74]. Mais, la technologie sans cesse plus innovante a permis la création de la machine de chiffrement/déchiffrement allemande *Enigma*[75]. Les alliés ont eu besoin de plus de rapidité dans les analyses afin de pouvoir contrecarrer la vitesse de transmission des nouvelles technologies[76]. Dans les années 1930, les services secrets polonais et français ont tenté d'unir leurs forces pour casser le code d'encryptage d'*Enigma*, mais cette alliance s'est soldée par un échec. Lors de la Seconde Guerre Mondiale, les alliés ont fondé la *Government Code and Cypher School* (GC&CS) (École Gouvernementale Britannique du Chiffre et du Code), une organisation secrète basée à Bletchley Park dans le Buckinghamshire sous le nom de code « *Golf, Cheese and Chess Society* »[77] (« Club de Golf de Fromage et d'Échecs »). C'est au cours de l'année 1941 qu'Alan Mathison Turing, mathématicien et cryptologue britannique, parvint, avec l'aide de Gordon Welchman et de Richard Pendered[78], à briser le mécanisme de codage allemand d'une machine *Enigma* dérobée plus tôt. Elle fut à l'origine de la construction d'une bombe cryptologique, tout premier outil de cryptanalyse de l'histoire qui devint une des clés principales de la victoire[79]. Nommée « Bombe de Turing, Welchman et Pendered », cette machine permit de tester automatiquement, une par une, toutes les solutions possibles d'un message codé, ne laissant aux cryptanalystes que l'examen des résultats obtenus.

[74] Demande envoyée le 16 janvier 1917. – Pour plus de détails sur l'affaire, v., LEHNING (Hervé), « Cryptologie et espionnage : comment a-t-on décrypté le télégramme Zimmermann ? », *Futura Sciences* [en ligne], 2017, https://www.futura-sciences.com/sciences/questions-reponses/mathematiques-cryptologie-espionnage-t-on-decrypte-telegramme-zimmermann-8082/.

[75] *Enigma* a été inventée par l'ingénieur néerlandais Hugo Alexander Koch en 1919. C'est une machine à chiffrage électromécanique qui a été utilisée par les allemands durant la Seconde Guerre Mondiale.

[76] RODRIGUEZ (Philippe), *La révolution blockchain : Algorithmes ou institutions, à qui donnerez-vous votre confiance ?*, éd. Dunod, 2017, p. 37.

[77] LEE (John A. N.), *International Biographical Dictionary of Computer Pioneers*, ed. Taylor & Francis, 1995, p. 331.

[78] Richard Pendered avait alors 18 ans.

[79] Après cette découverte, Alan M. Turing a décidé de poursuivre ses recherches sur la cryptographie à Teddington au Royaume-Uni en tant que directeur du Laboratoire national de physique. Après quelques années d'absence, il a obtenu la direction d'un projet visant à mettre au point le tout premier ordinateur mondial, Mark I. Mais il en a été par la suite écarté à cause de la gêne qu'a occasionnée son homosexualité dans le Royaume-Uni des années 1950. – Pour plus de précisions, v., RODRIGUEZ (Philippe), *op. cit.*, pp. 40 et s.

De Blaise Pascal[80], Alexander Graham Bell[81], Joseph-Marie Jacquard[82], Charles Babagge[83], Howard Aiken[84], ou, plus tard, John Von Neumann[85], John Backus[86], ou encore Steve Jobs et Stephen Wozniak[87], la cryptanalyse est aussi intimement liée avec le développement d'un système de traitement, devenu informatisé avec l'apparition de l'ordinateur[88].

Un second « élément symbolique de transition » prend naissance avec le « projet GIMPS » (« *Great Internet Mersenne Prime Search* ») de 1996[89]. Il s'agissait d'utiliser la nouvelle technologie de l'époque, Internet, pour créer un réseau distribué d'ordinateurs à travers le monde pouvant, avec cette capacité de traitement optimisée, faire avancer la recherche en mathématiques[90]. En mettant ainsi à contribution un nombre important de

[80] Inventeur notamment de la calculatrice mécanique.
[81] Développeur du concept du téléphone.
[82] Qui a mis au point le métier à tisser automatisé appelé « métier Jacquard », l'ancêtre mécanique des ordinateurs.
[83] De 1834 à 1837, Charles Babagge a conçu une machine à calculer programmable en associant les inventions de Blaise Pascal et de Joseph-Marie Jacquard qu'il a appelé la « Pascaline ». À l'époque, cette technologie utilisait des instructions écrites sur des cartes perforées avec un lecteur de cartes pour les données et un autre pour les programmes. Ces lecteurs étaient reliés à des systèmes de mémoires, un calculateur central et une imprimante.
[84] Howard Aiken, mathématicien américain, a repris le concept de la Machine analytique de Charles Babagge. Son projet a très vite intéressé la société IBM de Thomas Watson Sr. qui a financé sa construction. Achevé en 1939 et testée en 1943 dans les locaux d'IBM, « Harvard Mark I », le tout premier ordinateur numérique était né. Sa mise sur le marché a été immédiate.
[85] Composé d'un organe de calcul, d'une mémoire d'organes d'entrée-sortie (périphériques) et d'une unité de commande, l'ancêtre des ordinateurs d'aujourd'hui a fait son apparition avec l'ordinateur de Neumann. Cet ordinateur était composé d' « *hardware* » que sont les éléments physiques et matériels de l'ordinateur (boîtier, processeur et disque-dur notamment), répondant aux instructions des « *software* » que sont les programmes des logiciels. En 1956, IBM a créé et commercialisé le premier disque dur, le « RAMAC 305 ». Ce disque dur était composé de 50 disques de 60 cm de diamètre empilés les uns sur les autres et avait une capacité de 5 méga-octets, ou « Mo », soit 100 000 fois moins que les actuels disques-durs de 500 « Go » (Si 1 Go = 1 024 Mo, alors 5 Mo = 0,005 Go, arrondi à la décimale supérieure).
[86] En 1957, il créé chez IBM le tout premier langage de programmation universel appelé le « *FORmula TRANslator* » (« *FORTRAN* »).
[87] En 1975 ils développent le prototype « Apple I » et fondent la société Apple en avril 1976. Les premiers Apple sont produits en Californie, au sein de la future Silicon Valley. L' « Apple II » d'Apple, le premier ordinateur personnel produit à grande échelle est considéré comme « la fine fleur des ordinateurs personnels à cette époque » (v., LECOMPTE SALMANDJEE (Yasmina) et LECOMPTE (Sébastien), *La culture high-tech pour les nuls*, Éditions First, coll. Pour les nuls, 2015, p. 79). Le 24 janvier 1984, l' « Apple Macintosh » est présenté au public par Steve Jobs. Cette machine est dotée d'une interface graphique, tourne à 8 MHz (méga-hertz), possède 128 kilo-octets de RAM, une souris, un écran noir et blanc et un lecteur de disquette 3 pouces ½. Son prix de 2 500 $ (soit 25 000 F), estimée peu onéreux pour l'époque, lui permet de remporter un très grand succès. Finalement, en octobre 1984, 1024 machines sont connectées sur Internet.
[88] Pour plus de précisions, v., ROCHAIN (Serge), *De la mécanographie à l'informatique : 50 ans d'évolution : Histoire des sciences et des techniques : Software, environnements and tools*, éd. ISTE, 2016. – LEFEVRE (Thierry), « Une très brève histoire de la technologie humaine », *Planète viable* [en ligne], 17 avr. 2017, http://planeteviable.org/histoire-technologie-humaine/.
[89] DOARÉ (Ronan), DANET (Didier), DE BOISBOISSEL (Gérard) (dir.), *op. cit.*, p. 7.
[90] Il s'agissait de résoudre le problème du nombre premier de Mersenne – plus exactement de Marin Mersenne, mathématicien du XVII^e siècle – venant compléter une suite appelée suite de Lucas [Pour plus de précisions techniques, v., LUCAS (Édouard), *Théorie des fonctions numériques simplement périodiques*, éd. Amer. J. Math., vol. 1, n° 2, 1878, pp. 184-196, 197-240, et 289-321]. Selon la règle posée, pour résoudre ce problème d'arithmétique il faut réussir à répondre à deux conditions cumulatives : que le résultat de l'équation de Mersenne *2n-1* soit par ailleurs un nombre premier, c'est-à-dire un nombre qui est divisible par 1 et par lui-même. Par exemple, le nombre de Mersenne M_4 n'est pas premier : 24 - 1 = 15 = 3 × 5.

calculateurs, le projet a réussi à quintupler les résultats[91]. Trois projets d'informatique distribuée ont suivi, mais n'ont cependant pas eu le même retentissement : *SETI@home* (« *Search for Extra-Terrestrial Intelligence* »), *Einstein@home* pour les ondes gravitationnelles, et enfin *MilkyWay@home* pour la création de structures tridimensionnelles représentant la dynamique stellaire[92].

L'association de ces recherches cryptographiques et de ces projets distribués plus ou moins étendus ont édifié ce qui allait devenir la pierre angulaire de la technologie *blockchain*, c'est-à-dire le principe d'une technologie massivement distribuée, au service de la sécurité des informations transmises. Par la suite, c'est grâce à un héritage pluridisciplinaire et à visée collective que la science a contribué à la réinvention des rapports de confiance entre les Hommes.

5. L'histoire du *bitcoin*. La naissance de la monnaie virtuelle et décentralisée découle de la volonté originelle de réaliser des transferts d'argent entre deux internautes sans qu'aucune autorité ou institution financière ne soit nécessaire en tant que tiers de confiance. Le concept du *bitcoin* apparaît à la suite d'un article de l'ingénieur Wei Dai sur la « *b-money* », constituant la première ébauche d'une crypto-monnaie[93]. Selon lui, deux fondamentaux doivent être réunis pour créer une monnaie électronique sûre et stable. Elle exige, d'une part, une base de données *fiable* enregistrant les biens en argent de chaque utilisateur et, d'autre part, sa *distribution* sur l'ensemble du réseau[94]. Il s'agit en définitive de trouver un protocole permettant de dépasser les problèmes techniques qui entravaient jusqu'alors les systèmes de stockage d'argent en ligne[95]. Après la publication de son article, Wei Dai suscite les vocations et, tandis que le système financier subit un krach bancaire, beaucoup sont ceux qui désirent mettre en œuvre cette crypto-monnaie[96]. Parmi ses émules, Nick Szabo, professeur de droit à l'Université George Washington aux États-Unis et membre du mouvement crypto-anarchiste des *Cypherpunks*, partisans d'une révolution numérique[97], est l'un des premiers à publier ses recherches en 1998, peu de

---

[91] En effet, alors qu'à peine dix nombres de Mersenne avaient jusqu'ici été trouvés, l'ensemble des calculateurs réunis ont réussi à en comptabiliser 50, dont le dernier trouvé – soit le plus grand nombre de Mersenne actuellement connu – étant $M_{77\,232\,917.}$ – Pour plus de précisions, v., Mersenne Research Inc., « GIMPS Project Discovers Largest Known Prime Number: 277 232 917-1 », *GIMPS* [online], 3 Jan. 2018, https://www.mersenne.org/primes/?press=M77232917.

[92] RODRIGUEZ (Philippe), *op. cit.*, pp. 41-42.

[93] DAI (Wei), « b-money, an anonymous, distributed electronic cash system », [online], 1998, http://www.weidai.com/bmoney.txt.

[94] *Id.*

[95] RODRIGUEZ (Philippe), *op. cit.*, p. 44.

[96] *Supra* n° 3.

[97] Ce mouvement, qui a pris naissance dans les années 1980, réunit une communauté d'utilisateurs du web s'érigeant contre ce qu'ils perçoivent comme l'autoritarisme ou le totalitarisme de certains gouvernements, et demande la protection de la vie privée sur Internet et le web. Selon les auteurs, « [c]ontrairement aux

temps après la création de la plateforme de monnaie électronique centralisée *Digi Cash Inc* par David Chaum[98]. Après sept années de recherches sur un projet conjuguant des techniques de hachage, d'horodatage et de chiffrement par clés publiques/privées, Nick Szabo crée le protocole *BitGold* de la crypto-monnaie éponyme. Il décide alors de publier en ligne un rapport destiné à poursuivre *BitGold* sur la toile. Cependant, souffrant de sa faible sécurité, il est abandonné avant même d'être lancé.

Pour autant, ses travaux sur les *smart contracts* permirent de faire émerger le concept de la chaîne de blocs[99]. En octobre 2008, un internaute, ou plusieurs, utilisant le pseudonyme « Satoshi Nakamoto »[100], publie(nt) l'article « *Bitcoin: A Peer-to-Peer Electronic Cash System* »[101]. Cet article, dont l'auteur (les auteurs) se dissimule(nt) derrière un nom japonais, une adresse courriel allemande et un bon niveau d'anglais écrit[102], pose pour la première fois les fondements de cette technologie que Satoshi Nakamoto nomme la « *Block Chain* »[103], expression qui vient remplacer celle de « *timestamp server* »[104]. En janvier 2009 est mis à disposition son logiciel « *Bitcoin-QT* »

---

sociétés traditionnellement associées au mot "anarchie", une crypto-anarchie ne détruit pas temporairement un gouvernement, mais elle l'interdit et le rend inutile de façon définitive. » (« *Unlike the communities traditionally associated with the word "anarchy", in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary*. » [notre trad.], DAI (Wei), « b-money, an anonymous, distributed electronic cash system », art. cit.), les membres d'un écosystème *blockchain* « […] partagent un intérêt particulier pour la préservation de la vie privée et de l'anonymat, contre des gouvernements et firmes qui abusent de leur emprise sur l'information et les canaux de sa circulation. Ils veulent concevoir des protocoles informatiques dont l'architecture même, par ses incitations structurelles, permettent la coopération interindividuelle, hors identification *intuitu personæ*, dans une communauté plus démocratique, puisque constituée en réseaux décentralisés. Auto-déclarés "*libertarian*" [MAY (Timothy C.), « The Crypto Anarchist Manifesto », *Activism.net* [online], 22 Nov. 1992, https://www.activism.net/cypherpunk/crypto-anarchy.html], ils affichent une défiance envers toutes institutions centrales qui, par nature, ont un pouvoir exorbitant. Les technologies qu'ils forgent sont les moyens qui rendront impotents toutes entités à prétention orwellienne. Ils visent explicitement les États dont la gouvernementalité serait rendue inopérante et illégitime. » (ROLLAND (Maël), « Les crypto-monnaies à l'aune des monnaies parallèles, sociales et complémentaires : continuité et rupture dans le champ de la gouvernance monétaire », *in* MARTÍ (José) (dir.), *Conferencia Internacional Por El Equilibrio Del Mundo*, Cuba, 10-14 Mayo 2017, inedito [en línea], https://www.swisscurrencyconfederation.ch/wp-content/uploads/2018/04/Rolland-M.-Les-crypto-monnaies-%C3%A0-laune-des-monnaies-sociales-et-compl%C3%A9mentaires-continuit%C3%A9-et-rupture-dans-le-champs-de-la-r%C3%A9appropriation-mon%C3%A9taire.pdf). – V. également, RODRIGUEZ (Philippe), *op. cit.*, pp. 54-65.

[98] Cette plateforme permettait d'effectuer des transactions monétaires sur Internet, de manière anonyme et ce, grâce à un mécanisme d'encryptement avancé. Elle s'est maintenue huit années consécutives malgré un développement timide du *e-commerce* chez les consommateurs-utilisateurs d'Internet, ce qui, par la suite, causa sa fermeture définitive. V., RODRIGUEZ (Philippe), *op. cit.*, p. 42.

[99] KELLY (Brian), *The Bitcoin Big Bang: How Alternative Currencies are about to Change the World*, ed. John Wiley & Sons, 2014, p. 153.

[100] FAVIER (Jacques), TAKKAL BATAILLE (Adli), *Bitcoin. La monnaie acéphale*, éd. CNRS, coll. Économie Droit, 2017, p. 272.

[101] NAKAMOTO (Satoshi), « Bitcoin: A Peer-to-Peer Electronic Cash System », [online], Oct. 2008, https://bitcoin.org/bitcoin.pdf.

[102] FRISBY (Dominic), *Bitcoin: The Future of Money?*, ed. Random House, 2014, p. 7.

[103] RODRIGUEZ (Philippe), *op. cit.*, p. 46.

[104] BEAUDEMOULIN (Nathalie) *et al.*, « Les enjeux de la Blockchain pour la Banque de France et l'Autorité de Contrôle prudentiel et de Résolution (ACPR) », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 29.

et sont créées les toutes premières unités de monnaie numérique *bitcoin* qui valent alors 0,001 USD (pour 1 BTC)[105]. Le 3 janvier 2009, le « *block genesis* », tout premier bloc de la chaîne *Bitcoin*[106], est inscrit *via* une transaction de 50 BTC entre Satoshi Nakamoto et le cryptologue Hal Finney, spécialiste de la preuve de travail (*Proof of Work* (PoW)) dont se sert *Bitcoin*[107]. Le protocole de Satoshi Nakamoto a finalement réussi à mettre en œuvre la monnaie électronique sûre et stable conçue par Wei Dai. À la différence des précédentes tentatives de protocoles, *Bitcoin* se concrétise grâce à la combinaison de plusieurs avancées technologiques[108], à savoir la *b-money*, les clés cryptographiques, le système de PoW *via Hashcash* d'Adam Black, mais aussi l'idée du protocole décentralisé du projet GIMPS[109]. Cet ensemble de « couches technologiques » permet à un développeur de Jacksonville en Floride d'acheter le 21 mai 2010 deux pizzas de la marque Papa John's (ou Domino's) à un autre utilisateur de la plateforme pour 10 000 BTC[110], soit l'équivalent huit ans plus tard de plus de 279 millions de dollars au cours actuel du *bitcoin*[111]. Par la suite, le réseau *Bitcoin-QT* connaît une première faille qui permet à deux utilisateurs de subtiliser temporairement au protocole plusieurs centaines de millions d'unités BTC[112]. Même si, à l'image d'un retour au *statu quo ante*, la brèche de sécurité est rapidement colmatée et la transaction déloyale totalement effacée, et qu'aucune autre faille d'une telle ampleur n'a plus affecté la *blockchain Bitcoin*, les opposants aux crypto-monnaies restent marqués par cet épisode[113].

6. Fonctionnement du protocole *Bitcoin*. *Bitcoin* est un protocole informatique permettant des transactions spécifiquement financières en *Peer-to-Peer* (P2P), soit de pair à pair, *via* Internet. Elles se réalisent sans intervention tierce et encore moins centrale puisqu'il s'agit d'un système entièrement décentralisé, c'est-à-dire que nul n'exerce un

[105] USD est l'abréviation officielle du dollar américain, la devise des États-Unis.
[106] *Bitcoin* avec une majuscule se réfère au protocole informatique décrivant le réseau, tandis que *bitcoin* avec une minuscule se réfère à la monnaie cryptographique.
[107] GEIBEN (Didier), JEAN-MARIE (Olivier), VERBIEST (Thibault) *et al.*, *Bitcoin et Blockchain : Vers un nouveau paradigme de la confiance numérique ?*, éd. RB, coll. Les essentiels de la banque et de la finance, 2016, p. 21.
[108] ANTONOPOULOS (Andreas M.), *Mastering Bitcoin*, ed. O'Reilly, 2nd edition, 2017, p. 10.
[109] RODRIGUEZ (Philippe), *op. cit.*, p. 43.
[110] « Les deux pizzas les plus chères du monde », *Bitcoin Monde* [en ligne], 24 mai 2017, http://bitcoinmonde.com/index.php/2017/05/24/les-deux-pizzas-les-plus-chers-du-monde/.
[111] Il s'agit de 278,527,700 USD (1 BTC = 27,852.77 USD), selon le site de change XE.com [v. : https://www.xe.com/currencyconverter/convert/?Amount=1&From=XBT&To=USD] à la date du 1er févr. 2021. – C'est d'ailleurs ce qui a valu à ces pizzas de développer une notoriété internationale en tant que « pizzas les plus chères du monde ». V., « La pizza la plus chère du monde », *Bitcoin.fr* [en ligne], 22 mai 2011, https://bitcoin.fr/la-pizza-la-plus-chere-du-monde/.
[112] RODRIGUEZ (Philippe), *op. cit.*, p. 45.
[113] *Ibid.*, p. 46.

quelconque contrôle sur le réseau[114]. En règle générale, chaque ordinateur du réseau, appelé « nœud » (*node*), télécharge une copie du registre de transactions *Bitcoin* dès son adhésion à la chaîne et œuvre à la tenir à jour[115]. Finalement, les nœuds contrôlent le réseau, sans toutefois le contrôler individuellement. Ainsi réunis, les membres volontaires de la communauté jouent, ensemble, ce rôle instigateur de confiance. Ce principe de distributivité trouve sa source dans les fondements du mécanisme du *Bitcoin*, à savoir l'appréhension de la double dépense (*double-spending problem*), c'est-à-dire qu'un utilisateur puisse dépenser *x* unités BTC en les transférant à l'adresse d'un autre utilisateur, sans que ces *x* unités BTC ne soient débités de son portefeuille, ce qui lui permettrait de dépenser à nouveau ces unités. Les systèmes de crypto-monnaies qui ont précédé *Bitcoin* étaient caractérisés par ce type de fonctionnement, ce qui les empêchait d'aboutir à des systèmes de stockage d'argent en ligne fiables et sécurisés. En effet, selon Boris Barraud, « lorsqu'on envoie une chose sous forme de données en utilisant un réseau pair-à-pair classique ou le web, cette chose n'est qu'une copie et l'envoyeur conserve l'original ; il y a toujours accès. Il lui est donc possible de transférer librement autant de copies que souhaité. Le bien est non rival, sa possession n'est pas exclusive : [...] Internet, sans *blockchains*, est par conséquent inutile pour transférer des choses qui ont de la valeur comme des titres ou des actions. Il permet seulement des partages »[116]. Or, de manière tout à fait inédite, « le protocole *Bitcoin* a réussi à créer un bien numérique non reproductible »[117]. Sur une *blockchain*, lorsque la transaction est scellée entre deux personnes, celle-ci est envoyée sur le réseau pour « validation » par les membres de l'écosystème. À raison de 50 BTC de récompense (*block reward*) toutes les dix minutes au lancement de *Bitcoin* en 2009 et durant les quatre premières années, puis divisé par deux tous les quatre ans[118], les mineurs, qui sont les participants volontaires au réseau et

---

[114] GEIBEN (Didier), JEAN-MARIE (Olivier), VERBIEST (Thibault) *et al*., *Bitcoin et Blockchain : Vers un nouveau paradigme de la confiance numérique ?*, *op. cit.*, p. 26.

[115] MARIN-DAGANNAUD (Gautier), « Comprendre la blockchain Ethereum – Article 1 : Bitcoin, première implémentation de la blockchain (1/2) », *Ethereum France* [en ligne], 3 juin 2016, https://www.ethereum-france.com/comprendre-la-blockchain-ethereum-article-1-bitcoin-première-implementation-de-la-blockchain-12/.

[116] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 6.

[117] FAVIER (Jacques), TAKKAL BATAILLE (Adli), *op. cit.*, pp. 1 et s. – D'ailleurs, selon Guillaume Helleu et Anthony Masure [v., HELLEU (Guillaume), MASURE (Anthony), « Total Record. Les protocoles blockchain face au post-capitalisme », *Multitudes* 2018/2, n° 71, pp. 73-74] : « Ce mécanisme rend par conséquent impossible, contrairement à l'économie de la dette, l'obtention de soldes négatifs. »

[118] Le protocole *Bitcoin* est programmé pour cesser l'émission de *bitcoins* lorsque celle-ci aura atteint un total de 21 millions de *bitcoins* émis. L'émission est donc programmée pour cesser en 2140. Chaque *bitcoin* est divisible à la puissance 8, autrement dit, la plus petite valeur est le *satoshi*, cent millions de fois plus petit que le *bitcoin*. Dans l'ordre croissant, il s'agit du *bitcoin* (1 BTC), puis du deci-*bitcoin* (0,1 BTC), du *bitcent* (ou centi-*bitcoin*, 0,01 BTC), du *millibit* (ou milli-*bitcoin*, 0,001 BTC), du *bit* (ou micro-*bitcoin*, 0,000001 BTC), du *finney* (0,0000001 BTC), du *satoshi* (0.00000001 BTC), et enfin du milli-*satoshi* (0.000000001 BTC).

propriétaires de la puissance de calcul, vérifient puis intègrent de manière définitive la transaction à la chaîne *Bitcoin* en résolvant un problème informatique[119]. De cette façon, aucune transaction de *bitcoins* ne peut, en principe, être modifiée, ajoutée, ou supprimée de la *blockchain* puisqu'une telle manipulation serait automatiquement annulée par les pairs membres du réseau.

Par ailleurs, contrairement aux monnaies traditionnelles, les *bitcoins* sont totalement virtuels, il n'existe donc pas de pièce de monnaie – physique ou numérique – représentant un *bitcoin*. En réalité, les *bitcoins* et l'adresse de leurs propriétaires sont imbriqués dans les chaînes de transaction, ce qui permet de parfaire les échanges de valeurs entre utilisateurs. Le registre ne liste pas seulement les transactions de *bitcoins* : il est l'incarnation de l'ensemble des *bitcoins* inscrits sur la chaîne. Un *bitcoin* n'existe donc que sous la forme de son inscription dans la *blockchain*[120].

De cette façon, les utilisateurs peuvent transférer des *bitcoins* sur le réseau et les utiliser de la même manière que des pièces de monnaie ou des fonds déposés sur un compte bancaire pour acheter ou vendre des biens et services, envoyer de l'argent, demander un crédit ou un change, … L'objectif désormais est d'instituer le *bitcoin* dans la vie de tous les jours en permettant de l'échanger contre une monnaie légale ou encore de payer un commerçant[121]. La technologie *Bitcoin* a su mettre en œuvre des fonctionnalités reposant sur le cryptage et les signatures numériques afin d'assurer la sûreté du réseau, faisant du *bitcoin* une monnaie en théorie idéale pour les transactions numériques *via* Internet. Par exemple, *A* décide d'envoyer à une autre personne *B* une valeur de *x* BTC. *A* fait appel à son « *wallet* », qui est un portefeuille numérique pour *bitcoins*[122], et utilise le service « donner des bitcoins » de celui-ci. De cette façon, le *wallet* sollicite de *A* quelques informations telles que le montant de la transaction, le mot de passe de *A* acceptant ladite transaction qui, en réalité, déverrouille la « clé privée » contenue dans le *wallet* et permet de débloquer les fonds, et enfin l'identifiant du *wallet* de *B*, qui correspond à un dérivé de la « clé publique » de son *wallet* et permet de réceptionner les fonds. Pour parvenir jusqu'au *wallet* de *B*, il faut que ce dernier accepte la transaction *via* la saisie de son mot de passe, qui déverrouille de la même manière sa propre clé privée associée au dérivé de la clé publique de réception, dans le service « recevoir des bitcoins » de son propre *wallet*[123]. Ceci effectué, la transaction est

[119] GEIBEN (Didier), JEAN-MARIE (Olivier), VERBIEST (Thibault) *et al.*, *Bitcoin et Blockchain : Vers un nouveau paradigme de la confiance numérique ?*, *op. cit.*, pp. 25-27. – *Infra* n° 96.
[120] V., Annexe n° 1. Extrait d'une transaction sur *Bitcoin*, p. 433.
[121] À titre d'exemple, *Paymium* le rend possible.
[122] Il s'agit d'une interface informatique rendant le fonctionnement de *Bitcoin* accessible *via* des menus simplifiés et compréhensibles du plus novice.
[123] V., Annexe n° 2. Schéma simplifié du mécanisme de transaction sur *blockchain*, p. 434.

mélangée à d'autres transactions pour former un bloc, lequel est envoyé sur le réseau pour vérification, validation, et inscription définitive sur la *blockchain* du *Bitcoin*[124]. Il faut en moyenne dix minutes pour que les transactions contenues dans un bloc soient intégrées sur *Bitcoin*[125]. En réalité, ce qui fait l'objet d'une vérification est notamment le fait que *A* dispose véritablement de la somme qu'il veut transférer à *B*. L'intérêt du protocole est de pouvoir alors remonter l'intégralité de la chaîne de transactions jusqu'au bloc *genesis*, le tout premier de la chaîne, et effectuer ce contrôle.

Les utilisateurs de *Bitcoin* accèdent à l'écosystème et – s'ils le veulent – au minage (*mining*) *via* les utilitaires *bitcoin* et *bitcoind* téléchargeables[126] sous la forme de logiciels *open source*[127], dont le plus connu est le « client Satoshi »[128]. Il est possible de le télécharger sur une large gamme d'ordinateurs, y compris les ordinateurs portables ou les smartphones, ce qui *de facto* rend la technologie accessible[129]. Les mineurs peuvent décider d'être des « nœuds complets » ou « clients lourds » en choisissant de gérer entièrement l'installation de la pile du protocole *Bitcoin* et *a fortiori* en téléchargeant l'intégralité de la chaîne[130]. Ils peuvent également choisir d'être « clients légers » en ne téléchargeant que les entêtes des blocs de la chaîne (*header*)[131], mais en payant des frais de transaction (*transaction fees*), ou alors être « clients web » et utiliser un serveur-tiers pour accéder au réseau *Bitcoin*[132].

7. De *Bitcoin* à la *blockchain.* *Bitcoin* apparaît comme le « point culminant » de dizaines d'années de recherche en cryptographie[133]. Selon Andreas M. Antonopoulos, le protocole inclut quatre révolutions fondamentales, à savoir le protocole en lui-même qui consiste en un réseau décentralisé P2P, le registre public de transactions financières, le

---

[124] V., Annexe n° 3. Schéma simplifié du mécanisme d'inscription d'une transaction sur *blockchain*, p. 435.
[125] ANTONOPOULOS (Andreas M.), *op. cit.*, p. 10 (trad., préc.) : « Le protocole *bitcoin* inclut des algorithmes prédéfinis qui régulent la fonction de minage sur le réseau. La difficulté de l'exécution de la tâche effectuée par les mineurs – afin d'enregistrer un bloc de transaction sur le réseau *bitcoin* – est ajustée de façon à ce qu'en moyenne quelqu'un y arrive toutes les 10 minutes, peu importe le nombre de mineurs (et de CPUs) travaillant sur cette tâche à un instant *t.* »
[126] Il est possible de le télécharger par exemple sur le site : https://bitcoin.org/fr/telecharger.
[127] Il s'agit d'un logiciel informatique gratuit dont le code source est distribué sous une licence qui permet à quiconque de le lire, le modifier ou même le redistribuer. À titre d'exemple, la suite *Open Documents* est un logiciel *open source*, alors que la suite *Microsoft* (*Word, Excel,* etc.) ne l'est pas puisqu'elle est payante et privée.
[128] ANTONOPOULOS (Andreas M.), *op. cit.*, p. 12.
[129] *Ibid.*, p. 10.
[130] *Infra* n° 135. – V. également, Annexe n° 10. Schéma du contenu d'un bloc d'une *blockchain* : l'exemple de *Bitcoin* (blocs n°ˢ 549 313 à 549 315), p. 442.
[131] *Idem.*
[132] PAVEL (Ilarion), « La blockchain : Les défis de son implémentation », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 21. – Pour plus de détails sur le sujet, v., ANTONOPOULOS (Andreas M.), *op. cit.*, pp. 14 et s.
[133] ANTONOPOULOS (Andreas M.), *op. cit.*, p. 12.

système d'émission décentralisé, mathématique et déterministe de la monnaie illustré au sein du mécanisme de *mining* distribué, et enfin le mécanisme de vérification des transactions entièrement décentralisé[134]. Le réseau a débuté en 2009 avec une programmation basée sur la publication de Satoshi Nakamoto, puis a été révisé à de nombreuses reprises au fil des années par d'autres développeurs membres de l'écosystème[135]. Aujourd'hui, la totalité du marché *Bitcoin* a atteint les 1 000 milliards de dollars[136], détenant ainsi la première place des crypto-monnaies utilisées au niveau mondial. La plus importante transaction opérée sur la chaîne a franchi les 150 millions de dollars, transmise instantanément et opérée sans aucun frais[137].

Actuellement, la technologie qui sous-tend le *bitcoin* suscite vivement la curiosité dans de nombreux domaines d'activité. En effet, le protocole *Bitcoin* soutenant l'intégralité du système est basé sur une infrastructure inédite, qui révèle une vision beaucoup plus générale que la facette économique du *bitcoin*, à savoir celle d'un grand livre public, décentralisé et infalsifiable. La *blockchain* conquiert de plus en plus de secteurs, ses domaines d'application se diversifient et dépassent la fonction initiale de crypto-monnaie. Satoshi Nakamoto laisse derrière lui un héritage d'une valeur inestimable aux citoyens-internautes, s'incarnant dans un système capable d'instaurer de la sécurité, de la transparence, de l'immuabilité, et finalement de la *confiance* entre les Hommes.

D'après certains auteurs, la technologie *blockchain* a connu trois phases[138]. La *Blockchain 1.0* correspondrait aux transactions de monnaies électroniques. La *Blockchain 2.0* réunirait l'ensemble des utilisations dans le domaine financier et économique autres que les applications liées à la crypto-monnaie, telles que les actions, titres, obligations, prêts, hypothèques, votes, et enfin contrats intelligents. La *Blockchain 3.0* introduirait des applications sortant du contexte économique et financier, par exemple en matière de santé, de sciences, d'art et culture, ou encore d'administration publique. Finalement, ces trois phases reflètent une analyse fonctionnelle des applications de la *blockchain*. Or, il est possible d'adopter une approche évolutive de ses cas d'usage. Sous ce prisme, il convient de retenir que la technologie *blockchain* a commencé à se développer dans la

---

[134] *Id*.
[135] Satoshi Nakamoto a confié depuis le 12 décembre 2010 la gestion de *Bitcoin-QT via* le forum *bitcointalk* à Gavin Andresen [v., sur le forum *bitcointalk*, Post du 12 déc. 2010, 18:22:33, https://bitcointalk.org /index.php?action=profile;u=3;sa=showPosts], internaute présent depuis les origines du protocole, lequel devra céder sa place lorsqu'il l'aura jugé nécessaire à Hal Finnney [v., FAVIER (Jacques), TAKKAL BATAILLE (Adli), *Bitcoin. La monnaie acéphale*, *op. cit.*, p. 7].
[136] D'après le site *CoinMarketCap*, en date du 1er février 2021 [v., https://coinmarketcap.com/].
[137] ANTONOPOULOS (Andreas M.), *op. cit.*, p. 13.
[138] PAVEL (Ilarion), art. cit., p. 20.

sphère financière avec les crypto-actifs[139]. La *Blockchain 2.0* lui succédant correspond, au-delà du protocole *Bitcoin* et des crypto-actifs, à une vision beaucoup plus globale de la *blockchain*, fondée sur sa qualité de registre décentralisé et infalsifiable (*ledger*), capable de garantir la sécurité et l'intégrité des informations inscrites. La *Blockchain 3.0* équivaut quant à elle à une version automatisée de la *blockchain* nommée « *smart contracts* », programmée pour rendre exécutable les écritures inscrites au sein du *ledger*. Par extension du protocole *Bitcoin*, la *blockchain* peut désormais prendre soit la forme d'une base de données immuable, soit celle d'un système d'automatisation d'obligations prédéfinies. Même si ces applications feront l'objet de plus amples développements par la suite, il peut être intéressant d'en présenter les contours.

8. Les débouchés technologiques de la *blockchain* : le registre décentralisé. En qualité de « registre décentralisé et infalsifiable », la *blockchain* rend possible la traçabilité tant des actions que des dates auxquelles ces dernières ont été effectuées, et assure par conséquent un archivage pour une durée en principe illimitée. Selon Éric Barbry, « on ne perd jamais rien [sur la *blockchain*] [...] Au contraire, on y retrouve tout, et tout le monde y a accès »[140]. Ainsi est-il possible d'affirmer que le rêve d'un « très grand cahier que [...] tout le monde puisse lire, sur lequel chacun puisse écrire, mais qui soit impossible à modifier et indestructible », installé « place de la Concorde à Paris », de Jean-Paul Delahaye[141], est devenu lui aussi réalité. Les applications de la *blockchain* en tant que registre – *ledger* ou « *record keeping* » – décentralisé et public sont nombreuses et variées[142].

En effet, l'usage de la *blockchain* est un avantage dans le domaine de la conservation des données puisque, si elle sert de grand livre sûr et immuable, elle facilite tout autant le partage sécurisé des données inscrites sur ses pages. La sphère bancaire a très vite perçu son potentiel et, malgré quelques réticences originelles[143], a décidé d'investir dans la technologie des blocs[144], notamment en matière de KYC (*Know Your*

---

[139] D'après la définition du Portail de l'Économie, Des Finances, de l'Action et des Comptes Publics [https://www.economie.gouv.fr/], les crypto-actifs « représentent "des actifs virtuels stockés sur un support électronique permettant à une communauté d'utilisateurs les acceptant en paiement de réaliser des transactions sans avoir à recourir à la monnaie légale." ». – V., Bercy Infos, « Crypto-monnaies, crypto-actifs... Comment s'y retrouver ? », *economie.gouv.fr* [en ligne], 4 juill. 2018, https://www.economie.gouv.fr/particuliers/cryptomonnaies-cryptoactifs.

[140] BARBRY (Éric), « Smart contracts... Aspects juridiques ! », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 78.

[141] DELAHAYE (Jean-Paul), *Mathématiques et mystères*, éd. Belin, coll. Pour la science, 2016, p. 40.

[142] V. par exemple, U Change, *Livre blanc : Comprendre la blockchain*, éd. Creative Commons, 2016, pp. 34-53.

[143] COLLOMB (Alexis), SOK (Clara), LEGER (Lucas), « Technologie des registres distribués : quel impact sur les infrastructures financières ? », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 25.

[144] BEAUDEMOULIN (Nathalie) *et al*., art. cit.,p. 30.

Customer)[145]. Cette « Connaissance Client » concerne d'un côté, les règles en matière de Lutte Contre le Blanchiment et le Financement du Terrorisme (LCB-FT) et, de l'autre, la protection du client notamment vis-à-vis de ses placements financiers. Ce dernier volet, qui s'impose d'ailleurs de plus en plus comme un enjeu de conformité, requiert une adéquation entre les investissements conseillés par le professionnel et le profil financier du client détenu par celui-ci. C'est pourquoi la « Connaissance Client » doit être toujours plus précise et répertorier méticuleusement les informations sur l'identité, les coordonnées, les conditions familiale et professionnelle, la rémunération, le patrimoine, les dettes, … Seulement, les changements de situation sont fréquents et le KYC est *de facto* difficile à maintenir à jour pour les opérationnels[146]. C'est ainsi qu'une centaine d'établissements financiers ont décidé de se regrouper pour former le *Consortium R3*[147] dont l'un des objectifs à long terme est le partage des données KYC *via* une *blockchain* commune[148]. De cette façon, chaque banque profiterait du travail des autres banques en la matière, ce qui permettrait d'éviter les redondances, de diminuer les coûts de traitement des dossiers, et de rendre réactives les banques face à l'évolution constante de la normalisation dans le domaine[149].

Les banques ne sont pas les seules à s'être emparées de la technologie *blockchain*, les compagnies d'assurances y voient également une opportunité de sécuriser le partage et certifier les données entre elles. À titre d'exemple, le réassureur français SCOR a ainsi rejoint l'initiative mondiale B3i (*Blockchain Insurance Industry Initiative*) dans un objectif de partage de dossiers de réassurance *via* le réseau d'une *blockchain*[150].

Au-delà des domaines bancaire et assurantiel, la sphère de la santé voit également un intérêt à introduire la technologie des blocs dans ses protocoles. D'une part, la

---

[145] Depuis une ordonnance du 1er décembre 2016 (Ord. n° 2016-1635, 1er déc. 2016, renforçant le dispositif français de lutte contre le blanchiment et le financement du terrorisme, *JORF* n° 0280, 2 déc. 2016, texte n° 14), est concernée « toute personne qui, à titre habituel, soit se porte contrepartie, soit agit en tant qu'intermédiaire en vue de l'acquisition ou de la vente de tout instrument contenant sous forme numérique des unités de valeur non monétaires pouvant être conservées ou transférées, dans le but d'acquérir un bien ou un service, mais ne représentant pas de créance sur l'émetteur ». – Pour plus de détails, v., ORIOT (Linda), « Blockchain et KYC : premier pas vers l'identité numérique ? », *La Chain Tech* [en ligne], 30 janv. 2018, https://www.chaintech.fr/blog/blockchain-kyc-identite-numerique/.

[146] Pour plus de précisions sur le sujet, v., STARK (Josh), « Applications of Distributed Ledger Technology to Regulatory & Compliance Processes », R3 Reports [online], 14 Dec. 2017, https://www.r3.com/wp-content/uploads/2018/01/Reg_Compliance_R3.pdf.

[147] RAYNAL (Juliette), « R3 lève plus de 100 millions de dollars pour propulser des applications de la blockchain sur le marché », *Usine Digitale* [en ligne], 30 mai 2017, https://www.usine-digitale.fr/article/r3-leve-plus-de-100-millions-de-dollars-pour-propulser-des-applications-de-la-blockchain-sur-le-marche.N546433.

[148] ORIOT (Linda), « Blockchain et KYC : premier pas vers l'identité numérique ? », art. cit.

[149] *Id.*

[150] VIVAR (Mariona), « Blockchain : Scor rejoint l'initiative B3i », *News Assurances Pro* [en ligne], 8 févr. 2017, https://www.newsassurancespro.com/blockchain-scor-rejoint-linitiative-b3i/0169312694 : « La rationalisation de la communication et des transactions permettrait d'améliorer tant les processus que la qualité des services d'assurance proposés aux consommateurs ». – V. le site officiel de B3i, https://b3i.tech/.

blockchain pourrait intervenir pour résoudre l'importante progression de la compromission des infrastructures informatiques des instituts médicaux[151], problématique de cybersécurité à plusieurs reprises dénoncée en raison de la présence sur Internet de données de santé de millions de patients de différentes nationalités, y compris française[152]. D'autre part, la technologie intéresse également le secteur par sa fonction de traçabilité des opérations inscrites. Selon le dossier « *blockchain rallyes for healthcare* » de la société IBM (International Business Machines Corporation)[153], sa capacité à assurer l'intégrité des données tout en mettant en place un système de partage entre différentes parties est de nature à instaurer une véritable collaboration entre les services de soins de santé. De cette façon, la technologie *blockchain* pourrait assurer une prise en charge adaptée en cas de situation d'urgence et, d'une manière générale, améliorer les modèles de soins de santé communautaires. D'après IBM, cette technologie peut également relier les soins de santé, les finances et les paiements complexes en lien avec les soins fournis[154]. Elle estime enfin que la *blockchain* peut fournir le suivi d'un médicament, du fabricant au patient. Cela permet d'améliorer sa traçabilité à mesure qu'il traverse la chaîne d'approvisionnement, et d'aider à prévenir la contrefaçon de substances médicamenteuses[155]. IBM soutient finalement que « les propriétés inhérentes aux mécanismes d'accès par clés publique/privée cryptographiques, de *Proof of Work* et de réseau distribué, créent un niveau d'intégrité inédit dans le domaine de l'information relative aux services de santé »[156]. Une telle avancée est essentielle à l'amélioration et à

---

[151] HALDER (Steve), « September 2019 Healthcare Data Breach Report », *HIPAA Journal* [online], 21 Oct. 2019, https://www.hipaajournal.com, Home > Healthcare Cybersecurity > September 2019 Healthcare Data Breach Report. – V. également, TERZIAN (Jean), « Des hackers ont ciblé des données liées au vaccin de Pfizer et BioNTech contre le Covid-19 », *L'Usine Nouvelle* [en ligne], 10 déc. 2020, https://www.usinenouvelle.com/article/des-hackers-ont-cible-des-donnees-liees-au-vaccin-de-pfizer-et-biontech-contre-le-covid-19.N1038564 ; LEGRAND (Salomé), « Une cyberattaque tous les trois jours dans les hôpitaux : "Il est temps pour les États d'agir" », *Europe1* [en ligne], 26 mai 2020, https://www.europe1.fr/technologies/une-cyberattaque-tous-les-3-jours-dans-les-hopitaux-il-est-temps-pour-les-etats-dagir-3970734 ; « TRIBUNE : "Les cyberopérations visant des structures de soins de santé sont illégales et inacceptables" », *Le Monde* [en ligne], 26 mai 2020, https://www.lemonde.fr/idees/article/2020/05/26/les-cyberoperations-visant-des-structures-de-soins-de-sante-sont-illegales-et-inacceptables_6040741_3232.html.

[152] *Id.* ; WILLIAMS (Chase), « Data Leaks in the Medical Industry: A Worldwide Epidemic », *WizCase* [online], 12 Mar. 2020, https://www.wizcase.com/blog/medical-breaches-research/ ; « Protecting Patients, Providers and Payers. 2019 Healthcare Threat Report », *ProofPoint* [online], 2019, https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-2019-healthcare-threat-report.pdf.

[153] FRASER (Heather), « How Blockchains Can Provide New Benefits for Healthcare », *IBM* [online], 20 Feb. 2017, https://www.ibm.com/blogs/think/2017/02/blockchain-healthcare/ ; « Neuf fuites de données liées à des acteurs de la santé répartis dans le monde », *Portail d'Accompagnement Cybersécurité des Structures de Santé* [en ligne], https://www.cyberveille-sante.gouv.fr/cyberveille-sante/1475-neuf-fuites-de-donnees-liees-des-acteurs-de-la-sante-repartis-dans-le-monde.

[154] MARISSA (Laura), « Blockchain in Healthcare », *Medium* [online], 2 Feb. 2017, https://medium.com/@blockxlabs/blockchain-in-healthcare-6a0f8ee7cc4f.

[155] FRASER (Heather), art. cit.

[156] « *The inherent properties of cryptographic public and private key access, proof of work and distributed data, creates a new level of integrity for healthcare information.* » [notre trad.], SHARMA (Udit),

l'individualisation de la santé dans les communautés du monde entier. À cet égard, l'Estonie a institué, sous le nom de projet « *e-Estonia* », notamment[157], une carte d'identité nationale à puce, nommée « *electronic ID-card system* », reliée directement au dossier médical stocké sur *blockchain* de l'individu détenteur de la carte[158]. Aux USA, le projet *MedRec* envisage également la possibilité d'un partage des dossiers médicaux *via* un système de multi-signatures sur *blockchain*[159]. En effet, le problème relevé à de nombreuses reprises dans le secteur est celui d'un manque de visibilité des données des patients du fait d'un éclatement de la gestion médicale entre plusieurs institutions de santé[160]. Traitées tantôt dans un organisme, tantôt dans un autre, l'accès à l'ensemble du dossier est de plus en plus compliqué, et permet d'éviter toute erreur de diagnostic. L'objectif de *MedRec*, comme celui *d'e-Estonia*, est de remplacer les intermédiaires centralisés, permettre l'échange intègre et sécurisé des données sensibles, et ce, en mettant en place un système distribué et de validation, accessible et transparent, usant de la technologie des chaînes de blocs[161]. En contrepartie, les mineurs de la chaîne chez *MedRec*, dûment contingentés puisqu'il ne s'agirait que de chercheurs en médecine, auraient la possibilité de bénéficier d'un accès anonyme aux données à des fins de recherches médicales[162]. En parallèle, la *start-up* Blockfarma expérimente l'utilisation de la *blockchain* dans le domaine des médicaments avec l'objectif de donner la possibilité à chacun, *via* son smartphone, de contrôler instantanément l'authenticité d'une boîte de médicaments après achat[163]. Sur le continent européen, les projets *MyHealthMyData*, financé par la Commission européenne dans le cadre du programme de recherche et d'innovation Horizon 2020[164], et *PharmaLedger*, issu du partenariat de l'Innovative Medicines Initiative avec la Fédération Européenne des Associations et Industries

---

« Blockchain in healthcare: Patient benefits and more », *IBM* [online], 30 Oct. 2017, https://www.ibm.com/blogs/blockchain/2017/10/blockchain-in-healthcare-patient-benefits-and-more/.

[157] « Notamment », car les projets d'*e-Estonia* dépassent le domaine de la santé pour trouver application dans les secteurs juridique, bancaire, ou encore cadastral avec *e-Health Record, e-Prescription database, e-Law and e-Court systems, e-Police data, e-Banking, e-Business Register* ou encore *e-Land Registry*.

[158] Pour plus d'informations sur le sujet, v., le site officiel d'*e-Estonia* et son communiqué d'informations, respectivement : https://e-estonia.com ; https://e-estonia.com/wp-content/uploads/faq-a4-v02-blockchain.pdf.

[159] LEGEAIS (Dominique), « Blockchain », *JCl. Com.*, fasc. 534, n° 55.

[160] mitMediaLab, « MedRec Technical Documentation », MedRec [online], 2017, p. 1, https://medrec.media.mit.edu/images/medrec_technical_documentation.pdf.

[161] *Ibid.*, pp. 1-2.

[162] MARR (Bernard), « This is Why Blockchains Will Transform Healthcare », *Forbes* [online], 29 Nov. 2017, https://www.forbes.com/sites/bernardmarr/2017/11/29/this-is-why-blockchains-will-transform-healthcare/#4240a6961ebe. – MOLTENI (Megan), « Moving patient data is messy, but blockchain is here to help », *Wired* [online], 2 Jan. 2017, https://www.wired.com/2017/02/moving-patient-data-messy-blockchain-help/.

[163] LEGEAIS (Dominique), *op. cit.*, n° 35. – Pour plus de précisions, v., https://www.blockpharma.com/.

[164] V. le site officiel du projet, http://www.myhealthmydata.eu/. – COM(2011) 0808 final de la Commission au Parlement européen, au Conseil, au Comité économique et social européen, au Comité des régions, 30 Nov. 2011, Horizon 2020, The Framework Programme for Research and Innovation.

Pharmaceutiques (EFPIA)[165], ont pour objectif d'intégrer la technologie *blockchain* dans un processus de gestion de données de santé fiable, efficace et sécurisé. Alors que certains auteurs pensent que les capacités techniques de la *blockchain* pourraient constituer une garantie d'authenticité des prochains vaccins anti-Covid[166], des *start-ups* comme TIXnGO[167], VST Enterprises[168], SICPA et Guardtime[169], SGInnovate et Accredify[170], ou IBM[171] ont rapidement pris la mesure des difficultés à assurer l'intégrité des certificats et attestations de dépistage et ont développé une solution de passeport (ou certificat) de santé numérique délivré par des autorités officielles et enregistré sur un système de *blockchain*.

Dans le secteur diamantaire, la technologie de la chaîne de blocs a également trouvé à s'appliquer. Everledger, une *start-up* mondiale, qui, face à 45 milliards de dollars perdus chaque année pour des raisons de fraude à l'assurance et de recel de diamants issus de zones de conflits, a décidé de créer un registre numérique mondial répertoriant, accompagnant et protégeant les actifs précieux tout au long de leur existence[172]. Les membres d'Everledger collectent les caractéristiques de ces actifs[173], vérifient leur

---

[165] V. le site officiel du projet, https://www.imi.europa.eu/projects-results/project-factsheets/pharmaledger?.

[166] V. notamment, LOVETT (Laura), « Blockchain could be the key to vaccine distribution, says IBM », *Mobi Health News* [online], 25 Nov. 2020, https://www.mobihealthnews.com/news/blockchain-could-be-key-vaccine-distribution-says-ibm ; KORIN (Netta), « Using blockchain to monitor the COVID-19 vaccine supply chain », *World Economic Forum* [online], 20 Nov. 2020, https://www.weforum.org/agenda/2020/11/using-blockchain-to-monitor-covid-19-vaccine-supply-chain/ ; KLEIN (Christian), « From the Laboratory to the World: Distributing the COVID Vaccine », *LinkedIn* [online], 4 Dec. 2020, https://www.linkedin.com/pulse/from-laboratory-world-distributing-covid-vaccine-christian-klein/. – La pandémie a d'ailleurs significativement révélé le potentiel de la technologie, v. notamment, LACITY (Mary), VAN HOEK (Remko), « How the Pandemic Is Pushing Blockchain Forward », *Harvard Business Review* [online], 27 Apr. 2020, https://hbr.org/2020/04/how-the-pandemic-is-pushing-blockchain-forward.

[167] « Health n Go, une solution mobile sécurisée de remise de certificats de santé », *ELCA* [en ligne], 20 juill. 2020, https://www.elca.ch/fr/news/2020/health-n-go-une-solution-mobile-securisee-de-remise-de-certificats-de-sante.

[168] V. le site officiel, https://v-healthpassport.co.uk/?v=79cba1185463#:~:text=The%20'digital%20health%20passport'%20%26,in%20the%20most%20secure%20way. – V. également, « COVID-19 verified passport: World's first by a British tech firm », *UKTN* [online], 7 Dec. 2020, https://www.uktech.news/news/covid-19-verified-passport-worlds-first-by-a-british-tech-firm-20201207.

[169] « Passeport santé COVID-19 sécurisé », *SICPA* [en ligne], 19 avr. 2020, https://www.sicpa.com/fr/news/un-passeport-sante-covid-19-securise-par-blockchain-pour-accompagner-le-deconfinement.

[170] « Accredify and Parkway Pantai to Issue Verifiable Digital COVID-19 Swab Results to Travellers », *SG innovate* [online], 27 Oct. 2020, https://www.sginnovate.com/pressroom/accredify-and-parkway-pantai-issue-verifiable-digital-covid-19-swab-results-travellers ; « SGInnovate Venture Building Project Leverages Blockchain Technology for Personal COVID-19 Medical Records », *SG innovate* [online], 29 Sept. 2020, https://www.sginnovate.com/pressroom/sginnovate-venture-building-project-leverages-blockchain-technology-personal-covid-19 ; « SGInnovate, Accredify to launch Digital Health Passport », *Singapore Business Review* [online], 1st Oct. 2020, https://sbr.com.sg/information-technology/more-news/sginnovate-accredify-launch-digital-health-passport.

[171] PISCINI (Eric), « IBM Digital Health Pass puts privacy first », *IBM* [online], 25 Aug. 2020, https://www.ibm.com/blogs/watson-health/health-pass-puts-privacy-first/.

[172] Le site internet d'*Everledger*, v., https://www.everledger.io/.

[173] Les caractéristiques des diamants sont définies à partir des « quatre C », qui correspondent aux quatre éléments principaux d'évaluation d'une pierre en bijouterie, à savoir le carat (qui correspond au poids), la clarté, la couleur et la taille (*cut*) de la pierre. – V. également, MAURER (Bill), « Blockchains Are a

historique et leur propriété suivant les prescriptions internationales données par le SCPK (Système de Certification du Processus de Kimberley)[174], puis les enregistrent de façon permanente sur la chaîne de blocs. Cette *digital incarnation* ou *thumbprint* (« incarnation numérique », « empreinte digitale ») est utilisée par divers intervenants à travers la chaîne d'approvisionnement pour certifier la provenance et vérifier l'authenticité du produit. Actuellement, la plateforme *Everledger* comptabilise 980 000 enregistrements de spécifications sur des diamants au sein de la chaîne *Bitcoin*[175].

Dans le même ordre d'idée, des projets émergent avec l'idée d'enregistrer les marques sur la chaîne et de mettre en place des certifications communes au sein des *market places* dans le cadre notamment du projet de l'UE « *Import Control System2* » (ICS2)[176], ou encore d'attribuer un « passeport digital » aux œuvres d'art en les authentifiant et en traçant leur(s) changement(s) de propriétaire(s)[177].

La *blockchain* pourrait aussi, selon certains auteurs, faciliter les systèmes traditionnels notariés en permettant l'échange et le partage instantanés de documents entre études notariales, et autres administrations et organismes pouvant intervenir dans le domaine, tels que les services de publicité foncière, l'administration fiscale, les collectivités territoriales, les bureaux d'études et d'audits, ou les architectes[178]. Elle pourrait également assurer le rôle de registre pour les administrations publiques et l'État[179]. À titre d'exemple, et au-delà de l'application aux registres d'état civil, dans

Diamond's Best Friend: Zelizer for the Bitcoin Moment », *in* BANDELJ (Nina), WHERRY (Frederick F.), ZELIZER (Viviana A.), *Money Talks: Explaining How Money Really Works*, ed. Princeton University Press, 2017, p. 215-229.

[174] Résol. Assemblée Générale des Nations Unies n° 55/56, 29 janv. 2001, sur le rôle des diamants dans les conflits: briser le lien entre le négoce illicite des diamants bruts et les conflits armés afin de contribuer à la prévention et au règlement des conflits.

[175] « Everledger Plans Base de données Blockchain pour combattre la fraude artistique », *Bitcoin on Air* [en ligne], 2017, https://fr.bitcoinonair.com/everledger-plans-blockchain-database-to-combat-art-fraud.

[176] V. le site officiel du projet, https://ec.europa.eu/taxation_customs/general-information-customs/customs-security/import-control-system-2-ics2_fr, Commission européenne > Fiscalité et Union douanière > Informations générales sur les douanes > Sécurité et douanes > Import Control System 2 (ICS2) : « Le programme de sécurité et de sûreté avant arrivée des marchandises renforcera l'efficacité des contrôles douaniers fondés sur les risques tout en facilitant la libre circulation des échanges commerciaux légitimes aux frontières extérieures de l'UE. Il représente la première ligne de défense en termes de protection du marché intérieur de l'UE et des consommateurs de l'UE. » – V. également, MAXIMIN (Nathalie), « Le plan d'action des douanes contre la contrefaçon », *D. IP/IT* 2021, n° 3, *in* Dossier de Presse « Présentation du plan contrefaçon 2021-2022 », Roissy, févr. 2021, p. 122.

[177] Pour plus d'informations sur l'utilisation de la *blockchain* en matière de propriété intellectuelle, v., MARRAUD DES GROTTES (Maëlle), « Vincent FAUCHOUX, co-fondateur de BlockchainyourIp : "En matière de propriété intellectuelle, la blockchain présente l'avantage de couvrir toute la zone de l'avant-brevet" », *Wolters Kluwer France* [en ligne], 17 oct. 2017, https://www.actualitesdudroit.fr/browse/tech-droit/blockchain/9566/vincent-fauchoux-co-fondateur-de-blockchainyourip-en-matiere-de-propriete-intellectuelle-la-blockchain-presente-l-avantage-de-couvrir-toute-la-zone-de-l-avant-brevet. – V. également, le site internet de *Blockchain Your Ip*, https://blockchainyourip.com/.

[178] GEIBEN (Didier), JEAN-MARIE (Olivier), VERBIEST (Thibault) *et al.*, *Bitcoin et Blockchain : Vers un nouveau paradigme de la confiance numérique ?*, *op. cit.*, p. 52.

[179] En novembre 2019, Álvaro, un bébé né à Rio de Janeiro, est ainsi devenu le premier individu à être reconnu et à bénéficier d'une déclaration de naissance *via* la technologie *blockchain* (il s'agissait en l'espèce

certains pays où la corruption et la spoliation des propriétés foncières sont fréquentes, il serait intéressant d'instaurer un système de cadastre. Seulement, d'après Arnaud Manas et Yoram Bosc-Haddad, dans ces États, la transposition d'une administration « à l'occidentale » serait probablement « vouée à l'échec »[180]. D'autant plus qu'il n'est pas certain qu'un simple système d'attribution *via* registres fonciers traditionnels soit assez sécurisé et *de facto* adapté à ces situations. Il en va ainsi du système hondurien, qui consentit que ses résidents soient expulsés de leurs domiciles alors même qu'ils en détenaient les titres de propriété[181]. La *blockchain* est donc apparue comme un moyen de créer une forme de « wiki-cadastre » entièrement transparent, sécurisé et par-dessus tout infalsifiable et décentralisé[182]. Afin de mettre fin aux divers abus fonciers et spoliations des biens immobiliers auxquels ils étaient eux aussi confrontés, les gouvernements du Ghana et de Géorgie ont décidé de dématérialiser la gestion des cadastres sur le réseau d'une *blockchain* en collaboration notamment avec BitFury, une entreprise utilisant la *blockchain Bitcoin*[183]. Les citoyens ont désormais la possibilité de défendre leurs terres[184]. La même logique peut s'appliquer aux diplômes universitaires, qui font d'ailleurs l'objet de recherches financées par l'Éducation Nationale française[185], aux votes

---

de la solution *Notary Ledgers de Growth Tech*, qui utilise la technologie de la plate-forme *IBM Blockchain*) [« Primeiro bebê registrado com blockchain é brasileiro », *Olhar Digital* [online], 1 de novembro de 2019, https://olhardigital.com.br/2019/11/01/noticias/primeiro-bebe-registrado-com-blockchain-e-brasileiro/]. – En France, la gestion du Registre des commerces et des sociétés (RCS) est, depuis 2019, dématérialisée à travers les blocs d'une *blockchain* dédiée [V. par exemple, DUMOURIER (Arnaud), « Les tribunaux de commerce s'appuient sur la blockchain pour sécuriser la gestion du registre du commerce et des sociétés », *Le Monde du Droit* [en ligne], 18 mars 2019, https://www.lemondedudroit.fr/decryptages/63174-tribunaux-commerce-blockchain-securiser-gestion-registre-du-commerce-societes.html].

[180] MANAS (Arnaud), BOSC-HADDAD (Yoram), art. cit., p. 102.

[181] En l'espèce, il s'agissait de l'expulsion de Mariana Catalina Izaguirre, tandis qu'elle détenait un titre officiel la désignant propriétaire de la terre sur laquelle elle se trouvait. Mais les registres de l'Institut de la propriété du pays indiquaient qu'une autre personne était également enregistrée en tant que propriétaire, et cette personne a convaincu un juge de signer un ordre d'expulsion. Au moment où la fraude a été révélée et que la confusion juridique a finalement été réglée, la maison de Mme Izaguirre avait été démolie [v., « The great chain of being sure about things », *The Economist* [online], 31 Oct. 2015, https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things].

[182] MANAS (Arnaud), BOSC-HADDAD (Yoram), art. cit., p. 102.

[183] Pour plus de précisions, v., Blockchain France, *La blockchain décryptée : Les clefs d'une révolution*, éd. Netexplo, 15 juin 2016, p. 23. – « Des cadastres sur la blockchain », *Blockchain France* [en ligne], 3 mars 2016, https://blockchainfrance.net/2016/03/03/des-cadastres-sur-la-blockchain/ – « Honduras : fin de la fraude à la propriété grâce à la Blockchain », *Medium* [en ligne], 15 sept. 2017, https://medium.com/@BCDiploma/honduras-fin-de-la-fraude-%C3%A0-la-propri%C3%A9t%C3%A9-gr%C3%A2ce-%C3%A0-la-blockchain-392fc1d230d1.

[184] RILEY (Duncan) « Honduras to use Bitcoin Blockchain tech to run its land registry », *Silicon Angle* [online], 17 May 2015, https://siliconangle.com/blog/2015/05/17/honduras-to-use-bitcoin-blockchain-tech-to-run-its-land-registry/. – V. également, « Blockchain: Honduras 1-France 0 ? », *Blockchain France* [en ligne], 16 sept. 2015, https://blockchainfrance.net/2015/09/16/le-honduras-adopte-la-blockchain/.

[185] DE COETLOGON (Perrine) (dir.), « Réunion d'information #GTnum #Blockchain4Édu », Villeneuve d'Ascq (Laboratoire Cristal, M3, Cité scientifique), 26 juin 2018, non publié. Il s'agit du projet « #BLOCKCHAIN4EDU », piloté par Perrine de Coetlogon, experte numérique pour l'Enseignement Supérieur Europe & International. Pour plus d'informations, v., http://eduscol.education.fr/numerique/tout-le-numerique/veille-education-numerique/archives/2016/juin-2016/blockchain-education ; https://blockchain.sciencesconf.org/. V. également, LAMONTAGNE (Denys), « Blockchain en éducation : la gestion infalsifiable de la confiance – Certification, accès, authentification, découvrez les

électroniques[186], aux fonctions d'archivage des administrations publiques[187], aux documents administratifs nécessaires pour obtenir une pièce d'identité ou autre document officiel[188], et bien d'autres[189]. Les Émirats Arabes Unis comptent sur la participation de Dubaï au projet *LinuxOne* d'IBM pour « numériser les processus gouvernementaux ainsi que les services citoyens » d'ici 2021[190]. Reste à savoir quelles fonctions les Émirats entendent réellement déléguer aux protocoles.

Les cas d'usage se répandent et gagnent progressivement des secteurs variés tels que le commerce, le transport ou encore la logistique. Les grands groupes s'associent aux jeunes *start-ups* spécialisées dans la chaîne de blocs pour créer *la* plateforme de référence[191]. Que ce soit pour tracer l'acheminement des marchandises et ainsi prouver le respect des normes sanitaires[192], pour réduire les coûts liés à la multiplication des

---

possibilités du blockchain », *Thot Cursus* [en ligne], 26 nov. 2015 (dernière mise à jour le 20 janv. 2016), https://cursus.edu/articles/34938#.W1rbxNUzbIU.

[186] PINTARIC (Pierre), « Sécuriser ses archives numériques », *Information, données & document* 2017/3 [en ligne], vol. 54, pp. 40-41, https://www.cairn.info/revue-i2d-information-donnees-etdocuments-2017-3-page-40.htm. – V. également, le projet d'*e-voting* de *Luxoft*, associé à la ville de Zoug et à l'Université des sciences appliquées de Lucerne en Suisse, https://digital.luxoft.com/work/case-studies/blockchain.

[187] Des députés espagnols avaient soumis une proposition de loi à ce sujet : « Proposición no de Ley sobre la introducción de tecnología Blockchain en la Administración Pública en España » (« Introduction de la technologie blockchain dans l'administration publique d'Espagne ») par le Partido Polular (PP). V. à ce sujet, RIVERO (Jacqueline), « Grupo Parlamentario Popular propone utilizar blockchain en la administración pública española », *CriptoNoticias* [en línea], 29 jun. 2018, https://www.criptonoticias.com/regulacion/grupo-parlamentario-popular-propone-utilizar-blockchain-administracion-publica-espanola/. V. également, P. (Stanislas), « Espagne : Le Parti populaire propose d'utiliser la blockchain dans l'Administration », *Cryptonaute* [en ligne], 2 juill. 2018, https://cryptonaute.fr/espagne-parti-populaire-blockchain-administration/. – Grupo Parlamentario Popular en el Congreso, *Proposición no de Ley relativa a establecer un marco regulatorio para la inversión en criptomonedas eICOs n° 162/000588*, Presentado el 07/02/2018 [en línea], calificado el 13/02/2018, http://www.congreso.es/portal/page/portal/Congreso/Congreso/Iniciativas?_piref73_2148295_73_1335437_1335437.next_page=/wc/servidorCGI&CMD=VERLST&BASE=IW12&PIECE=IWC2&FMT=INITXD1S.fmt&FORM1=INITXLUS.fmt&DOCS=3-&QUERY=%28I%29.ACIN1.+%26+%28BLOCKCHAIN%29.ALL. – La France relève également la nécessité d'implanter la *blockchain* dans les services d'administration publique afin de pourvoir à leur amélioration, v. en ce sens, Rapp. AN n° 1501, 12 déc. 2018, de Laure DE LA RAUDIÈRE et Jean-Michel MIS sur les chaînes de blocs (*blockchains*).

[188] La République et canton de Genève a récemment mené un travail de concert avec la *blockchain Ethereum* concernant un système permettant de renforcer et sécuriser la délivrance d'extraits électroniques, ce qui permettrait de généraliser l'utilisation de la *blockchain* au sein des services d'administration publique dans le cadre de son action dans *l'e-Government* suisse (v., https://www.egovernment.ch/fr/umsetzung/innovationen/innovations-20172018/). V. également, l'ordonnance fédérale sur l'établissement d'actes authentiques électroniques et les légalisations électroniques (OAAE) du 23 sept. 2001, https://www.admin.ch/opc/fr/classified-compilation/20111505/201701010000/943.033.pdf.

[189] MEKKI (Mustapha), « Les mystères de la blockchain », *D.* 2017, n° 37, pp. 2160 et s., n° 13.

[190] DALTO (Leesa), « Smart Dubai and IBM to Offer the First Government-Endorsed Blockchain Platform in the Middle East », *IBM* [online], 30 Oct. 2018, https://newsroom.ibm.com/2018-10-29-Smart-Dubai-and-IBM-to-Offer-the-First-Government-Endorsed-Blockchain-Platform-in-the-Middle-East ; ZAGHET (Camille), « IBM et Dubaï en collaboration pour instaurer une plateforme de blockchain aux Emirats arabes unis », *Siècle Digital* [en ligne], 31 oct. 2018, https://siecledigital.fr/2018/10/31/ibm-et-dubai-en-collaboration-pour-instaurer-une-plateforme-de-blockchain-aux-emirats-arabes-unis/. – V. également, le site dédié au projet *LinuxOne*, https://www.ibm.com/fr-fr/it-infrastructure/linuxone.

[191] BERBAIN (Côme), art. cit., p. 8.

[192] L'utilisation du système a ainsi permis à une entreprise norvégienne importatrice de saumon d'inclure dans l'emballage de ses produits une série d'informations sur la qualité du poisson vendu, de son origine à son régime alimentaire ou aux vaccins appliqués, par le biais de *QR-Codes* [VIK AAM (Astrid), BERGAN

intermédiaires intervenant dans la chaîne logistique, pour prévenir les risques de fraude, ou pour éviter les erreurs d'aiguillages de conteneurs, le secteur fait appel à la technologie des blocs[193]. Depuis mars 2018, Carrefour, groupe français de la grande distribution, en collaboration avec le consortium *IBM Food Trust*, déploie la *blockchain* pour tracer les filières du « poulet d'Auvergne FQC » et celle de la « tomate allongée cœur Filière Qualité Carrefour », pour assurer aux producteurs comme aux consommateurs, *via* la *blockchain*, des pratiques de production agricole respectueuses du bien-être animal et de l'environnement[194]. Concrètement, les consommateurs peuvent trouver une étiquette de type *QR-Code* sur le produit, grâce à laquelle, *via* leur smartphone, ils pourront accéder à l'ensemble des informations utiles sur l'origine du produit, le nom du producteur, le type de culture et enfin la date de plantation, stockées sur *blockchain*. D'ici 2022, l'entreprise devrait ainsi tracer l'intégralité de ses produits de la « Filière Qualité Carrefour »[195].

9. Les débouchés technologiques de la *blockchain* : le *smart contract.* Une multitude de services non-financiers se sont directement appuyés sur le système de transactions de *Bitcoin* pour se développer. Désormais, que ce soit pour signaler qu'une technologie présente des similitudes ou au contraire se différencie du protocole *Bitcoin*, le terme « *blockchain* » est devenu incontournable, et sa comparaison avec *Bitcoin* inévitable. Par la suite, la technologie des blocs s'est développée au-delà du protocole qui l'a révélée et introduite sur le marché. C'est à partir de cette rupture protocolaire que sont nés les *smart contracts*, c'est-à-dire les « contrats intelligents », selon la traduction française la plus courante.

Dès 1993, le cryptographe, informaticien et juriste américain Nick Szabo s'intéresse à ce qu'il nommera par la suite les « *smart contracts* »[196]. Son idée est alors de créer une interface prenant en charge l'intégralité des étapes d'une relation contractuelle (« offre, pourparlers, convention, exécution et éventuellement décision de justice »), dans

(Lise), « Cermaq contributes to traceability with blockchain », *Cermaq* [online], 20 Nov. 2019, https://www.cermaq.com/news/cermaq-contributes-to-traceability-with-blockchain.

[193] U Change, *Livre blanc : Comprendre la blockchain*, préc., pp. 46-47.

[194] « Carrefour : poursuit le déploiement de la blockchain avec la tomate Filière Qualité Carrefour », *Zone Bourse* [en ligne], 4 juill. 2018, https://www.zonebourse.com/CARREFOUR-4626/actualite/Carrefour-poursuit-le-deploiement-de-la-blockchain-avec-la-tomate-Filiere-Qualite-Carrefour-26874208/. – V. également, le site de Carrefour, http://www.carrefour.com/fr/actualites/carrefour-poursuit-le-deploiement-de-la-blockchain-avec-la-tomate-filiere-qualite.

[195] HAREL (Camille), « Carrefour déploie une nouvelle blockchain sur son camembert de Normandie », *LSA* [en ligne] 23 sept. 2019, https://www.lsa-conso.fr/carrefour-deploie-une-nouvelle-blockchain-sur-son-camembert-de-normandie,328616 ; https://actforfood.carrefour.fr/nos-actions/la-blockchain-alimentaire.

[196] Expression utilisée en 1997 dans son article « *Formalizing and Securing Relationships on Public Networks* ». V., SZABO (Nick), « Formalizing and Securing Relationships on Public Networks », [online], 1st Sept. 1997, http://firstmonday.org/ojs/index.php/fm/article/view/548/469.

le cadre d'un marché d'affaires notamment, et de lui apporter les bénéfices des avancées technologiques *via* un protocole informatique[197]. L'objectif est de remplacer les tiers de confiance à chaque phase contractuelle. Au-delà d'un idéal distribué préservant la confiance, la technologie doit remplir les exigences de rapidité, de facilité, de sécurité et de performance[198], essentielles en matière contractuelle[199]. En 2002, *Scheme*[200], un langage programmatique minimaliste développé dans les années 1970[201], transcrivait les relations contractuelles sous la forme de contrats numériques[202]. Il faut malgré tout attendre *Bitcoin* et la création de la technologie *blockchain* par Satoshi Nakamoto en 2009[203] pour que le *smart contract* devienne accessible[204], puis décembre 2013, pour que le concept de « contrat intelligent » prenne réellement forme.

Alors âgé de 19 ans, le russo-canadien Vitalik Buterin[205] ambitionne de développer un « ordinateur mondial, que n'importe qui peut programmer et utiliser

---

[197] Nick Szabo précise à ce sujet que « les *smart contracts* réduisent les calculs informatiques ainsi que les frais de transaction généralement exigés par les mandants, tierces parties au contrat ou leurs machines. De plus, les *smart contracts* intègrent les différentes étapes du processus contractuel, à savoir l'offre, les pourparlers, la convention, l'exécution et éventuellement la décision de justice. Ils ont vocation à couvrir l'intégralité de ces étapes, en mettant l'accent sur la performance. Les *smart contracts* utilisent des protocoles et des interfaces utilisateurs dans le but de faciliter chaque étape du processus contractuel. Ce système met en place de nouveaux dispositifs de formalisation et de sécurisation des relations numériques beaucoup plus fonctionnels que leurs ancêtres contrats papiers inanimés. » (« *Smart contracts reduce mental and computational transaction costs imposed by either principal, third parties, or their tools. The contractual phases of search, negotiation, commitment, performance, and adjudication constitute the realm of smart contracts. This article covers all phases, with an emphasis on performance. Smart contracts utilize protocols and user interfaces to facilitate all steps of the contracting process. This gives us new ways to formalize and secure digital relationships which are far more functional than their inanimate paper-based ancestors*. », [notre trad.], *id.*).

[198] BARBRY (Éric), art. cit., p. 77.

[199] SZABO (Nick), « Formalizing and Securing Relationships on Public Networks », préc.

[200] Et depuis 2013 sous sa dernière version R7RS. V., RODRIGUEZ (Philippe), *op. cit.*, p. 140.

[201] Développé par Gerald Jay Sussman et Guy L. Steel. Pour plus de détails sur le sujet, v., SHASHA (Dennis) et LAZERE (Cathy), *Quand la vie remplace le silicium : Aux frontières de la bio-informatique*, éd. Dunod, coll. Quai des sciences, 2011, p. 115. – SUSSMAN (Gerald Jay) et L. STEELE, Jr. (Guy), « The First Report on Scheme Revisited », *Higher-Order and Symbolic Computation*, Vol. 11, No. 4, 1st Dec. 1998, pp. 399-404.

[202] *Scheme* est un langage de programmation ou langage machine, qui nécessite un logiciel interprète, tel que le logiciel *Bigloo*, pour traduire le langage humain. Le but étant de demander au processeur de la machine d'effectuer les actions permettant de calculer et de donner le résultat d'une requête préalablement saisie – l' « expression ». – Pour plus de précisions, v., BLOCH (Laurent), *Initiation à la programmation avec Scheme*, éd. TECHNIP, 2011, notamment pp. 26-30 pour les notions de base de la programmation *via Scheme*.

[203] Sur l'histoire de *Bitcoin*, *supra* n° 5.

[204] DE KRUIJFF (Tilburg), WEIGNAND (Hans), « Ontologies for Commitment-Based Smart Contracts », *in* PANETTO (Hervé), DEBRUYNE (Christophe), GAALOUL (Walid) *et al*., *On the Move to Meaningful Internet Systems. OTM 2017 Conferences: Confederated International Conferences: CoopIS, C&TC, and ODBASE 2017, Rhodes, Greece, 23-27 October 2017, Proceedings, Partie 2 : Vol. 10574 de Lecture Notes in Computer Science*, éd. Springer, 2017, p. 384.

[205] Notamment président de *Bitcoin France*, Philippe Rodriguez [v., RODRIGUEZ (Philippe), *op. cit.*, p. 60] décrit Vitalik Buterin comme l'incarnation : « d'une génération de jeunes "*geeks*", le teint pâle, la voix fluette, l'air absorbé, à mi-chemin entre la passion et la démence ». Vitalik Buterin a également co-fondé *Bitcoin Magazine* dès ses 17 ans. Il a étudié à *Abelard School* puis à l'Université de Waterloo à Ontario au Canada, qu'il a ensuite quittées pour se concentrer sur son projet.

comme il le souhaite, […] toujours allumé, […] très sécurisé, et […] public »[206]. Préalablement à son lancement, il rédige un livre blanc pour partager son idée[207]. Finalement, ce projet se concrétise sous le nom d'*Ethereum*. Selon lui, la *blockchain Bitcoin* a été créée dans le but d'être un protocole éminemment performant lorsqu'il évolue dans un seul et unique domaine, comme les transactions financières. En effet, le protocole SMTP (*Simple Mail Transfer Protocol*) ne peut constituer une base sur laquelle construire tous les autres types[208]. En revanche, Vitalik Buterin voit en la *blockchain* un extraordinaire potentiel. Ainsi persuadé que la technologie sous-jacente du protocole *Bitcoin* dispose d'un fort potentiel d'innovation au-delà des échanges de crypto-monnaies, il décide au début de l'année 2014 de financer le déploiement de sa plateforme. Afin d'obtenir les fonds nécessaires, il organise la prévente des e*thers* (ETH) sous la forme d'un fonds d'investissement en capital risque[209]. Converties, les sommes récoltées s'élèvent, à l'époque, à plus de 18 millions de dollars[210]. Dès le mois de mars 2015, Vitalik Buterin réussit à constituer une équipe de 30 employés à temps plein qu'il réunit au sein de la société Ethereum Switzerland GmbH (EthSuisse), localisée en Suisse. Ensemble, ils mettent au point *Frontier*, la première version d'*Ethereum* alors uniquement dédiée aux tests des développeurs[211], et le tout premier bloc de la chaîne – appelé *bloc genesis* – est créé. Alors qu'il n'avait conçu l'*ether*, crypto-monnaie d'*Ethereum*, que pour le bon fonctionnement de la *blockchain*, Vitalik Buterin est confronté à une hausse importante de son cours[212], ce qui rend sa gestion difficile. Par conséquent, il crée The Ethereum Foundation, une société à but non lucratif. La *blockchain* de Vitalik Buterin n'a pas été mise en place dans le but de concurrencer la *blockchain Bitcoin*, ni l'*ether* créé pour concurrencer le *bitcoin*. Les deux *blockchains* sont à la fois fondamentalement différentes et indubitablement complémentaires. « La

[206] POLROT (Simon), « Qu'est-ce qu'Ethereum ? », *Ethereum France* [en ligne], 14 févr. 2016, https://www.ethereum-france.com/quest-ce-que-lethereum/.
[207] BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », *github* [liens de publication originaux supprimés] [online], Nov. 2013, https://github.com/ethereum/wiki/wiki/White-Paper. Trad. : Asseth (Stéphane Roche, Jean Zundel, Frédéric Jacquot, Alexandre Kurth et Etienne Jouin), v., http://www.asseth.fr/2016/11/09/traduction-whitepaper-ethereum/.
[208] Il considère que le *bitcoin* est certes une « évolution radicale de la monnaie », mais qu'il est profondément limité notamment par son manque de reconnaissance étatique en ce sens qu'il « n'est adossé à aucun autre actif ni n'a de "valeur intrinsèque", ni émetteur centralisé ou régulateur » [*id.*].
[209] La vente de cette monnaie cryptographique rattachée à la *blockchain Ethereum* se poursuit du 22 juillet au 2 septembre.
[210] L'équivalent de 31 591 *bitcoins* à la date du 2 décembre 2014. – LELOUP (Laurent), *Blockchain : la révolution de la confiance*, éd. Eyrolles, 2017, p. 74.
[211] Après un échec avec *Olympic*, c'est *Frontier*, la première version d'*Ethereum* dédiée aux tests des développeurs, qui est mise sur le réseau le 30 juillet 2015. – RODRIGUEZ (Philippe), *op. cit.*, p. 60.
[212] Le 24 décembre 2018 à 12:00, le cours de l'ETH était de 122,80 EUR. V., https://courscryptomonnaies.com/ethereum.

blockchain Bitcoin a été conçue spécifiquement pour les devises alors qu'*Ethereum* permet de créer tout type d'applications », selon Vitalik Buterin[213]. Souvent surnommée « *Bitcoin 2.0* »[214], cette évolution de la technologie *blockchain* est finalement fondée sur un approfondissement des systèmes de protection de *Bitcoin*, à savoir la sécurisation des dépôts, le processus de prédiction, la protection des identités-utilisateurs, le dispositif de réputation, ou encore le mécanisme de sécurité à clés multiples[215]. En tant qu'outil de consensus distribué fondé sur les principes de fonctionnement des *blockchains*, et imprégné de l'ambition de son fondateur de coupler les caractéristiques de la *blockchain* avec des applications logicielles, *Ethereum* est présenté comme un protocole d'échanges décentralisés, s'exécutant sur un réseau distribué[216]. Par la suite, le protocole a continué à évoluer et, courant 2016, une nouvelle version nommée *Homestead* fait son apparition. Vitalik Buterin dirige désormais les nouvelles équipes de recherche d'*Ethereum* pour développer les prochaines versions *Metropolis* et *Serenity*, qui permettront à chacun d'accéder à la technologie des *smart contracts*, y compris l'individu non-initié[217].

Un *smart contract* est donc un contrat numérique rédigé sous la forme de protocoles cryptographiques, s'appuyant sur la technologie *blockchain* afin de sécuriser et plus particulièrement d'automatiser l'exécution des termes et conditions définis par les parties (deux ou plus). Il remplace ainsi le traditionnel contrat papier par un contrat auto-exécuté qui, une fois lancé, n'a plus que pour objectif de réaliser les volontés contractuelles transcrites au sein de la chaîne de blocs. Cette caractéristique est à l'origine du qualificatif « *unstoppable* »[218]. Le contrat écrit traditionnel est programmé dans un objectif de simplification et d'effectivité. De plus, son caractère *enforceable* (exécutoire) oblige à l'exécution stricte des termes prédéfinis. Ainsi, s'il advenait qu'une des parties n'exécutait pas son obligation, elle serait immédiatement sanctionnée en vertu des dispositions du contrat conclu sur la chaîne, par exemple financièrement[219].

---

[213] BUTERIN (Vitalik), « White Paper Ethereum », préc.
[214] LELOUP (Laurent), *Blockchain : la révolution de la confiance*, *op. cit.*, p. 73.
[215] RODRIGUEZ (Philippe), *op. cit.*, p. 60.
[216] Blockchain France, *La blockchain décryptée : Les clefs d'une révolution*, *op. cit.*, p. 8.
[217] Une discussion ayant eu lieu entre les membres de l'écosystème sur *Ethereum* permet de préciser les tenants et aboutissants de ces différentes versions. V., LEE (David), CHUEN (Kuo), DENG (Robert H.), *Handbook of Blockchain, Digital Finance, and Inclusion: vol. 2:ChinaTech, Mobile Security, and Distributed Ledger*, ed. Academic Press, 2017, pp. 158 et s.
[218] BASHIR (Imran), *Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained*, ed. Packt Publishing Ltd, 2nd edition, 2018, p. 262.
[219] Nick Szabo explique qu' « il est possible d'intégrer [un *smart contract*] au sein du matériel et du logiciel informatique utilisés, afin de rendre la rupture du contrat onéreuse (voire prohibitive) pour le contractant ayant manqué à ses obligations. » (« [*a smart contract*] can *be embedded in the hardware and software we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher* » [notre trad.], SZABO (Nick), « Formalizing and Securing Relationships on Public Networks », préc.).

Contrairement à *Bitcoin, Ethereum* fait appel à un langage « Turing-complet ». Celui-ci lui permet d'intégrer aux lignes de code des fonctions complexes, notamment pour que les contrats programmés puissent être mis à jour en temps réel et s'exécuter en fonction des instructions définies par les utilisateurs, telles qu'une suite de dispositions contractuelles[220]. La conception d'un langage « non-Turing complet » permet en revanche à *Bitcoin* d'éviter de nombreux risques de mauvaise programmation en cas, par exemple, de boucle infinie[221], et *a fortiori* de paralyser l'intégralité du réseau. C'est toutefois cette caractéristique du langage Turing-*in*complet qui lui a valu de ne pas être le protocole à l'origine des *smart contracts*[222].

10. Le fonctionnement de la *blockchain*. Aujourd'hui, la technologie permet de dépasser la simple sécurisation des transferts de monnaies ou d'actifs[223], et s'applique à tout secteur mettant en œuvre un échange, une sauvegarde ou même une preuve. Comme le constate Dominique Legeais, « la technologie *blockchain* constitue le support du *bitcoin* mais s'en distingue fondamentalement »[224]. Ainsi, *Bitcoin* n'est pas seulement le *bitcoin*, il constitue l'avènement de la *blockchain* en tant que technologie autonome. Une certaine divergence entre les auteurs est apparue avec, d'une part, ceux qui optent pour l'expression « des *blockchains* » afin d'appuyer le fait qu'il n'y pas qu'une seule *blockchain* qui a découlé de celle du *Bitcoin*[225] et, d'autre part, ceux qui, d'une manière générale et indissociable, évoquent « la *blockchain* » dans le sens de « la technologie *blockchain* »[226]. Les deux dénominations semblant pourtant trouver leur place, pour un souci de pertinence, il semble acceptable d'utiliser alternativement l'une comme l'autre selon les situations. Par ailleurs, la Commission d'enrichissement de la langue française relatif au vocabulaire informatique a officialisé sa propre définition de la *blockchain* en mai 2017 et considère que la « chaîne de blocs » est un « mode d'enregistrement de données produites en continu, sous forme de blocs liés les uns aux autres dans l'ordre chronologique de leur validation, chacun des blocs et leur séquence étant protégés contre toute modification »[227]. La mission d'information de l'Assemblée nationale a, pour sa

[220] LEE (David), CHUEN (Kuo), DENG (Robert H.), *op. cit.*, p. 155.
[221] Les boucles infinies, aussi appelées bombes logiques, sont en fait une action qui ne termine jamais car la condition est toujours vérifiée.
[222] BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », préc. – Pour plus de précisions sur la notion « Turing-complet », *infra* n° 68.
[223] DRILLON (Sébastien), « La révolution Blockchain », *RTD com.* 2016, p. 893, n° 1.
[224] LEGEAIS (Dominique), « Blockchain », *JCl. Sociétés Traité*, fasc. 2160, n° 2.
[225] BEAUDEMOULIN (Nathalie) *et al.*, art. cit., p. 29.
[226] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 9.
[227] Avis de la Commission d'enrichissement de la langue française relatif au vocabulaire informatique, *JORF* n° 121, 23 mai 2017, texte n° 20.

part, défini la *blockchain* comme « un registre, une grande base de données qui a la particularité d'être partagée simultanément avec tous ses utilisateurs […], et qui ont également tous la capacité d'y inscrire des données […]. Il n'y a pas d'autorité de contrôle centralisée […]. Les transactions ou les informations échangées entre les utilisateurs du réseau sont regroupées sur des blocs […], ils forment une chaîne : la blockchain. Les écritures enregistrées sur ce bloc et sur tous ceux qui le précèdent sont inaltérables et infalsifiables […] garanties […] par le fonctionnement même du réseau informatique et des règles cryptographiques qui y sont attachées »[228]. Alors que la résolution du Parlement Européen du 3 octobre 2018 mentionne également « les technologies des registres distribués et les chaînes de blocs » [229], le législateur français se contente de citer un « dispositif d'enregistrement électronique partagé »[230], excluant des textes les termes « *blockchain* » et « chaîne de blocs ». Se pose, malgré tout, la question de savoir à quoi correspond techniquement cette technologie.

Quel que soit son type ou son appellation, la *blockchain* consiste en « un très grand cahier, que tout le monde peut lire librement, gratuitement, sur lequel tout le monde peut écrire, qui est impossible à effacer et indestructible »[231]. Techniquement, la chaîne de blocs est un système informatique de stockage spécial, différent des disques-durs ou *clouds* habituels[232], puisqu'il permet à n'importe qui d'enregistrer des données (y compris non financières) et éventuellement de les transmettre à d'autres utilisateurs *via* un système entièrement immuable. Personne, pas même le propriétaire de la donnée inscrite, ne peut corriger, modifier ou supprimer une donnée car son inscription dans la *blockchain* est définitive. Pour ce faire, l'ensemble de ces inscriptions sont regroupées au sein d'un bloc ou, d'une « page »[233]. Puis, les blocs sont accrochés les uns aux autres, du plus ancien au plus récent, pour former la chaîne de blocs[234]. Pour pouvoir accrocher le bloc au reste de la chaîne – la page au reste du livre – celui-ci doit franchir les étapes de vérification et de validation[235]. Une à une, les inscriptions sont contrôlées, notamment pour que le système s'assure qu'il n'y a eu aucun changement ou aucune erreur. Le contrôle et la décision

[228] Rapp. AN n° 1501, préc.
[229] Résol. Parlement européen n° 2017/2772(RSP), 3 oct. 2018, sur les technologies des registres distribués et les chaînes de blocs : renforcer la confiance par la désintermédiation.
[230] CMF, art. L. 223-12, R. 211-1 et s. ; C. com., art. R. 225-86, al. 1er, R. 228-8, al. 2, R. 228-10.
[231] DELAHAYE (Jean-Paul), « Les blockchains, clefs d'un nouveau monde », *Pour la Science*, n° 449, Mars 2015, pp. 80-85.
[232] GUILHAUDIS (Élise), art. cit., p. 2.
[233] DELAHAYE (Jean-Paul), « Les blockchains, clefs d'un nouveau monde », art. cit., p. 80.
[234] FÉNÉRON PLISSON (Claire), « La blockchain, un bouleversement économique, juridique voire sociétal », *Information, données & documents* 2017/3, vol. 54, p. 21.
[235] Avis de la Commission d'enrichissement de la langue française relatif au vocabulaire informatique, préc. : « la validation d'un bloc [correspond à l'] opération informatique utilisée pour rendre un bloc infalsifiable et le valider dans une chaîne de bloc ».

finale d'accepter un bloc ou non n'appartiennent plus à un tiers de confiance centralisé comme dans un système traditionnel, mais à l'ensemble des membres du réseau P2P, appelés mineurs[236]. Cette validation s'opère par un procédé fondé sur un vote à la majorité des mineurs, nommé « consensus »[237]. La décision d'intégrer un bloc à la chaîne étant prise, ce bloc est ensuite scellé au reste de la chaîne par une suite complexe de chiffres et de lettres mélangeant à la fois les informations contenues dans le bloc, et celles contenues dans les blocs précédents[238]. Cette suite a pour fonction de graver de manière indélébile la position du bloc ainsi que son contenu au sein de la chaîne. Ces blocs, validés et reliés les uns aux autres et formant la *blockchain*, sont ensuite transmis à tous les autres utilisateurs du réseau[239]. De cette façon, si un utilisateur souhaite modifier son inscription, il ne peut le faire que sur sa propre version de la chaîne. En effet, personne ne peut modifier les versions possédées par les autres membres du réseau car les mineurs sont en principe beaucoup trop nombreux pour que l'un d'eux puisse infiltrer chaque ordinateur de chaque utilisateur en même temps, ou à tout le moins dans un laps de temps assez court pour qu'un second bloc ne soit pas déjà ajouté à la chaîne. Dans une telle hypothèse, la modification serait immédiatement rejetée comme étant non-conforme à la majorité des versions du réseau selon le principe de consensus. En règle générale, toute falsification est rendue inopérante *ab initio*. De plus, cette configuration permet de prémunir la chaîne de blocs de toute tentative de *hacking* puisque la chaîne n'est plus enregistrée sur un serveur unique et vulnérable mais par l'ensemble de la communauté[240]. Le concept des chaînes de blocs consiste donc en « une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle », selon Blockchain France[241]. Ainsi, l'essence-même de ce système inédit est la sécurité dans la distribution, la confiance dans la décentralisation, et, finalement, la relation sans intermédiaire.

11. La problématique de la disruption. Du latin *disruptus*, participe passé du verbe *disrumpere* (ou *dirumpere*) – qui signifie briser en morceaux, faire éclater, rompre,

[236] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., n° 3. – V., Annexe n° 3. Schéma simplifié du mécanisme d'inscription d'une transaction sur *blockchain*, p. 435.
[237] Le terme « consensus » doit être considéré dans son acception anglo-saxonne. V., DELAHAYE (Jean-Paul), « Les blockchains, clefs d'un nouveau monde », art. cit., p. 81.
[238] FÉNÉRON PLISSON (Claire), art. cit., p. 22.
[239] *Ibid.*, p. 21.
[240] *Id.* – V. également, GOSSA (Julien), art. cit., p. 393 : « les *blockchains* sont conçues pour que, lorsque tous les participants honnêtes dépensent une quantité d'énergie raisonnable, un participant malveillant doive dépenser une quantité d'énergie déraisonnable ».
[241] YERETZIAN (Antoine) (dir.), *La blockchain décryptée : les clefs d'une révolution*, éd. Netexplo, 15 juin 2016, p. 10.

détruire – l'adjectif « disruptif » désigne ce qui sert à rompre, ou ce qui correspond à une rupture soudaine. Toutes les activités fondées sur la confiance sont potentiellement sur le point d'être réformées[242]. En effet, comme le fait remarquer Mustapha Mekki, la *blockchain* offre des possibilités d'applications presque illimitées, « l'informatique étant devenue la plus belle école de l'imagination »[243]. Étant donné la grande diversité des problématiques que suscitent ces nouvelles pratiques, il convient d'élargir l'analyse de cette disruption révolutionnaire au-delà de l'utilisation purement financière de la *blockchain*. C'est la raison pour laquelle il semble davantage pertinent d'élire les questions relatives aux autres utilisations de la confiance en tant qu'objet central d'étude. De la même manière, l'attention aurait pu être portée à titre principal sur les questions de responsabilité ou même de droit applicable à ce nouveau pan de la technologie *blockchain*. Toutefois, excepté le cas très spécifique des minibons et des *Initial Coins Offering* (soit « ICOs »)[244], il n'existe à ce jour aucune régulation portant sur la *blockchain* en tant que telle[245], que ce soit du point de vue de *Bitcoin* ou des autres applications de la technologie. Il convient donc, par défaut, de se placer sous l'angle du droit existant. De plus, il apparaît en réalité que ces diverses interrogations se fondent dans une problématique plus vaste correspondant à la question de savoir quelle est ou sera la place des nouveaux usages de la *blockchain* dans les sociétés modernes et hiérarchisées. La technologie *blockchain* semble susceptible de surmonter cette défiance qui existe originellement entre les Hommes[246]. Elle serait en cela pleinement capable de disrupter l'intégralité des tiers de confiance actuellement discrédités[247], c'est-à-dire à la fois les tiers historiques et les nouveaux tiers spécialisés dans l'intermédiation. Son caractère « anti-système » viendrait à créer un mécanisme mutualisant les intérêts privés afin de produire de la vertu publique[248]. Même malhonnête et individualiste, volontairement ou involontairement, la communauté ne pourrait qu'œuvrer au nom de l'intérêt général[249]

---

[242] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 6.
[243] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., *loc. cit.*
[244] C. mon. et fin., art. L. 552-2 nouveau et s. – V. également sur le sujet, MESTRE (Jacques) (dir.), « Cas particulier de l'offre au public de jetons (Initial Coin Offering ou actifs numériques). Article 83 de la loi Pacte n° 2019-486 du 22 mai 2019 », *Le Lamy Sociétés Commerciales* 2021, n° 4844.
[245] Excepté au niveau de l'UE. En effet, le Parlement européen a adopté une résolution le 3 octobre 2018 sur les technologies des registres distribués et les chaînes de blocs (préc.), et la Commission européenne a publié, en octobre 2019, le rapport « *Blockchain Now and Tomorrow* », rédigé par son Centre commun de recherche, afin d'expliquer les mécanismes, tenants et aboutissants de la technologie *blockchain*. V., FIGUEIREDO DO NASCIMENTO (Susana), ROQUE MENDES POLVORA (Alexandre), ANDERBERG (Amanda), *et al.*, « Blockchain Now and Tomorrow », Publications Office of the European Union [online], 2019, http://publications.jrc.ec.europa.eu/repository/bitstream/JRC117255/blockchain_online.pdf.
[246] ROUSSEAU (Denise M.), SITKIN (Sim B.), BURT (Ronald S.), CAMERER (Colin), art. cit., pp. 393-404.
[247] GUILHAUDIS (Élise), art. cit., p. 1.
[248] MANAS (Arnaud), BOSC-HADDAD (Yoram), art. cit., p. 102.
[249] *Id.*

car le mécanisme en lui-même serait le garant de l'honnêteté collective[250]. En ce sens, les relations entre les Hommes pouvant être facilitées par la technologie, la confiance en l'autre n'est plus une variable essentielle[251]. La *blockchain* est souvent examinée comme la technologie qui bouleversera à terme « la manière dont la confiance est générée »[252] puisque c'est la technologie elle-même qui sera garante de la confiance qu'auront les utilisateurs en elle[253]. Son intégrité, qu'elle tient de la fiabilité technique de ses algorithmes[254], l'émancipe de tout tiers de confiance[255] et principalement de la tutelle des pouvoirs institués[256]. C'est ce qui lui vaut le nom de « *the trust machine* » (« la machine à créer de la confiance »)[257]. Finalement, l'innovation sans cesse grandissante porte en elle la promesse d'une nouvelle révolution technologique. Elle constitue indubitablement un tremplin stratégique pour la croissance appelant, de nouveau, une profonde transformation des modes de production et des modèles économiques actuels, voire de la vie de chaque citoyen et de leurs rapports avec le monde. Mais il semble parfois que la technologie soit victime de ses propres complexités, car son protocole demande des connaissances pointues qui le rendent difficilement accessible[258]. Mais, n'était-ce pas le cas également lorsqu'Arpanet – ancêtre d'Internet – est apparu dans les années 1980 ? Les espérances dans les nouvelles technologies sont parfois exagérées, le scepticisme à leur égard l'est souvent tout autant[259]. Seulement, le potentiel de cette technologie inédite est réel. C'est la raison pour laquelle de nombreuses *start-ups* nationales se saisissent de cette innovation et incitent le gouvernement à les soutenir dans leurs démarches[260], lorsqu'elles ne sont pas déjà soutenues par la Commission européenne ou le Conseil

[250] BARRAUD (Boris), « Les blockchains et le droit », art. cit., *loc. cit.*
[251] MANAS (Arnaud), BOSC-HADDAD (Yoram), art. cit., p. 102.
[252] FABRIZI-RACINE (Nina), « La blockchain : (R)évolution d'État ? », *JCP A* 2017, n° 49, p. 2306, n° 1.
[253] MANAS (Arnaud), BOSC-HADDAD (Yoram), art. cit., pp. 97, 102.
[254] FABRIZI-RACINE (Nina), art. cit., n° 1. – Arrêté du 27 juin 1989 relatif à l'enrichissement du vocabulaire de l'informatique : « [L'algorithme est] l'étude de la résolution de problèmes par la mise en œuvre de suites d'opérations élémentaires selon un processus défini aboutissant à une solution ». – Dictionnaire en ligne Larousse : un algorithme est un « Ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations. Un algorithme peut être traduit, grâce à un langage de programmation, en un programme exécutable par un ordinateur. »
[255] ZOLINSKY (Célia), « Fintech - Blockchain et smart contracts : premiers regards sur une technologie disruptive », *RD bancaire et fin.* 2017, dossier 4, n° 8.
[256] BARRAUD (Boris), « Les blockchains et le droit », art. cit., *loc. cit.*
[257] « The promise of the blockchain: The trust machine », *The Economist* [online], 31 Oct. 2015, https://www.economist.com/leaders/2015/10/31/the-trust-machine.
[258] BARRAUD (Boris), « Les blockchains et le droit », art. cit., *loc. cit.*
[259] *Id.*
[260] BERBAIN (Côme), art. cit., p. 8. – Le Sénat français a d'ailleurs tenu à rappeler l'importance pour la France et la recherche française de se positionner, d'abord scientifiquement, puis économiquement, dans le domaine des technologies numériques, et notamment de la *blockchain*. À ce titre, le Sénat soutient la demande faite par le Gouvernement de porter à 37 % l'objectif de l'effort de recherche (publique) en France sur ces sujets [Rapport n° 40 de M. Jean-Pierre MOGA au nom de la commission des affaires économiques sur le projet de loi de programmation, adopté par l'Assemblée nationale après engagement de la procédure accélérée, de la recherche pour les années 2021 à 2030 et portant diverses dispositions relatives à la recherche et à l'enseignement supérieur, 13 oct. 2020].

européen de l'innovation[261]. D'une manière générale, toutes se rangent derrière un plaidoyer pour le refus de manquer à nouveau « le tournant de la *blockchain* »[262], comme la France a raté celui d'Internet en misant sur le Minitel[263]. Même si certains ne voient dans la *blockchain* qu'un outil supplémentaire, amplificateur, de confiance[264], elle pourrait être l'instrument qui parviendra à instituer les fondements d'un véritable système décentralisé[265]. Aussi, la *blockchain* pourrait-elle à terme inverser les modes verticaux et hiérarchiques d'organisation publique et de régulation juridique, ce que n'ont pas réussi à faire les plateformes d'intermédiation du type Uber qui ont préféré « remplacer des prédateurs capitalistes par d'autres prédateurs capitalistes »[266]. D'ailleurs, le Conseil d'État français relève que « cette technologie peut être regardée comme un aboutissement du processus de désintermédiation »[267], voire de « désubérisation »[268]. Dans un contexte où la technologie se mêle à la fois à l'enthousiasme de la nouveauté, à l'excitation des promesses de bouleversements qu'elle pourrait générer, mais également au vocabulaire « *hype* »[269], il est finalement nécessaire de discerner la réelle innovation du simple effet de mode. Face à cet engouement généralisé, son caractère de « *trust machine* » se doit

[261] L'UE s'est positionnée sur le sujet dès 2018 en créant, d'une part, l'Observatoire-forum des *blockchains* de l'UE, dont la mission est de recenser les initiatives *blockchains* dans les États membres et d'accélérer l'innovation et le développement de l'écosystème de la *blockchain* au sein de l'UE pour ainsi contribuer à consolider la position de l'Europe en tant que leader mondial [https://www.eublockchainforum.eu/] et, d'autre part, l'Infrastructure européenne de service blockchain (EBSI), premier projet de réseau distribué à travers l'Europe ayant vocation à fournir des services publics transfrontaliers, tant aux administrations nationales qu'aux citoyens européens [https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/ebsi]. Par ailleurs, de nombreux financements, prenant la forme d'appels à projets ou de prix, ont été assurés par la Commission européenne (le programme Horizon 2020, par exemple, pour lequel le FEI a investi 100 millions d'euros) et par le Conseil européen de l'innovation (prix « *Blockchains for Social Good* » (« des blockchains pour le bien commun », qui a octroyé 5 millions d'euros à chacun des six lauréats), v. notamment, BOSSÉ (Vianney), « L'Europe est à l'aube de l'ère de la blockchain », *Voxeurop* [en ligne], 13 août 2020, https://voxeurop.eu/fr/europe-ere-blockchain/).

[262] GOETZ (Etienne), « Blockchain : France Stratégie presse le gouvernement d'agir pour ne pas rater le tournant », *Les Échos* [en ligne], 21 juin 2018, https://www.lesechos.fr/finance-marches/banque-assurances/0301857031847-france-strategie-presse-le-gouvernement-dagir-pour-ne-pas-rater-le-tournant-de-la-blockchain-2186084.php. – Rappelé notamment par le rapport rendu par la Fondation Concorde, Bpifrance et Havas Blockchain, v., « Blockchain : Une opportunité pour l'Europe Pourquoi la zone euro ne doit pas rater la seconde révolution d'internet ? », *Fondation Concorde* [en ligne], 4 déc. 2020, pp. 4-5, https://www.fondationconcorde.com, Fondation Concorde > Études.

[263] G'SELL (Florence), « L'appréhension des blockchains par le droit : Les questions d'Assas Legal Innovation », *French Web* [en ligne], 14 mars 2018, https://www.frenchweb.fr/lapprehension-des-blockchains-par-le-droit-les-questions-dassas-legal-innovation/319441.

[264] ZOLINSKY (Célia), art. cit., n° 8.

[265] Internet était à l'origine un système décentralisé également, mais, sous l'influence des sociétés monopolistiques, sa gestion a été centralisée. V., BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 7.

[266] *Ibid.*, p. 6.

[267] Conseil d'État, « Puissance publique et plateformes numériques : accompagner l'ubérisation - Étude annuelle 2017 », éd. Documentation française, n° 68, sept. 2017, cité dans : BARRAUD (Boris), « Les blockchains et le droit », art. cit., *loc. cit.*

[268] MARTIAL-BRAZ (Nathalie), « De quoi l'ubérisation est-elle le nom ? », *D. IP/IT* 2017, n° 4, p. 133.

[269] « *Hype* » signifiant « être à la pointe de la mode » d'après le dictionnaire en ligne Larousse. – RODA (Jean-Christophe), « Smart contracts, dumb contracts ? », *D. IP/IT* 2018, n° 2, p. 397, n° 9.

donc d'être évalué, car il convient de se demander si les *blockchains* peuvent réellement égaler, voire dépasser, les qualités attendues des tiers de confiance actuels.

L'investigation n'est pas sans conséquences, puisqu'il est question de changer en profondeur le système de gestion de la confiance dans les relations humaines[270], et notamment dans les métiers du droit[271]. D'ailleurs, si le droit a été instauré pour maintenir la justice et la paix dans un monde de « guerre de tous contre tous », le droit des contrats œuvre spécifiquement à instituer la confiance entre les Hommes. Or, la crise de 2008 a fait prendre conscience que derrière chaque contrat se trouvaient des individus faits « de chair et d'os », et pas seulement un bien de valeur marchande[272]. Il est ainsi essentiel d'analyser ce que la technologie est prête à changer et possiblement à améliorer dans les relations entre les Hommes. À ce titre, la *blockchain* dispose du système cryptographique assurément le plus évolué, sécurisé, et rapide. Mais il reste que les algorithmes « inquiètent autant qu'ils fascinent »[273]. En effet, la technologie est avant tout conçue pour être une solution. Pourtant, cette solution n'est pas parfaitement neutre, d'autant plus que l'Homme en est à l'origine. Bien souvent, « l'erreur est humaine »[274] et aucun algorithme n'est véritablement à l'abri d'un détournement de ses fonctions initiales[275]. Alors, si les utilisateurs discernent aisément l'intérêt pratique que soulève une telle technologie, ils ne doivent pas perdre de vue les risques qu'amène son emploi à grande échelle. C'est d'ailleurs ce qui, pour le moment, empêche la technologie *blockchain* de tenir pleinement son rôle d'espace libre de partage et d'échange entièrement sécurisé.

12. Plan. Il existe au sein du protocole de la *blockchain* une véritable volonté de simplification des relations humaines en général, et contractuelles en particulier. C'est la raison pour laquelle il conviendra d'analyser les apports de la *blockchain* en tant que système incubateur de confiance (PARTIE 1). Toutefois, il subsiste, au sein de la communauté *blockchain*, une difficile acceptation du système juridique actuel, ce que reflètent certaines caractéristiques qui constituent les spécificités de la technologie. Il s'agira alors de relever et d'évaluer les impacts qui pourraient, à plus ou moins long terme, représenter des freins à l'institution d'une confiance algorithmique (PARTIE 2).

---

[270] BERBAIN (Côme), art. cit., p. 8.
[271] *Ibid.*, p. 6.
[272] FABRE-MAGNAN (Muriel), « Chapitre V. La justice », *in* FABRE-MAGNAN (Muriel), *Le droit des* contrats, éd. Presses Universitaires de France, coll. « Que sais-je ? », 2018, pp. 119-121.
[273] ABITEBOUL (Serge), DOWEK (Gilles), *Le temps des algorithmes*, éd. Le Pommier, 2017, 4e de couverture.
[274] *Id.*
[275] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 8.

PARTIE 1

LES APPORTS DE LA *BLOCKCHAIN* EN TANT QUE SYSTÈME INCUBATEUR DE CONFIANCE : UNE VOLONTÉ DE SIMPLIFICATION DES RELATIONS CONTRACTUELLES

13. Dans les relations entre personnes privées, il est fréquent qu'une partie doive faire face à la mauvaise foi ou à l'inexécution de l'autre partie, que ce soit pour cause d'impossibilité, ou de refus. Le créancier sera alors contraint de saisir le juge afin de prouver ses droits et contraindre le débiteur défaillant à exécuter ses obligations à son égard.

Depuis sa naissance en 2008, la technologie des blocs a saisi de nouvelles opportunités de développement qui lui ont permis de décupler ses cas d'usage et de devenir « la version transactionnelle des réseaux de pair à pair » selon Jean-Paul Delahaye[276]. Ainsi, par extension du protocole *Bitcoin*, la *blockchain* peut prendre deux autres formes, à savoir celle d'une base de données distribuée et décentralisée (*ledger*), et celle d'un système automatisé d'obligations prédéfinies (*smart contracts*).

Le croisement de ces mécanismes avec les problématiques constatées ouvre de nouvelles perspectives ayant le potentiel d'éviter *ab initio* les complications révélées par la pratique. Il apparaît en effet que la technologie est capable, d'une part, *via* les *smart contracts*, d'automatiser l'exécution des obligations contractuelles, instituant ainsi une modalité technique d'exécution inédite (TITRE 1) et, d'autre part, *via* le système de registre décentralisé propre à toute *blockchain*, de faire bénéficier les contractants, en particulier si un contentieux surgit, de l'intégrité de principe du système pour apporter plus facilement la preuve de leur demande, promettant ainsi une sécurité juridique accrue (TITRE 2).

[276] Rapp. AN n° 1092, rapp. Sénat n° 584, 20 juin 2018, Comprendre les blockchains : fonctionnement et enjeux de ces nouvelles technologies, présenté par Valéria FAURE-MUNTIAN, Claude DE GANAY, et Ronan LE GLEUT, au nom de l'office parlementaire d'évaluation des choix scientifiques et technologiques.

TITRE 1. Les *smart contracts* : programmation d'une modalité technique d'exécution inédite

14. La mise en place d'une *blockchain* exécutant automatiquement ou, à tout le moins, sollicitant automatiquement d'exécuter les termes d'un contrat prédéterminé, établit un suivi dans l'exécution de celui-ci. Cette assistance est de nature à renforcer l'efficacité de la force contractuelle donnée à l'engagement, et à instaurer *ipso facto* un climat de confiance entre les parties dès la formation du contrat (Chapitre 1). Par ailleurs, l'innovation montre qu'il est possible de surpasser la fonction de support technique, et de faire matériellement et donc immédiatement exécuter les termes du contrat. L'objectif est de supprimer définitivement toute période d'expectative inutile et la potentielle mauvaise foi au sein de la relation contractuelle. En alliant le protocole du *smart contract* et la technologie des objets connectés et/ou intelligents, la *blockchain* rend l'exécution du contrat instantanée et contribue ainsi à amplifier l'efficacité de la force contractuelle (Chapitre 2).

Chapitre 1.
Renforcer l'efficacité de la force contractuelle : l'automatisation comme aide et suivi à l'exécution

15. Déjà sous l'Antiquité romaine, la *fides* – « la foi en la parole donnée, le respect des engagements, la loyauté », découlant de *Fides populi romani*, la déesse de la Bonne Foi du peuple romain – dictait les rapports des citoyens romains entre eux et avec les autres peuples[277]. Aujourd'hui, au-delà même du droit, l'ensemble des relations conventionnelles, et en particulier les relations d'affaires qui, par définition, « s'inscrivent dans une certaine durée » (CMF, art. L. 561-2-1), implique une confiance réciproque reposant sur le respect de la parole donnée. Chaque contractant se doit d'y veiller, au risque d'entraîner une rupture avant terme et sans reconduction des relations établies. Dans un rôle de « *trust machine* »[278], l'exécution automatique proposée par la *blockchain* apparaît comme un support actif au respect des engagements durant toute la vie du contrat. En incitant ainsi les parties à contracter et à exécuter de bonne foi leurs obligations, le *smart contract* veille indirectement à la pérennité des relations contractuelles (Section 1), et finit par transformer les rapports de confiance jusqu'ici établis entre les Hommes (Section 2).

Section 1. Pour la pérennité des relations contractuelles

16. À l'image d'un « clone numérique »[279], le *smart contract* est réputé être « une technologie [...] facilitant la conclusion, l'exécution et l'extinction des conventions »[280]. Il convient donc de déterminer en quoi consistent effectivement ces contrats auto-exécutés *via blockchain* (§ 1), afin d'évaluer leurs potentiels bénéfices pour les relations contractuelles (§ 2).

[277] CORNIOLEY (Pierre), *Naturalis obligatio, Essai sur l'origine et l'évolution de la notion en droit romain*, Suisse : Université de genève, Imprimerie du Journal de Genève, 1964, pp. 88-89.
[278] « The promise of the blockchain: The trust machine », *The Economist* [online], 31 Oct. 2015, https://www.economist.com/leaders/2015/10/31/the-trust-machine.
[279] VERBIEST (Thibault), « Blockchain : une révolution juridique ? », *RLDA* 2017/9, n° 129.
[280] GUERLIN (Gaëtan), « Considérations sur les smart contracts », *D. IP/IT* 2017, n° 10, p. 512.

§ 1. Les propriétés du contrat auto-exécuté *via blockchain*

17. Érigée sur les fondations de *Bitcoin* et mise au point pour accueillir toutes sortes d'applications, la *blockchain Ethereum* est devenue l'instrument protéiforme des relations entre les Hommes. S'ouvrant ainsi à une multitude d'utilisations bénéficiant des caractéristiques et spécificités de la technologie *blockchain*, le *smart contract* a pour ambition de révolutionner le droit contractuel, raison pour laquelle il est nécessaire d'examiner ses fondements et de comprendre son fonctionnement (A). L'appellation de « contrat intelligent » faisant néanmoins débat au sein de la doctrine, afin d'apprécier toutes les nuances de cette technologie, il s'agira d'apporter quelques éclaircissements relatifs à ce que certains auteurs évoquent comme étant « l'ambigüité du *smart contract* »[281], ou encore « le faux ami »[282] (B).

A. Fondements des smart contracts : le fonctionnement du « Bitcoin 2.0 » contractuel

18. **Définition.** Rédigé sous la forme de protocoles cryptographiques s'appuyant sur l'architecture décentralisée et distribuée de la technologie *blockchain* dévoilée par Satoshi Nakamoto, un *smart contract* prend la forme d'un contrat numérique capable de mettre automatiquement à exécution les termes et conditions définies par les parties (qui peuvent d'ailleurs être deux, ou plus). Il convertit le contrat traditionnel (« *fiat* »[283]), papier ou électronique, en un contrat automatisé – ou dynamique – grâce à une suite d'instructions algorithmiques[284] qui, une fois lancée, n'a plus que pour objectif la réalisation des volontés contractuelles transcrites au sein de la *blockchain*. En effet, selon certains auteurs, « les *smart contracts* s'auto-exécutent conformément aux termes de l'accord entre les parties, directement écrits dans les lignes de code »[285]. Seul le rapport de la Mission d'information commune sur les chaînes de blocs (*blockchains*) de décembre 2018 donne une définition officielle du « contrat intelligent » – selon la traduction française la plus courante –, indiquant qu'ils sont « des programmes informatiques

[281] *Id.*
[282] GRYNBAUM (Luc), « Assurances et blockchain », *in* « Dossier : Blockchain, une révolution juridique ? », *RLDA* 2017/9, n° 129.
[283] Le contrat « *fiat* » est le contrat conclut dans le monde réel, par opposition au contrat qui serait conclu sur *blockchain*. – Pour plus de précisions, v., MEKKI (Mustapha), « Les mystères de la blockchain », *D.* 2017, n° 37, n° 7.
[284] Définition *supra*, note 253 sous n° 11.
[285] « *Smart contracts are self-executing contracts with the terms of the agreement between the parties directly written into lines of code*. » [notre trad.], HYMAN (Gayle M.), DIGESTI (Matthew P.), « New Nevada Legislation Recognizes Blockchain and Smart Contracts Technologies », *Nevada Lawyer* [en ligne], Aug. 2017, p. 15, https://www.nvbar.org/wp-content/uploads/NevadaLawyer_Aug2017_Blockchain-1.pdf.

inscrits dans la *blockchain* », composés de « lignes de code qui permettent l'exécution de plusieurs commandes ("si la condition X est remplie, alors effectuer l'opération Y") de façon automatique », ajoutant qu' « une fois inscrit dans la *blockchain*, le *smart contract* est automatique, indélébile et transparent : son exécution aura lieu exactement comme prévu, puisque le code ne peut pas être modifié et qu'il peut être librement lu et vérifié par les parties en présence »[286]. Enfin, « le code est auto-exécutoire plutôt qu'exécutoire en vertu de la loi »[287], ce qui induit qu'aucun intermédiaire, donc aucun tiers de confiance, n'est nécessaire pour veiller à la bonne application de ses termes. Grâce à la distributivité et à la décentralisation de la *blockchain*, le *smart contract* se suffit à lui-même puisqu'il est auto-exécutant. Finalement, comme le constate Blockchain France, devenue Blockchain Partners[288], « [il présente] trois principaux apports : une vitesse accrue, une meilleure efficacité, et une certitude que le contrat sera exécuté comme convenu »[289].

19. Programme ou logiciel ? Alors que certains auteurs s'en tiennent à considérer le *smart contract* comme « un système algorithmique »[290], dans sa définition, Myriam Quéméner oscille entre considérer ce « contrat intelligent » comme étant un programme informatique, ou comme étant un logiciel autonome[291]. Y-a-t-il cependant une réelle différence entre ces deux termes ? En informatique, un programme est défini comme « une séquence d'instructions introduites en mémoire, et à laquelle le microprocesseur accède pour faire fonctionner l'ordinateur »[292]. Il s'agit de « travaux, calculs arithmétiques ou logiques, ou simulation d'un déroulement »[293], exécutés de manière automatique par une machine, sur la base d'un ensemble d'opérations prédéterminées. Un logiciel quant à lui inclut un ensemble plus vaste d'informations. Sa définition fait état d'une « notion large regroupant l'ensemble des programmes informatiques ainsi que les modes d'emploi »[294]. Un logiciel englobe donc des informations relatives à des

[286] Rapp. AN n° 1501, 12 déc. 2018, de Laure DE LA RAUDIÈRE et Jean-Michel MIS sur les chaînes de blocs (*blockchains*), p. 31.
[287] « *Code is self-enforcing as opposed to legally enforceable* » [notre trad.], LELOUP (Laurent), *Blockchain : la révolution de la confiance*, éd. Eyrolles, 2017, p. 80.
[288] La fusion s'est achevée en mai 2017 avec le Labo Blockchain [v., https://blockchainfrance.net/nos-experts-blockchain/].
[289] Blockchain France, *La blockchain décryptée : Les clefs d'une révolution*, éd. Netexplo, 15 juin 2016, p. 11.
[290] ORDONNEAU (Pascal), *Monnaies cryptées et blockchain : La confiance est-elle un algorithme ?*, éd. Arnaud Franel, 2017, p. 121.
[291] QUEMENER (Myriam), *Le droit face à la disruption numérique : Adaptation des droits classiques - Émergence de nouveaux droits*, éd. Gualino, Hors collection, 2018, n° 125.
[292] LILEN (Henri), *Dictionnaire informatique numérique*, éd. edi8, 2nd édition, 2014, section 24.
[293] Définition donnée par l'Encyclopédie informatique du web [AMBA, Accueil > Encyclopédie du Web > programme, http://www.amba.fr/encyclopedie-du-web.html].
[294] LILEN (Henri), *Dictionnaire informatique numérique*, *op. cit.*, *loc. cit.*

traitements effectués automatiquement par un appareil informatique, incluant des instructions de traitement regroupées sous forme de programmes, des données et de la documentation. À cet égard, il semble en effet difficile de trancher la question, si ce n'est que selon les informations transcrites au sein de la *blockchain*, le *smart contract* épousera les formes, alternativement, d'un logiciel complet si, par exemple, de précédents contrats inscrits au sein de la *blockchain* sont liés au contrat actuel, ou que d'anciennes transactions effectuées sont nécessaires pour traiter la nouvelle transaction[295], sinon d'un simple programme exécutant une tâche déterminée n'ayant aucun antécédent.

20. Définition technique et fonctionnement des *dApps* d'*Ethereum*. Les *smart contracts* sont apparus avec la création du protocole *Ethereum* qui a permis en outre leur concrétisation[296]. Un retour sur le fonctionnement de ce protocole semble alors indispensable afin de donner une vision informatique – et même algorithmique – à la définition des *smart contracts*.

Ethereum est donc un ordinateur mondial (« *Ethereum Virtual Machine* », sous le sigle « EVM ») que chacun peut programmer et utiliser comme il le souhaite, et notamment en créant des applications décentralisées appelées « *dApps* ». En pratique, celles-ci sont conçues à partir d'un ou plusieurs *smart contracts* programmés par l'utilisateur. Pour créer un contrat dit « intelligent », ce dernier traduit un contrat traditionnel en langage informatique utilisant des instructions conditionnelles de type « *IF (condition booléenne) – THEN (instruction) – ELSE (instruction alternative) – End If* », permettant de modifier un paramètre selon les conditions observées. Lorsque Nick Szabo décrivait le *smart contract* comme étant « un ensemble de promesses, spécifiées sous forme numérique, y compris les protocoles par le biais desquels les parties exécutent ces promesses »[297], il décrivait essentiellement la contractualisation de conditions, et en particulier des conditions d'affaires. Ainsi, à titre d'exemple, *A* et *B* sont des partenaires commerciaux qui possèdent conjointement une société vendant un produit. Il s'agirait de programmer, non un simple transfert de *bitcoins* de *A* vers *B*, mais une condition d'affaires telle que « - SI la vente entraîne un profit, ALORS diviser le montant du

[295] En ce sens que, s'il y a lieu de faire intervenir une crypto-monnaie, il sera primordial de connaître le montant détenus par chacun des *wallets* pris en compte.
[296] LEE (David), CHUEN (Kuo), DENG (Robert H.), *Handbook of Blockchain, Digital Finance, and Inclusion: vol. 2:ChinaTech, Mobile Security, and Distributed Ledger*, ed. Academic Press, 2017, p. 156.
[297] « *A smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises* » [notre trad.], SZABO (Nick), « Smart Contracts: Building Blocks for Digital Markets » [extract], Extropy #16 [online], 1996, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

bénéfice dans un rapport 60[A] : 40[B] ; - SINON, SI la vente aux enchères donne lieu à un seuil de rentabilité, ALORS donner 100 euros à [A et B] : - SINON, SI la vente entraîne une perte, ALORS récupérer le montant de la perte dans un rapport de 70[A] : 30[B] »[298].

L'exécution du « contrat intelligent » implique pour les cocontractants d'être en mesure de fournir du *gas*[299], sorte de carburant numérique permettant de rémunérer les mineurs pour la tâche exécutée[300], c'est-à-dire pour le téléchargement, la vérification et l'inscription sur la *blockchain* de la transaction contractuelle[301]. Pour l'écosystème, ce *gas* payé par l'utilisateur correspond à des « frais de traitement »[302]. Techniquement, le prix en *gas* nécessaire dépend de quatre facteurs, à savoir la complexité de la transaction, le cours de l'*ether* mis à jour automatiquement, le prix demandé par les mineurs, et enfin la patience de l'utilisateur. En effet, plus l'opération est urgente et complexe, c'est-à-dire plus elle contient de lignes de code, plus elle sera coûteuse. Certains calculs de base nécessitent un nombre prédéterminé de *gas* et il est facile pour les *wallets* de fournir ces estimations en fonction du type d'opération que l'utilisateur essaie d'effectuer. À titre d'indication, la transaction basique pour *Ethereum* correspondant à un virement simple entre deux utilisateurs requiert 21 000 *gas* – l'équivalent de 0,00047 *ether* en frais de traitement[303], soit 0,29 euro[304]. Toutefois, s'agissant d'un *smart contract*, l'exécution des termes du contrat entraînera une ou plusieurs opérations postérieures à leur inscription sur la chaîne. Or, ces futures opérations doivent être acquittées dès la souscription du *smart contract*. Il s'agira donc, pour les cocontractants, d'anticiper la quantité de *gas* à fournir à leur transaction, qui sera proportionnelle au nombre de fonctions à exécuter au cours de la validité du *smart contract*, le reliquat étant reversé le cas échéant. Dans le cas contraire, l'inscription en cours de validation pour laquelle il manquerait du *gas* serait annulée[305]. Par ailleurs, si le cours de l'*ether* évolue, il n'est pas le seul car, en fonction

---

[298] Exemple donné par un ingénieur indien, Mayukh Mukhopadhyay, qui propose d'ailleurs une analyse complète en quatre points de la définition de Nick Szabo précédemment citée. Pour plus de précisions sur le sujet, v., MUKHOPADHYAY (Mayukh), *Ethereum Smart Contract Development: Build blockchain-based decentralized applications using solidity*, ed. Packt Publishing Ltd, 2018, pp. 124-125.

[299] Ce *gas* représente une mesure infinitésimale de l'*ether*, 1 *gas* = 0,0000000225 *ether*.

[300] LELOUP (Laurent), *Blockchain : la révolution de la confiance*, *op. cit.*, p. 82.

[301] BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », *github* [liens de publication originaux supprimés] [online], Nov. 2013, https://github.com/ethereum/wiki/wiki/White-Paper.

[302] GUILHAUDIS (Élise), « Comprendre la blockchain à travers l'étude d'un cas pratique : le covoiturage "Blockcar" », *RLDI* 2017/12, nº 143, p. 4.

[303] TYCHEY (Jde), « uPort ou la gestion de l'identité par la blockchain », *Ethereum France* [en ligne], 27 sept. 2016 (mis à jour : 30 mai 2017), https://www.ethereum-france.com/uport-ou-la-gestion-de-lidentite-par-la-blockchain/.

[304] Il s'agit de 0.2888338 EUR (1 ETH = 614.54 EUR), selon le site de change https://courscryptomonnaies.com/ [v., https://courscryptomonnaies.com/ethereum#convertisseur] à la date du 1er janvier 2021.

[305] « [Le protocole exige] d'une transaction qu'elle fixe un nombre maximum d'étapes de calcul qu'elle est autorisée à effectuer. Si ce nombre est dépassé, le calcul est annulé mais les frais sont tout de même payés »,

du marché, chaque mineur peut fixer son propre prix en contrepartie de l'effort qu'il fournit[306]. Enfin, les transactions les plus rémunératrices étant exécutées en priorité par les mineurs, et inversement[307], selon l'urgence de l'opération pour le contractant, celui-ci peut moduler son offre de frais de traitement. Étant précisé que pour posséder des *ethers* il faut participer au réseau, sinon en acheter sur des plateformes de change de crypto-monnaies[308].

21. Depuis quelques années, l'expression « contrat intelligent » est utilisée de plus en plus fréquemment[309], mais force est de constater qu'il ne l'est pas nécessairement à bon escient. En effet, son sens diffère selon les auteurs, si bien que la question du bien-fondé de l'appellation « *smart contract* », quoique discutée par la doctrine, reste entière.

B. Divergences doctrinales : l'appellation trompeuse du contrat intelligent

22. Entre « intelligence » et confusions terminologiques. Tout d'abord, il s'agit de préciser le caractère « *smart* » du contrat « blockchaîné ». Il est ainsi envisageable d'estimer que le fait d'être auto-exécutant n'en fait pas *ipso facto* un contrat qualifiable d' « intelligent ». D'autant plus que dans les esprits, bien souvent, l'usage de ce terme

---

[Trad. : Asseth (Stéphane Roche, Jean Zundel, Frédéric Jacquot, Alexandre Kurth et Etienne Jouin), v., http://www.asseth.fr/2016/11/09/traduction-whitepaper-ethereum/], BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », préc.

[306] Ces deux mécanismes réunis – annulation en cas d'insuffisance de *gas* et fixation du prix par les mineurs – ont plusieurs avantages, notamment pour les mineurs, de refuser de traiter rapidement les inscriptions trop lourdes sauf à obtenir des frais de traitement plus élevés, d'éviter que certaines opérations deviennent hors de prix lorsque le cours de l'*ether* s'apprécie, et enfin d'empêcher la création d'une boucle infinie au sein d'un code (problème informatique de l'arrêt) puisqu'au moment où l'intégralité du *gas* transféré pour la transaction a été consommée, le nœud interrompt immédiatement le traitement de l'opération et annule la transaction. D'ailleurs, selon Vitalik Buterin, « supposons que : - Une transaction mène à k opérations, offrant la récompense kR à tout mineur qui l'inclut où R est fixé par l'expéditeur et k et R sont (approximativement) visibles par le mineur au préalable. - Une opération a un coût de traitement C pour chaque nœud (c.à.d. que tous les nœuds ont une efficacité égale). - Il y a N nœuds de minage, chacun possédant une puissance de traitement exactement égale (c.à.d. 1/N du total). - Il n'existe aucun nœud complet qui ne mine pas. Un mineur est disposé à traiter une transaction si la récompense attendue est supérieure au coût. Ainsi, la récompense attendue est kR/N puisque le mineur a 1/N chance de traiter le bloc suivant, et le coût de traitement pour le mineur est tout simplement kC. Par conséquent, les mineurs vont inclure les transactions où kR/N > kC ou bien R > NC. On note que R représente les frais par opération fournis par l'expéditeur, par conséquent une borne inférieure sur l'avantage que l'expéditeur retire de la transaction, et NC est le coût pour l'ensemble du réseau de traiter une opération. Par conséquent, les mineurs sont incités à inclure uniquement les transactions pour lesquelles le bénéfice utilitaire total excède le coût », [[Trad. : Asseth, préc.], BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », préc.]

[307] MUKHOPADHYAY (Mayukh), *op. cit.*, p. 153.

[308] GUILHAUDIS (Élise), art. cit., p. 10. – Pour plus de précisions sur ce point, v., POLROT (Simon), « Comment obtenir des ether (ETH) ? », *Ethereum France* [en ligne], 12 févr. 2016, https://www.ethereum-france.com/obtenir-des-ether-eth/.

[309] GUERLIN (Gaëtan), art. cit., *loc. cit*.

aboutit à former un amalgame en considérant qu'une couche d'intelligence artificielle (IA) est présente dans le programme hébergeant les *smart contracts*. En effet, la notion d'IA fait état d'une capacité à reproduire des aptitudes ou des comportements naturels, plus ou moins humains, tels que le raisonnement ou l'apprentissage[310]. Il pourrait être défendu qu'à partir du moment où une *blockchain* s'appuie sur un langage de haut-niveau[311] lui permettant d'effectuer des opérations cognitives abstraites – telles le traitement du langage naturel, la prise de décision ou l'aide à la décision – elle se rapprocherait du concept de raisonnement d'une IA. Néanmoins, en l'état actuel de l'évolution de la technologie *blockchain*, celle-ci ne semble pas disposer de ces capacités. La *blockchain*, notamment dans sa version mettant en œuvre des *smart contracts*, n'est pour le moment programmée que par un cercle relativement fermé d'informaticiens pour suivre strictement une série d'instructions informatiques spécifiques, réunies sous le vocable d' « algorithme »[312]. Les programmes d'IA requièrent nécessairement l'emploi d'algorithmes, cependant un algorithme n'utilise pas toujours des techniques de l'IA. Partant de là, il ne faut pas déduire qu'un contrat qualifié d' « intelligent » recourt inévitablement à un programme d'IA[313], ni considérer qu'il est doté d'une « intelligence » aux sens biologique et psychophysiologique du terme[314]. Vitalik Buterin a d'ailleurs

[310] Il apparaît acceptable de ne pas entrer dans le détail d'un sujet qui n'est pas celui de cette étude. Pour quelques précisions sur la notion d'IA, *infra*, note 313 sous n° 22.
[311] Sur ce point, *infra* n° 68.
[312] Définition *supra*, note 253 sous n° 11.
[313] COIFFARD (Didier), « Entretien du mois : La Blockchain a un sens pour répartir une partie de la confiance en rendant une information infalsifiable mais cette confiance est très en deçà de celle conférée par le notaire », *RLDC* 2017/4, n° 147 : d'après l'auteur, le contrat n'est pas intelligent car les opérations qu'il exécute ne sont que des opérations de simple envergure, n'appréciant pas encore la pleine complexité des relations humaines. Bien que cette position soit difficilement réfutable, le contrat est malgré tout auto-exécutant et diffère en cela du contrat classique, papier ou électronique.
[314] D'après Gaston Viaud, « pour l'homme adulte, il faut considérer l'évolution de son intelligence au cours de la longue histoire de l'Humanité [...]. Sur le plan de l'action, se développe d'abord l'intelligence artisanale de l'Homo faber [...] après un grand détour par la "mentalité primitive", l'intelligence humaine se développe sur le plan de la pensée ; elle devient l'intelligence logique et rationnelle de l'Homo sapiens, en se créant un outillage mental extraordinairement efficace [...] l'action tend alors à devenir de moins en moins empirique et de plus en plus rationnelle… » [VIAUD (Gaston), *L'Intelligence*, éd. Presses Universitaires de France, 1969, notamment pp. 110-111], faisant ainsi état d'une faculté essentiellement humaine, découlant de l'évolution de l'Homme à travers les siècles et le différenciant parmi les espèces vivant sur Terre (« Nul autre que l'être intelligent ne peut dire, je veux, j'aime, j'agis, je suis » [DE BONALD (Louis G. A.), *Législation primitive, considérée dans les derniers temps par les seules lumières de la raison, suivie de plusieurs traités et discours politiques*, éd. Le Clere, t. I, 1802, p. 254]). En parallèle, un philosophe a fait naître la confusion parmi les scientifiques en apportant ce qui peut être considéré comme une preuve qu'une machine ne raisonne pas, mais ne fait qu'appliquer une série d'instructions, écrites dans le but de la mener à la solution, sans toutefois qu'elle ne comprenne le sens, ni de l'une, ni de l'autre. L'intelligence perçue chez certaines machines ne serait donc qu'une impression, telle une boîte vide (v., sur l'argument de la chambre chinoise, NEVEJANS (Nathalie), *Traité de droit et d'éthique de la robotique civile*, éd. LEH éditions, coll. Science, éthique et société, 2017, p. 35 ; notamment, HAWKINS (Jeff), *Intelligence*, éd. Pearson Education France – CampusPress, 2005, pp. 28 et s.). Georges Duhamel n'écrivait-il pas « [La naïveté] est le plus dangereux adversaire de l'intelligence, de l'intelligence qui comprend tout, qui pèse tout et qui choisit » ? [DUHAMEL (Georges), *Cécile parmi nous*, éd. Mercure de France, Chronique des Pasquier, t. VII, 1938, p. 52]. V. également, DELAHAYE (Jean-Paul), « Les débats sur l'intelligence artificielle », *SPS* [en ligne], juill. 2015, n° 313, http://www.pseudo-sciences.org/spip.php?article2525.

déclaré en 2018 regretter d'avoir adopté l'expression « *smart contracts* » au lieu de lui préférer un terme plus « ennuyeux et technique » tel que « *persistent scripts* »[315].

En dépit de son absence de lien avec l'IA, le *smart contract* garde son caractère d'outil informatique dans la mesure où il est automatisable et parfois automatisé[316]. Cette caractéristique le distingue des autres contrats, c'est-à-dire des contrats traditionnels (contrats *fiat*), y compris électroniques, dont la seule fonction est d'enregistrer sur support lisible les droits et obligations de chaque partie (C. civ., art. 1125 et s.). Il pourrait éventuellement être argué l'existence d'outils informatiques de suivi contractuel ayant des qualités en apparence similaires à celles du *smart contract*. Seulement, ceux-ci se limitent souvent à envoyer des notifications ou des messages de relances lorsqu'il faut fournir un document, par exemple, à assurer le suivi de délais tels que les délais de renouvellement, ou encore de proposition de rétractation, et à d'autres fonctions que la technologie *blockchain* a, dans l'état de l'art, surpassées[317]. D'après Éric Barby, « les promoteurs des *smart contracts* nous proposent d'aller un cran, que dis-je, dix crans plus loin »[318]. Une fois le contrat lancé, il s'exécute sans intermédiaires[319], et parfois même sans l'intervention directe des parties elles-mêmes. Il en va ainsi, par exemple, d'un paiement automatique avec prélèvement sur compte-courant s'exécutant dès lors qu'une série de conditions prédéfinies sont réunies, ou du versement d'une indemnité de retard dès l'instant où ce dernier est constaté par la *blockchain* et ce, sans demande préalable du créancier et sans refus possible du débiteur. Le *smart contract* ne fait pas que notifier une date butoir, il rend l'obligation exécutable, voire exécutée, à cette même date. Il n'évolue pas, il ne raisonne pas, il n'a aucune conscience, *mais* il n'est pas pour autant comparable aux autres contrats. Il exécute les clauses inscrites dans son algorithme, ce qui lui donne une apparence d'intelligence parce qu'il rend beaucoup plus performante la mise en œuvre du contrat[320]. Il rend au principe du respect de la parole donnée tout son sens et son essence.

---

[315] @VitalikButerin (Vitalik Non-giver of Ether) *via* le réseau *Twitter*, 13 Oct. 2018, 10:21, https://twitter.com/VitalikButerin/status/1051160932699770882 : « *To be clear, at this point I quite regret adopting the term "smart contracts". I should have called them something more boring and technical, perhaps something like "persistent scripts"*. »

[316] CLACK (Christopher D.), BAKSHI (Vikram A.), BRAINE (Lee), « Smart Contract Templates: foundations, design landscape and research directions », *ARXIV* [online], 4 Aug. 2016 (update 15 Mar. 2017), p. 3, https://arxiv.org/pdf/1608.00771.pdf.

[317] BARBRY (Éric), « Smart contracts... Aspects juridiques ! », *Annales des Mines – Réalités industrielles* 2017/3 (août 2017), p. 77.

[318] *Id*.

[319] COIFFARD (Didier), art. cit., n° 147.

[320] BARBRY (Éric), art. cit., *loc. cit*. – V. également, LEGEAIS (Dominique), « Blockchain », *JCl. Sociétés Traité*, fasc. 2160, n° 52.

Finalement, sans pouvoir réellement et complètement réfuter ce terme choisi par Nick Szabo, il faut en conclure qu'il peut être source d'ambigüités, d'où l'importance de ne pas confondre « automatisation » et « intelligence artificielle ». Toutefois, son qualificatif « *smart* » pourrait peut-être convenir lorsque la *blockchain* unit ses qualités à celles des objets connectés et/ou intelligents. En effet, ces dispositifs permettent d'exécuter la *blockchain* dans le réel d'une manière concrète, de sorte que le nouveau système technologique constitué s'apparenterait davantage à une IA en ce qu'il tendrait à devenir quasi autonome dans ses choix et dans ses actes[321]. Ce dernier constat mène à se demander si, en définitive, il ne s'agirait pas d'une simple problématique de traduction faussée par la multitude d'acceptions et utilisations existantes du mot « *smart* ». Il convient, notamment, de mettre en évidence l'expression « *smart machine* » qui évoque, pour les anglophones, les systèmes informatiques capables d'apprendre et de prendre des décisions en conséquence, proche de la capacité humaine de « *self-determining* », autrement dit la faculté de décision. D'ailleurs, les membres de la communauté Ethereum France traduisent « *smart contract* » non pas par « contrat intelligent » mais par « contrat autonome »[322], se rapprochant davantage de l'idée d'un contrat auto-exécuté (« *self-enforcing* »[323]).

23. Entre « faux ami » et faux contrat. Le terme « contrat » du *smart contract* fait, quant à lui, l'objet de critiques plus vives. Dénoncé comme étant un « faux ami »[324], d'après Eva Théocharidi, « cette question nécessite un examen de la conclusion du contrat intelligent ; [...] étant donné que ce que le monde de la *blockchain* appelle "contrat intelligent" n'est pas automatiquement un contrat pour le monde du droit »[325]. L'origine de ce doute quasi généralisé[326] – *quasi* car certains auteurs n'excluent pas totalement cette possibilité[327] – se situerait donc dans la phase de formation du contrat intelligent. En effet, le fonctionnement du *smart contract* est souvent comparé à celui d'un logiciel ou d'un programme informatique, constitué essentiellement de lignes de codes. Il ne peut donc,

[321] Sur cette question délicate, *infra* n°s 70 et s.
[322] [Trad. : Asseth, préc.], BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », préc.
[323] LELOUP (Laurent), *Blockchain : la révolution de la confiance*, *op. cit.*, p. 80.
[324] Par exemple, v., GRYNBAUM (Luc), art. cit., *loc. cit.* ; GUERLIN (Gaëtan), art. cit., p. 512 ; CATTALANO (Garance), « Smart contracts et droit des contrats », *AJ contrat* 2019, p. 321.
[325] THÉOCHARIDI (Eva), « La conclusion des smart contracts : révolution ou simple adaptation ? », *RLDA* 2018/6, n° 138.
[326] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., *loc. cit.*
[327] V., par exemple, RODA (Jean-Christophe), « Smart contracts, dumb contracts ? », *D. IP/IT* 2018, n° 2, p. 397, n° 9 ; MOUNOUSSAMY (Ludovic), « Le smart contract, acte ou hack juridique ? », *LPA* 20 févr. 2020, n° 150t0, pp. 12-13 ; GIUSTI (Jérôme), « Les smart contracts sont-ils des contrats ? », *WordPress* [en ligne], 27 mai 2016, https://jeromegiustiblog.wordpress.com/2016/05/27/les- smart -contracts-sont-ils-des-contrats/.

dans ce cas, incarner un accord de volontés au sens de l'art. 1101 du C. civ.[328]. Cependant, deux situations divergentes apparaissent selon la fonction attribuée au *smart contract*.

24. Envisagé uniquement en tant que « modalité technique d'exécution », le *smart contract* n'est, en effet, pas véritablement un contrat au sens juridique du terme puisqu'il ne remplace pas le morceau de papier ou l'accord électronique *fiat*. Bien qu'il prenne la forme d'une application informatique permettant de fournir à l'exécution traçabilité, rapidité et facilité, son utilisation ne modifie pas l'application du droit positif qui appréhende uniquement le contrat *fiat*. Programmé pour être rattaché aux effets d'un contrat, il ne fait que l'assister, tel un contrat d'exécution ou sur l'exécution – accessoire du contrat principal auquel il est directement lié. Autrement dit, s'il permet une autonomie dans l'exécution, il n'est pas lui-même autonome, mais dépend dudit contrat traditionnel préalablement conclu. Il n'est cependant pas un « faux contrat », en ce sens qu'il s'apparente à un double de l'acte juridique initial enregistré informatiquement – ce qui pourrait permettre, dans certains cas, d'apporter un commencement de preuve de la relation contractuelle[329] –, voire à un « clone numérique » institué pour renforcer le respect de ses termes dans le monde matériel[330]. Comme le constate Lêmy Godefroy, « le code […] est ici la synapse qui transporte le droit de l'*instrumentum* aux faits, qui le transforme en actes, qui lui donne vie »[331].

25. En revanche, l'appréciation se complique lorsqu'il s'agit d'utiliser le *smart contract* en tant qu'instrument juridique, et pas simplement en tant que clone numérique auto-exécutable[332]. Le problème soulevé par l'éventualité d'une relation contractuelle directement nouée *via* la *blockchain* tient au consentement[333], et particulièrement à la preuve de celui-ci[334]. Depuis le 1er janvier 2020, l'État de l'Illinois aux États-Unis reconnaît aux *smart contracts* et autres contrats enregistrés sur *blockchain* la même valeur

[328] GUERLIN (Gaëtan), art. cit., *loc. cit*.
[329] En vertu de l'art. 1358 du C. Civ., « hors les cas où la loi en dispose autrement, la preuve peut être apportée par tout moyen ». Il s'agit notamment des actes dont le montant est inférieur à 1 500 euros (C. civ., art. 1359, al. 1er), des actes de commerce (C. com., art. L. 110-3), et du commencement de preuve par écrit (C. civ., art. 1360 et s.).
[330] VERBIEST (Thibault), « Blockchain : une révolution juridique ? », art. cit., *loc. cit*.
[331] GODEFROY (Lêmy), « Le code algorithmique au service du droit », *D.* 2018, n° 4, pp. 734 et s.
[332] Claire Fénéron Plisson concède pour sa part que les *smart contracts* seraient des contrats « un peu particuliers et bien étranges » [FÉNÉRON PLISSON (Claire), « La blockchain, un bouleversement économique, juridique voire sociétal », *Information, données & documents* 2017/3, vol. 54, p. 21]. – V. également, GIUSTI (Jérôme), art. cit.
[333] CHARENTENAY (Simon), « Blockchain et Droit : Code is deeply Law », *Gaz. Pal*. 14 nov. 2017, n° GPL305g1, p. 15.
[334] GIUSTI (Jérôme), art. cit.

que les contrats papier[335]. La dématérialisation du contrat a depuis longtemps été admise dans le droit positif sous la forme des « contrats conclus par voie électronique » aux art. 1125 et s. du C. civ.[336]. Cependant, selon certains auteurs s'appuyant sur les diverses exigences de forme attachées aux contrats électroniques, en particulier les modalités de souscription fixées par l'art. 1127-1, al. 3, du C. civ., et plus largement celles de l'art. 1108 du C. civ., il apparaît indéniable que le *smart contract* ne peut être assimilé à un contrat au sens juridique du terme[337]. En effet, en l'état actuel, ces modalités ne sont pas programmées par défaut dans l'algorithme des *smart contracts*, sans oublier que le programme en lui-même ne constitue qu'un ensemble de lignes de codes écrites dans un langage de programmation spécifique, traductibles mais pas facilement lisibles pour l'individu inexpérimenté.

Seulement, il faut remarquer que Vitalik Buterin n'a, semble-t-il, pas conçu *Ethereum* et les *smart contracts* dans l'optique de mettre à disposition un programme et une application figés mais il a, au contraire, fondé un modèle ouvert à travers lequel les programmeurs peuvent, à leur tour, créer des applications ouvertes mettant en œuvre des *smart contracts*[338]. Il a doté sa *blockchain* d'un langage de programmation à la fois Turing-complet[339] et « très généraliste » spécifiquement pour permettre la programmation de tous types de relation contractualisable[340]. Poursuivre ainsi le raisonnement aboutit à constater qu'il est en principe possible d'adapter la conception d'un *smart contract* aux exigences légales. De cette manière, aucun obstacle ne devrait en résulter, tant au niveau de la formation que de la validité du contrat puisque le contenu ainsi que les modalités d'exécution de celui-ci seraient conformes aux textes dès la conception. Par exemple, il est concevable qu'un professionnel mette en œuvre la divulgation de son offre sous la forme d'une inscription sur la chaîne dans le respect des exigences imposées par l'art. 1127-1 du C. civ., et que cette inscription soit assimilée, en vertu des caractéristiques d'immuabilité et de transparence d'une *blockchain*, à un procédé de conservation et de

[335] Illinois House Bill No. 3575, 19 Aug. 2019, *Blockchain Technology Act*, Public Act No. 101-0514 [https://www.ilga.gov/legislation/publicacts/101/101-0514.htm].
[336] Ord. n° 2016-131, 10 févr. 2016, portant réforme du droit des contrats, du régime général et de la preuve des obligations, *JORF* n° 0035, 11 févr. 2016, texte n° 26.
[337] Par exemple, v., GRYNBAUM (Luc), art. cit., *loc. cit.* ; GUERLIN (Gaëtan), art. cit., *loc. cit.* ; CATTALANO (Garance), art. cit., *loc. cit.* ; MEKKI (Mustapha), « Le smart contract, objet du droit (Partie 2) », *D. IP/IT* 2019, n° 2, p. 27 ; LEGEAIS (Dominique), *op. cit.*, n° 62 ; POULLET (Yves), JACQUEMIN (Hervé), « Blockchain : une révolution pour le droit ? », *Journal des Tribunaux*, n° 6748, 10 nov. 2018, p. 816 ; CHRISTODOULOU (Hélène), « Intelligence artificielle – Les nouvelles technologies à l'origine de l'évolution contractuelle », *Comm. com. électr*. 2020, étude n° 11.
[338] BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », préc.
[339] Sur la notion de langage Turing-Complet, *infra* n° 68.
[340] *Id.*

reproduction au sens de l'al. 1er du présent article[341]. Une discussion pourrait également être ouverte sur la façon d'introduire la « procédure de double clic » de l'art. 1127-2 du C. civ. concernant les contrats de fourniture de biens et services avec un professionnel au sein du *smart contract*. En effet, la spécificité de la *blockchain* repose sur des caractéristiques inédites, incluant l'instantanéité. Or, le destinataire de l'offre doit avoir la possibilité de valider ou de revenir sur son choix avant la conclusion du contrat. Une première hypothèse pourrait être d'envisager la programmation d'un délai de *x* jours laissé au cocontractant, à l'instar du délai de rétractation des art. L. 221-18 à L. 221-28 du C. conso, entre l'inscription d'une version non-confirmée du contrat dont l'exécution est suspendue jusqu'à l'accomplissement de la ou des conditions prédéfinies, et une éventuelle rétractation. Le contrat auto-exécuté pourrait également permettre le commencement d'exécution après accord préalable manifeste du cocontractant[342]. De la même manière, concernant les exigences *ad validitatem*, d'une part d'un écrit pour certains contrats déterminés (C. civ., art. 1174) et, d'autre part, de lisibilité et de présentation auxquelles sont soumises certaines stipulations (C. civ., art. 1175), il suffirait de pouvoir introduire, par exemple, des couches de traitement de texte pour que visuellement ces clauses ressortent du contrat et attirent l'attention du cocontractant[343]. Ainsi vulgarisée, la « suite de lettres, de caractères, de chiffres ou tous autres signes ou symboles » composant le code du *smart contract* et, *a fortiori*, les éléments essentiels du contrat, deviendraient suffisamment lisibles et intelligibles pour être valablement acceptés[344]. Le respect de ces règles est subordonné à la capacité technique de les programmer[345]. Mais, au-delà du bouleversement, malgré tout, des notions traditionnelles de formation des contrats en ce qui concerne notamment la phase de pourparlers[346], les spécificités techniques de la *blockchain*, et en particulier le poids des mécanismes d'anonymisation, peuvent être sources de difficultés. En effet, lorsque le *smart contract*

[341] THÉOCHARIDI (Eva), art. cit., *loc. cit.* – V. également concernant la sécurisation des relations contractuelles *via* une nouvelle forme d'archivage décentralisé, *infra* n°s 141 et s. – On peut d'ailleurs estimer que la fonction de publication de messages, permise par le protocole d'*Ethereum* en parallèle des mécanismes de transactions et de *smart contracts* (v. sur le sujet, KAROCYT, « Introduction aux Smart Contracts », *GitHub* [en ligne], 1er juin 2017, github.com, solidity-fr > docs > introduction-to-smart-contracts.rst ; PHUC (Morgan), « Caractéristiques de Solidity », *Bit Conseil* [en ligne], 22 août 2019, https://bitconseil.fr/solidity-langage-ethereum/), pourrait constituer une proposition de contrat par voie électronique.

[342] À l'image du renoncement exprès du consommateur à son droit de rétractation pour un contrat de fourniture de services conclu à distance ou hors établissement (C. consom., art. L. 221-28, 1°). – Pour une étude plus détaillée sur les notions de délai de rétractation et de renoncement exprès du consommateur à son droit de rétractation pour un contrat de fourniture de services conclu à distance ou hors établissement, *infra* n° 30.

[343] THÉOCHARIDI (Eva), art. cit., *loc. cit.*

[344] GIUSTI (Jérôme), art. cit.

[345] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., n° 10.

[346] BARRAUD (Boris), « Les blockchains et le droit », *RLDI* 2018/4, nº 147, p. 13.

persiste à se heurter à l'application de l'art. 1101 du C. civ. relatif à la notion de contrat[347], la reconnaissance de sa valeur juridique reste simplement impossible.

26. Bien qu'il n'ait jamais envisagé son *smart contract* comme un contrat au sens juridique du terme, Nick Szabo estime qu'il constitue un support technique qui permettra de transformer « un contrat à l'état brut en contrat réifié » et de moderniser l'approche contractuelle traditionnelle en exécutant automatiquement les termes prédéfinis d'un contrat[348]. D'ailleurs, certains auteurs envisagent de créer une « sous-section 3 », jointe à la section consacrée aux « Effets du contrat entre les parties » (C. civ., art. 1193 à 1198), exigeant des cocontractants qu'ils anticipent les conséquences de la vie du contrat, par exemple, en cas d'annulation de celui-ci[349]. Face à l'imminence de la mise à jour vers *Metropolis*, la version « grand public » de la Fondation Ethereum censée rendre accessible à tous l'utilisation de la chaîne[350], il est nécessaire d'examiner les effets que peut engendrer l'exécution automatisée des *smart contracts* sur les relations contractuelles entre personnes privées.

§ 2. Les bénéfices du contrat auto-exécuté *via blockchain*

27. Se fondant sur une logique très anglo-saxonne de P2P, Nick Szabo a prescrit un procédé contractuel simplificateur « mettant l'accent sur la performance »[351]. Il a conçu en effet le *smart contract* comme « un protocole de transaction informatisé qui exécute les termes d'un contrat », en précisant que « les objectifs généraux sont la satisfaction des conditions contractuelles mutuelles (telles que le paiement aux termes convenus, les privilèges, la confidentialité et même l'exécution forcée), la minimisation des exceptions à la fois malicieuses et accidentelles, et la minimisation des besoins d'intervention d'un tiers médiateur. Les buts économiques afférents incluent une diminution des pertes liées à la fraude, des coûts d'application arbitraire ou forcée et des autres coûts de transaction »[352]. En soutenant le bon déroulé de la relation par l'intermédiaire d'une

[347] Sur l'aléa de l'identification en matière de *blockchain*, *infra* n^{os} 114-115.
[348] SZABO (Nick), « Formalizing and Securing Relationships on Public Networks », [online], 1st Sept. 1997, http://firstmonday.org/ojs/index.php/fm/article/view/548/469.
[349] BARREAU (Catherine), « La régulation des smart contracts et les smart contracts des régulateurs », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 76.
[350] LELOUP (Laurent), « Constantinople, le hard fork Ethereum de janvier 2019 », *Finyear Magazine* [en ligne], 13 déc. 2018, https://www.finyear.com/Constantinople-le-hard-fork-Ethereum-de-janvier-2019_a40327.html.
[351] « […] *with an emphasis on performance* » [notre trad.], SZABO (Nick), « Formalizing and Securing Relationships on Public Networks », préc.
[352] Trad. : RODRIGUEZ (Philippe), *La révolution blockchain : Algorithmes ou institutions, à qui donnerez-vous votre confiance ?*, éd. Dunod, 2017, p. 140.

assistance à l'exécution (A), secondée par un procédé de dissuasion à l'inexécution (B), les contrats inscrits sur la chaîne de transactions ont pour vocation d'inciter les parties à contractualiser leurs accords.

A. Une assistance à l'exécution

28. Le *smart contract* est dur, mais c'est le *smart contract*. Les applications de la *blockchain* sont nées de l'idée de limiter l'intervention des tiers au sein des relations entre les Hommes, et en l'occurrence des tiers de confiance, tels que les mandants, les avocats, les juges[353]. En ce qui concerne les *smart contracts*, cette volonté s'est répandue à l'égard des parties elles-mêmes. Le but de tout contrat ainsi codé est de s'exécuter de manière automatique dès lors que les faits matériels rencontrent les conditions pré-informatisées[354]. Son caractère « *enforceable* »[355] (« exécutoire ») doit obliger chaque partie à l'exécution stricte des termes prédéfinis. Par conséquent, fort d'une exécution entièrement automatisée et réputée neutre, le *smart contract* permet aux parties de bénéficier d'une exécution parfaite – de la formation à l'extinction du contrat[356] – dépourvue des usuelles mauvaise foi ou « erreur humaine » qui parasitaient la continuité des relations contractuelles établies. Selon plusieurs auteurs, l'auto-exécution des contrats serait la solution qui permettrait d'éviter *ab initio* l'ensemble des complications révélées par la pratique du contentieux en droit des obligations[357]. Afin d'apprécier l'importance d'une telle caractéristique, l'un d'eux invite à imaginer « un monde dans lequel l'exécution forcée n'est plus une cause d'action parce que les contrats exécutent eux-mêmes automatiquement l'accord des parties »[358].

C'est avec cette idée que Bruno Dondero théorise l'usage des *smart contracts* dans le domaine des pactes d'actionnaires et droit de préemption afin « d'éviter que puisse intervenir la cession au profit [d'un tiers], en rendant automatique l'exercice du droit de

[353] RODA (Jean-Christophe), art. cit., n° 19.
[354] BASHIR (Imran), *Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained*, ed. Packt Publishing Ltd, 2nd edition, 2018, p. 262. – Autrement dit, « il ne faut pas comprendre ici qu'ils s'exécutent par eux-mêmes, mais qu'ils sont exécutés automatiquement lorsque leurs conditions sont réunies » [GOSSA (Julien), « Les blockchains et smart contracts pour les juristes », *D. IP/IT* 2018, n° 7-8, p. 393].
[355] SZABO (Nick), « Formalizing and Securing Relationships on Public Networks », préc.
[356] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 12.
[357] HINKES (Andrew), « Blockchains, smart contracts, and the death of specific performance », *Inside Consel* [online], 29 Jul. 2014, http://web3.insidecounsel.com/2014/07/29/blockchains-smart-contracts-and-the-death-of-speci?slreturn=1532806704 ; POULLET (Yves), JACQUEMIN (Hervé), art. cit., p. 816.
[358] « *Imagine a world where specific performance of contracts is no longer a cause of action because the contracts themselves automatically execute the agreement of the parties* » [notre trad.], HINKES (Andrew), art. cit.

préemption et le transfert des actions concernées »[359]. Plus précisément, il s'agirait selon lui de créer un *smart contract* qui « proposera aux actionnaires, s'il détecte une vente à [*T* (le tiers)], que les bénéficiaires d'un droit de préemption puissent l'exercer s'ils le souhaitent. Sera alors généré, à partir de la vente à *T* qui était en attente d'exécution, un contrat de vente aux actionnaires bénéficiaires du droit de préemption, contrat qui recevra exécution sans besoin d'intervention de *A* (le cessionnaire) si la préemption est exercée », ajoutant que « les documents nécessaires à la réalisation de la cession par *A* de ses actions aux actionnaires ayant mis en œuvre la préemption seront produits automatiquement »[360]. En renforçant la promesse faite, le débiteur n'est plus censé ignorer la priorité consentie, de sorte que le bénéficiaire du droit de préemption est garanti contre d'éventuelles complications dues à une violation du pacte par le promettant (C. civ., art. 1123, al. 2). Plus encore, le tiers ne peut plus méconnaître l'existence du pacte, quand bien même aurait-il consciemment choisi de rester dans l'ignorance en n'exerçant pas l'action interrogatoire mise à sa disposition (C. civ., art. 1123, al. 3 et 4). Puisant son origine dans la loi ou résultant d'un acte contractuel volontaire en vertu des art. 1123, 1103 et 1104 du C. civ., l'utilisation du droit de préemption est en effet un gage de confiance entre le propriétaire d'un bien et un potentiel acheteur, lequel reçoit la promesse – ou le bénéfice légal – d'une priorité en cas de vente par le premier. Lorsque ce droit découle, notamment, d'une clause contractuelle, la pratique révèle une multitude de contentieux majoritairement fondés sur des divergences d'interprétation dans lesquelles le débiteur de la préemption essaye de s'engouffrer dans l'espoir d'échapper à ses engagements initiaux[361]. Un auteur ajoute que « de même, en cas d'inaliénabilité inscrite dans les statuts d'une société, le *smart contract* permettrait de bloquer la cession des titres si la durée de détention n'est pas atteinte ; le programme informatique rendrait impossible tout

[359] DONDERO (Bruno), « "Smart contracts", pacte d'actionnaires et droit de préemption », *brunodondero.com* [en ligne], 13 mars 2016, https://brunodondero.com/2016/03/13/smart-contracts-pacte-dactionnaires-et-droit-de-preemption/.

[360] *Id.*

[361] V., par exemple, Cass. Com., 15 mars 2017, n° 15-20.440 (droit de préférence et de préemption concernant la cession de parts sociales ou d'actions) ; Cass. Com., 21 juin 2017, n° 15-24.534 (pacte d'actionnaires instituant un droit de préemption en cas de cession de titres) ; PILLET (Gilles), « Le fonctionnement du pacte de préférence », *Rép. civ. Dalloz*, v° Pacte de préférence, 2016 (actualisation : janv. 2019), n[os] 67 et s. ; BLONDEAU (Christophe), « La cession des titres à l'épreuve des droits de préemption. Contentieux récents », *Option Droit & Affaires* [en ligne], 21 mars 2018, https://www.optionfinance.fr/droit-affaires/la-lettre-doption-droit-affaires/la-lettre-du-21-mars-2018/la-cession-des-titres-a-lepreuve-des-droits-de-preemption.html. Le contentieux s'étend par ailleurs au droit de préemption urbain (v., par exemple, BOUYSSOU (Fernand), « Le contentieux des préemptions ou l'absence de recours effectif », *AJDA* 2004, n° 11, pp. 561 et s. ; LE BOT (Olivier), PITTARD (Yves), « Dossier 540 – Contentieux de l'urbanisme », *Dalloz professionnels Pratique du contentieux administratif*, déc. 2018 (synthèse d'actualité : nov. 2019), Section 4. « Le contentieux des décisions de préemption », n[os] 540.2710-540.2730).

mouvement des titres dans la blockchain »[362]. Accessoiriser, pour le moins, une clause contractuelle d'un *smart contract* s'inscrit ainsi dans une logique de pérennité des relations établies. Cela peut concerner les associés, les actionnaires, les fournisseurs, les franchiseurs, les communes (C. urb., art. L. 210-1 et s.), les locataires d'habitation (Loi n° 89-462 du 6 juillet 1989, art. 15[363]), de locaux à usage commercial ou artisanal (C. com., art. L. 145-46-1), mais également les titulaires d'un droit de première offre, d'un droit de premier refus, ou d'une promesse unilatérale (C. civ., art. 1124), et, par extension, tout titulaire d'un droit en vertu d'un accord. Plus encore, l'utilisation du *smart contract* tendrait à limiter tant les contentieux que l'engorgement des tribunaux puisqu'en effet, dans une telle conjoncture, le non-respect des engagements ne serait plus, non plus, une cause d'action.

29. Sécurité et relations facilitées. Corollaire de la garantie d'une exécution parfaite, la technologie *blockchain* sur laquelle les *smart contracts* se fondent concentre des qualités de sécurité et d'immutabilité. Étant donné que le *smart contract* est censé se poursuivre jusqu'à ce qu'il trouve application conformément à ses stipulations contractuelles, il est, en principe, impossible de le modifier ou de le rompre en cours d'exécution. Autrement dit, il est « *unstoppable* » (« inarrêtable »)[364]. Cette caractéristique est primordiale puisqu'elle fait du *smart contract* un contrat sûr. En effet, il est de nature à renforcer l'efficacité de la force contractuelle donnée à un engagement, ce qui dans la pratique peut se révéler être un avantage non négligeable. Selon certains auteurs, cette garantie spontanée ne l'est qu'en apparence, puisque sa mise en œuvre doit être rémunérée[365]. Mais il n'en demeure pas moins qu'en prévoyant une exécution automatique, il instaure un climat de confiance entre les parties avant même qu'elles n'aient conclu de contrat. Plus encore, la technologie est en mesure de rassurer les parties qui parfois débutent une relation commerciale ou d'affaires, et ont besoin de garanties que l'autre respectera ses engagements. Or, les *smart contracts* suggèrent qu'il n'est plus nécessaire d'avoir confiance en son cocontractant puisqu'il suffit de se fier à la technologie.

---

[362] LECOURT (Arnaud), « Droit des sociétés et numérique », *Répertoire IP/IT et Communication Dalloz*, v° Numérique et fonctionnement de la société, 2020, n° 39.
[363] L. n° 89-462, 6 juill. 1989, tendant à améliorer les rapports locatifs et portant modification de la L. n° 86-1290 du 23 décembre 1986, *JORF*, 8 juill. 1989, art. 15, modifiée par l'ord. n° 2019-770, 17 juill. 2019, relative à la partie législative du livre VIII du code de la construction et de l'habitation, *JORF* n°0171, 25 juill. 2019, texte n° 52, art. 13, 3°.
[364] BASHIR (Imran), *op. cit.*, *loc. cit.*
[365] MARIQUE (Enguerrand), « Les smart contracts en Belgique : une destruction utopique du besoin de confiance », *D. IP/IT* 2019, n° 1, p. 22.

30. Automaticité et économie de temps. Un *smart contract* peut effectivement automatiser toute action prédéfinie dans ses conditions, sans oublier qu'il est capable d'opérer en interaction avec l'environnement numérique entier. Nick Szabo constatait que la technologie, telle qu'il la concevait, présentait quelques similarités avec le distributeur à billet et d'autres machines automatiques en ce sens que, dès lors qu'une pièce est insérée, le service est délivré. Il faudra toutefois remarquer que les bénéfices que procurent les *smart contracts* tendent à être davantage diversifiés que ceux des machines automatiques car ils peuvent être utilisés pour tous types de biens, mais également pour des services plus complexes[366].

À l'instar de l'exécution automatique du pacte de préférence avec envoi immédiat des documents afférents[367], un *smart contract* pourrait, d'une manière générale, se charger de toute clause exigeant un transfert de documents, y compris s'il s'agit de faire parvenir des ordres ou des requêtes de production de pièces aux parties, ou même à des tiers (les administrations publiques, les entreprises contractantes, par exemple)[368], ou un transfert de fonds à échéance programmée, sans requérir une quelconque action des parties. L'automatisation de tâches réputées simples, éventuellement répétitives et souvent chronophages dans le contexte d'une entreprise, a toujours eu pour conséquence d'aider et de soulager l'Homme[369]. D'une part, elle permet aux professionnels de consacrer leur temps à d'autres impératifs, comme la relation client, pour un recentrage axé sur le relationnel[370]. D'autre part, elle vise, pour chaque individu, un accroissement du temps accordé à l'épanouissement personnel et aux loisirs[371].

L'automatisation des termes prédéfinis d'un contrat pourrait également permettre d'épargner aux parties le travail parfois fastidieux requis pour s'assurer du suivi des prescriptions, pour recouvrer une créance, ou au contraire leur permettre de ne plus manquer de faire parvenir un paiement à échéance. Accessoiriser un contrat de vente ou de prestation de service (C. consom., art. L. 221-1 et s.) en vertu de l'art. L. 221-3 du C. consom., y compris à la suite d'une négociation commerciale entre deux entreprises, permettrait d'automatiser les actions nécessaires à la conclusion définitive de celui-ci,

---

366 SZABO (Nick), « Formalizing and Securing Relationships on Public Networks », préc.
367 *Supra* n° 28.
368 BARBRY (Éric), art. cit., p. 78.
369 V. à ce sujet, NEVEJANS (Nathalie), *Traité de droit et d'éthique de la robotique civile*, *op. cit.*, pp. 64-68.
370 EL FIDHA (Chokri), HÉDI CHARKI (Mohamed), « Le rôle des technologies de l'information et de la communication dans le développement de la qualité de la "relation client". Application à la relation banque/entreprise », *La Revue des Sciences de Gestion* 2008/1 [en ligne], n° 229, pp. 121-127, v. notamment p. 127, https://www.cairn.info/revue-des-sciences-de-gestion-2008-1-page-121.html.
371 COLLIN (Denis), *La fin du travail et la mondialisation. Idéologie et réalité sociale*, éd. L'Harmattan, coll. « L'ouverture philosophique », 1997, p. 51.

notamment s'il prévoit un droit de rétractation de *x* jours – quatorze jours en vertu de l'art. 221-18 du C. consom. Informatiquement, il s'agirait de suspendre l'exécution du contrat tout au long de ce délai, en programmant une instruction conditionnelle laissant la possibilité pendant quatorze jours au consommateur de se rétracter *via* un formulaire prérempli au sens de l'art. L. 221-21 du C. consom., sinon en érigeant un système de formulaire de rétractation à remplir sur la plateforme dédiée, accessible uniquement durant la période prévue, et permettant de contracter un avenant mettant fin au premier *smart contract*. Réciproquement, dès lors que le délai expire sans que le consommateur n'ait exercé son droit de rétractation en informant le professionnel de sa décision, le *smart contract* prendrait automatiquement la décision d'exécuter le transfert du montant contractuellement fixé directement à la partie concernée et enverrait une notification aux parties. Le contrat auto-exécuté pourrait également permettre le commencement d'exécution après accord préalable manifeste du cocontractant à l'image du renoncement exprès du consommateur à son droit de rétractation pour un contrat de fourniture de services conclu à distance ou hors établissement (C. consom., art. L. 221-28, 1°). Par ailleurs, la *blockchain* est un gage de confiance en elle-même puisqu'elle permettrait de stocker et de transmettre la preuve tant de l'absence que de l'existence du recours au droit de rétractation par le consommateur (C. consom., art. L. 221-22), en plus de constituer une version informatisée et sécurisée du contrat. En définitive, aucune limitation ne semble pouvoir rendre impossible l'adaptation d'une condition contractuelle au sein de la *blockchain*. D'ailleurs, il serait même possible de compléter l'automaticité du *smart contract* par des systèmes « multi-signatures ». Créée par un utilisateur de la *blockchain Bitcoin Core*[372], cette fonctionnalité permet d'imposer l'accord de plusieurs utilisateurs avant d'initier une opération[373], ce qui permettrait de maintenir un « effet de groupe » dans des décisions le requérant, en particulier dans le cadre d'une entreprise.

Les exemples peuvent en ce sens être multipliés puisqu'un *smart contract* pourrait automatiser de la même manière le versement des *royalties* en propriété intellectuelle (CPI, art. L. 131-8, L. 214-1, L. 311-1 et s.), les dividendes d'actionnaires après le vote conditionnel de l'assemblée générale (C. com., art. L. 232-11 et s.), les *stock-options* et autres rémunérations d'un dirigeant sur le départ[374], et être utilisé dans d'autres domaines contractuels[375].

---

[372] Pour lire le post, v., https://diyhpl.us/wiki/transcripts/gmaxwell-bitcoin-selection-cryptography/.

[373] VERLETTE (Nicolas), « Bitcoin : Qu'est-ce qu'une adresse multi-signatures ? », *Achat-Bitcoins* [en ligne], 18 mai 2014, https://achat-bitcoins.com/bitcoin-definition-multi-signatures/.

[374] Offrant par ailleurs une nouvelle forme de transparence sur les politiques de rémunération des mandataires sociaux conformément aux art. L. 225-185, al. 4, et L. 225-37-3 du C. com.

[375] D'après le professeur Mustapha Mekki, « on peut également imaginer les apports d'un *smart contract* en droit des sûretés. La garantie à première demande justifiée pourrait être mise en œuvre automatiquement

D'ailleurs, les propositions du cabinet *Deloitte*, rédigées conjointement avec la *Chamber of Digital Commerce* newyorkaise (USA), et visant à formaliser le cadre « idéal » de formation d'un *smart contract*, témoignent dès 2016 de l'intérêt croissant des entreprises à considérer cette technologie à l'œuvre dans leurs locaux[376]. Selon eux, une structure en six points doit être observée afin de programmer un contrat auto-exécuté au sein d'une entreprise. Préalablement à la définition des termes du contrat, il est fondamental d'identifier les opportunités de coopération pour les parties, ainsi que les accords potentiels sur les transferts de droits et d'actifs, ce qui mène à identifier l'accord en lui-même (« 1 – *Agreement Identification* »). Cette étape réalisée, il s'agit donc de fixer des déclencheurs conditionnels basés sur des événements – les auteurs proposent, par exemple, la survenance de catastrophes naturelles, d'un évènement géolocalisé, ou du cours d'un indice boursier –, et/ou des déclencheurs conditionnels-temporels, tels que fondés sur une période de vacances scolaires ou sur des anniversaires étatiques ou religieux (« 2 – *Condition Setting* »), tout en veillant à utiliser un type de codage basé sur des conditions familières au monde des affaires (« 3 – *Business Logic Coding* »). Les trois dernières étapes concernent plus spécifiquement la sécurisation du *smart contract* et mobilisent les mécanismes propres de la technologie *blockchain*, à savoir la signature numérique fournissant une authentification sécurisée des parties au *smart contract* mais également la possibilité d'une vérification des messages échangés (« 4 – *Digital Signature* »), l'exécution du processus de vérification/validation/inscription sur la chaîne de blocs permettant l'immuabilité du contrat et le suivi de son exécution (« 5 – *Process Execution* »), et enfin, la mise à jour du réseau, renforçant sa sécurité (« 6 – *Updating Network* »).

31. Automaticité et économie d'argent. Dans un rôle incitatif, le *smart contract* devient finalement le contremaître des relations contractuelles, et l'assistant parfait des entreprises. Tandis que le monde des Hommes est ainsi libéré des contentieux et divers problèmes juridiques traditionnels, le monde des affaires l'est plus spécifiquement de la « paperasse »[377], des prescriptions dépassées et des retards de traitement enrayant la

dès lors qu'un document prédéterminé dans le programme est remis au garant. [...] aussi en matière de promesse unilatérale de vente d'immeuble » [MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., n° 25]. V. également, MAXIME (Julienne), « Le nantissement de titres financiers inscrits en blockchain », *in* MAGNIER (Véronique), BARBAN (Patrick) (dir.), *Blockchain et droit des sociétés*, éd. Dalloz, 2019, p. 54 ; ROBINE (David), PAILLER (Pauline), « Instruments financiers », *Le Lamy droit des sûretés - Expert*, v° Assiette du nantissement, n° 251-31.

[376] Chamber of Digital Commerce of NYC & Deloitte, « Smart Contracts: 12 Use Cases for Business & Beyond », [online], 6 Dec. 2016, p. 12, https://digitalchamber.org/policy-positions/smart-contracts/.

[377] GOSSA (Julien), art. cit., p. 393.

machine économique[378]. Finalement, il devient facile de contracter, mais aussi plus sûr, plus économique et plus profitable. La technologie augmente et fluidifie les relations contractuelles. Elle s'inscrit ainsi dans la lignée des évolutions numériques ayant donné naissance aux processus de CLM, *Contract Lifecycle Management* (gestion du cycle de vie des contrats), qui permettent aux entreprises d'accroître leur efficacité grâce à des solutions digitales de gestion de leurs contrats[379], tout en présentant « l'avantage de susciter la confiance sans que l'intervention d'un tiers soit requise »[380]. Se présentant comme un « *business maker* », le *smart contract* incarne l'un des aspects les plus prometteurs et innovants de la technologie *blockchain*[381]. C'est la raison pour laquelle l'enjeu est important pour les entreprises. IBM France prétend ainsi avoir réduit le temps de résolution des divers litiges-clients de quarante-quatre à dix jours depuis que la technologie *blockchain* a été implantée au sein de l'entreprise, leur permettant d'économiser plus de 31 000 dollars en 2015 et de débloquer pour de nouveaux investissements le capital de 100 000 dollars initialement prévu pour se garantir de ce type de contentieux[382].

32. Corolaire de l'exécution automatisée, la sanction automatisée tend à préserver chacun des cocontractants contre les risques d'inexécution.

---

[378] BARBRY (Éric), art. cit., p. 77.

[379] Selon DocuSign, « la gestion du cycle de vie des contrats est un processus de gestion et de stockage centralisé des contrats » [« DocuSign nommé un des leaders du Magic Quadrant 2020 de Gartner sur la gestion du cycle de vie des contrats », *DocuSign* [en ligne], 24 mars 2020, https://www.docusign.fr/blog/leader-mq-gartner-sur-la-gestion-du-cycle-de-vie-des-contrats], c'est-à-dire de « tout document juridique contenant des obligations qui affectent une organisation » [« *CLM solutions manage any legal documents containing obligations that affect an organization.* » [notre trad.], Report No. ID G00465728, « Magic Quadrant for Contract Life Cycle Management », Gartner [online], 25 Feb. 2020, https://www.docusign.fr/gartner-magic-quadrant-gestion-cycle-de-vie-des-contrats]. Il s'agit de mettre en place une solution permettant de « sécuriser, uniformiser, rationaliser et automatiser le lancement, la création, la négociation, la signature et l'exécution de contrats jusqu'à leur échéance », autrement dit une « solution [ou] un processus permettant de gérer le cycle de vie des contrats créés et/ou administrés par l'entreprise, ou ayant un impact sur celle-ci » [« CLM : Qu'est-ce qu'une solution de gestion du cycle de vie des contrats (Contract Lifecycle management) ? », *DocuSign* [en ligne], 21 mai 2019, https://www.docusign.fr/blog/clm-solution-gestion-cycle-de-vie-des-contrats]. D'après Gartner, les contrats concernés « peuvent inclure des contrats avec des tiers, tels que contrats de sous-traitance, d'approvisionnement, de vente, de non-divulgation, de propriété intellectuelle, de location, de gestion des infrastructures et toute autre licence ou tout accord contenant des obligations contractuelles aujourd'hui et à l'avenir » [*Id.*]. – V. également, SINGH (Nitish), « How Contract Management Solutions And Blockchain Work Together », *101 Blockchains* [online], 12 Feb. 2020, https://101blockchains.com/contract-management-solutions-and-blockchain/ ; CONTE (Craig), « Contract Lifecycle Management: Blockchain and Smart Contracts – Are You Missing Out? », *Capgemini* [online], 15 Sept. 2017, https://www.capgemini.com/2017/09/contract-lifecycle-management-blockchain-and-smart-contracts-are-you-missing-out/.

[380] POULLET (Yves), JACQUEMIN (Hervé), art. cit., p. 816.

[381] YERETZIAN (Antoine) (dir.), *La blockchain décryptée : les clefs d'une révolution*, éd. Netexplo, 15 juin 2016, p. 78.

[382] *Ibid.*, p. 113.

33. Programmation d'un moyen de dissuasion : la sanction contractuelle. Le *smart contract* ambitionne de mettre fin aux ruptures anticipées, contestations, mauvaise foi, manquements, retards, et autres prétextes à l'inexécution par le biais d'un système de pressions contractuelles, dissuasives ou persuasives, infalsifiable et traçable. D'aspect, il peut sembler rendre obsolète les dispositions du Code civil, mais il s'avère qu'au contraire, sur certains points et notamment en ce qui concerne la force du contrat, il témoigne d'une volonté d'en optimiser l'application[383]. L'objectif est de réussir à introduire les subtilités du langage juridique dans le langage informatique. Cette action devait d'ailleurs, selon Nick Szabo, être obligatoirement une pénalité financière ayant un rôle dissuasif et ce, tant pour renforcer la qualité d'auto-exécution que pour endiguer les risques d'inexécution[384]. Au-delà de la seule annulation de l'accord par la *blockchain*, il convient de mettre en place une véritable sanction. Celle-ci peut prendre différentes formes et découler de différentes procédures. Deux configurations seront examinées, selon, d'une part, que la dissuasion découle d'une clause spécifique de résolution avec réparation ou, d'autre part, qu'elle émane de l'intégration, originelle ou spéciale, des règles de droit en la matière.

34. Anticipation au cas par cas : l'utilisation de la clause résolutoire. Tout d'abord, afin d'éviter l'aléa que peut parfois représenter une action judiciaire, il est courant que les parties prévoient une clause résolutoire en application de l'art. 1224 du C. civ. Elles pourraient, de la même manière, anticiper les risques d'inexécution dans le contexte d'un *smart contract*. Pour cela, elles programmeraient une liste expresse d'engagements en vertu de l'art. 1225 du C. civ.[385], dont l'inexécution conduirait systématiquement à une rupture de plein droit de la relation contractuelle inscrite sur la chaîne (C. civ., art. 1225, al. 1er), avec allocation immédiate de dommages et intérêts dont le montant serait prédéfini (C. civ., art. 1231 à 1231-5). Si cette liste n'est soumise à aucune condition de gravité (C. civ., art. 1224), les parties doivent veiller cependant à ce

[383] MEKKI (Mustapha), « Blockchain : l'exemple des smart contracts », *blog mekki.fr* [en ligne], 25 mai 2018, p. 8, http://www.mekki.fr/files/sites/37/2018/05/Smart-contracts.pdf.
[384] SZABO (Nick), « Formalizing and Securing Relationships on Public Networks », préc.
[385] Toutefois, le professeur Alain Benabent précise qu' « elle ne peut […] pas jouer pour des fautes qui résultent du droit commun mais non des mentions au contrat – alors même que les manquements sont incontestables. » [BENABENT (Alain), *Droit des obligations*, éd. LGDJ, 18e édition, coll. Précis Domat, Privé, 2019, p. 307].

qu'elle soit exprimée dans des termes dénués d'équivoque[386], en particulier s'agissant d'une exécution automatique effectuée par un algorithme.

En poursuivant la relation algorithmique « *IF – THEN* », dès l'instant où un manquement serait constaté par le *smart contract*, celui-ci enverrait à la partie défaillante, selon les termes du contrat, soit une mise en demeure préalable (C. civ., art. 1225, al. 2) indiquant précisément les manquements reprochés[387], ainsi que le délai pour s'y conformer[388], soit un avertissement préalable[389]. Dans l'hypothèse où le contractant défaillant ne se serait pas exécuté après la mise en demeure, le *smart contract* ferait produire effet au jeu de la clause en vertu des art. 1229 et 1230 du C. civ.[390]. Il peut d'ailleurs être programmé pour effectuer automatiquement l'exécution de potentielles restitutions et réparations. Dans la mesure où la situation ne lui permettrait pas d'agir directement, par exemple si la restitution matérielle d'un objet est requise, il lui appartiendrait simplement d'en superviser l'exécution.

35. Algorithmes d'exécution du droit : l'intégration originelle ou spéciale des règles de droit. En parallèle, il semble que les parties pourraient manipuler des *smart contracts* mettant naturellement en œuvre le droit des contrats. Dans cette hypothèse, il s'agirait d'une application, voire d'une *blockchain*, spécialement dédiée aux relations contractuelles. Le développeur pourrait avoir intégré, dès sa conception, l'éventail de sanctions offert par le droit des contrats – autrement dit le dispositif de l'art. 1217 du C. civ. Une telle configuration permettrait aux parties de bénéficier de la protection du droit au cours de l'exécution de leur contrat, sans l'avoir préalablement et personnellement anticipé. Inversement, il pourrait également s'agir d'un *smart contract* programmé expressément par les parties pour prévoir l'intégralité des diverses réponses juridiques de l'art. 1217. Quelle que soit l'origine de sa programmation, le *smart contract* mettrait en œuvre l'ensemble des règles de droit, en commençant par les défaillances résultant d'un cas de force majeure de l'art. 1218 du C. civ.[391]. Un auteur suggère d'ailleurs d'inclure dans des clauses de force majeure les risques d' « indisponibilité du réseau, d'une

[386] Cass. Civ. 1ère, 25 nov. 1986, *Bull. civ.*, I, n° 279. – Cass. Civ. 3e, 7 déc. 1988, *Bull. civ*., III, n° 176. – Cass. Civ. 3e, 8 juin 2006, *Bull. civ.*, n° 143.
[387] Cass. Com., 17 févr. 2015, n° 13.27-117.
[388] Cass. Civ. 3e, 28 nov. 1968, *Bull. civ.*, III, n° 468.
[389] L'art. 1225 du C. civ. n'érige pas la mise en demeure préalable au rang d'obligation d'ordre public. Les parties peuvent donc y déroger en prévoyant un avertissement préalable, ou en ne prévoyant rien.
[390] À savoir, fixation de la date d'extinction du contrat qui dans le cas d'une clause résolutoire est la date indiquée par celle-ci (C. civ., art. 1229), et maintien des clauses relatives à la fin du contrat (C. civ., art. 1230).
[391] C. civ., art. 1218 : « Il y a force majeure [...] lorsqu'un événement échappant au contrôle du débiteur, qui ne pouvait être raisonnablement prévu lors de la conclusion du contrat et dont les effets ne peuvent être évités par des mesures appropriées, empêche l'exécution de son obligation par le débiteur. »

cyberattaque, d'une corruption de données lors de l'hébergement ou lors du transport de ces données […] »[392]. Si le débiteur ne démontre pas l'existence d'un tel fait dans un délai prédéfini, alors la *blockchain* confirmerait l'existence d'un manquement et appliquerait la sanction prévue. Difficile mais pas impossible[393], il s'agirait, avant l'envoi de la mise en demeure, de proposer un choix de sanctions prédéfinies aux parties, le *smart contract* se chargeant de l'exécution de la sanction et, au surplus, de la preuve des circonstances de celle-ci. En pratique, c'est au créancier insatisfait qu'appartient cette décision[394]. Seulement, à l'instar du débiteur dont la responsabilité est engagée pour avoir fait obstacle à l'exécution du *smart contract*, le créancier devra décider de la sanction tout en ayant lui aussi conscience de la traçabilité permise par la technologie utilisée. Ainsi, le créancier est incité à s'abstenir de toute décision arbitraire, et à préférer l'honnêteté, au risque d'engager sa propre responsabilité. D'autant plus que la *blockchain*, réputée neutre et immuable, confirmerait sans peine l'existence de sa faute. Concrètement, le créancier pourrait donc, à ses risques et périls, poursuivre l'exécution forcée (C. civ., art. 1221 et 1222) ou solliciter une réduction du prix (C. civ., art. 1223). Celle-ci peut d'ailleurs être déterminée dès la conception du *smart contract* sous la forme d'un pourcentage dégressif mais proportionnel de la somme due[395], et/ou soumis à acceptation du montant, et non du principe de la réduction, par le créancier, et/ou encore remis à expertise. De la même manière, il pourrait encore opter pour une exception d'inexécution, par exemple, s'il considère le manquement contractuel de son cocontractant suffisamment grave (C. civ., art. 1219). Dans l'intérêt des parties, il pourrait être intéressant d'inscrire préalablement dans l'algorithme les inexécutions considérées comme étant « suffisamment graves » pour justifier l'inexécution de la contre-prestation. Par exemple, si l'assuré n'honore pas le paiement d'une prime dans le temps imparti (en général dans les dix jours de son échéance), après mise en demeure préalable, la garantie sera alors automatiquement suspendue dans les trente jours (C. ass., art. L. 113-3). Dans le même sens, si l'acheteur ne paye pas le prix du produit acheté, alors le vendeur n'aura pas l'autorisation de l'expédier (C. civ., art. 1612). Éventuellement, le système de fourniture de bordereaux d'expédition pourrait même être automatisé en vertu d'un ou plusieurs autres *smart contracts* génériques, appelés par le premier à s'exécuter en parallèle, rendant alors matériellement impossible l'expédition en cas de défaut de paiement.

[392] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., *loc. cit.*
[393] En principe toute règle en soi peut être exprimée sous le langage « IF – THEN », SI – ALORS.
[394] BENABENT (Alain), *op. cit.*, p. 291.
[395] Attention toutefois, cette solution pourrait être assimilée à une clause pénale soumise au contrôle du juge.

Force est de constater que le *smart contract* tend à optimiser la loi des parties contractantes[396]. Mais il n'en demeure pas moins que, même si les algorithmes permettent de réguler l'exécution du contrat, le droit continue d'encadrer les modalités de cette régulation.

36. Vers de nouvelles formes d'incitation au respect de la parole donnée. Certains auteurs invitent le législateur à mettre en œuvre de nouvelles formes de sanctions, telle qu'une sanction générale d'indemnisation du préjudice subi dès lors que l'exécution découle de clauses nulles ou réputées non-écrites[397], ou bien encore la possibilité, selon les circonstances, de programmer une sanction temporaire dont l'objet serait d'interdire l'accès à la *blockchain* et *a fortiori* à l'utilisation des *smart contracts*[398]. Il a également été proposé de mettre en place un système de réputation contractuelle, publié et visible par tout un chacun sur la chaîne[399], sous la forme, par exemple, d'une notation par les pairs, anciens cocontractants. Comme le constate Simon De Charentenay, « le bilan coût/avantage incite au respect »[400].

37. Diminution conjointe des risques de contentieux. Sous la menace du déclenchement de la sanction, le débiteur est incité à honorer ses engagements[401]. Ainsi, le *smart contract* insuffle l'espoir d'un contrat plus efficace ou, à tout le moins, d'une adhésion spontanée du défaillant au litige en raison du sentiment d'objectivité émanant de la technologie. La remarque de Alain Bénabent concernant le nouveau dispositif de sanction de l'inexécution contractuelle de la loi n° 2018-287 du 20 avril 2018[402] selon laquelle « le juge est donc privé de son pouvoir d'appréciation »[403] n'a sans doute jamais fait autant sens qu'en s'appliquant à l'auto-exécution du *smart contract*[404]. C'est une des raisons pour laquelle certains auteurs examinent cette loi comme la première étape de

[396] Concernant la notion de « loi des parties », v., AYNES (Laurent), « Le contrat, loi des parties », *Cahiers du conseil constitutionnel* [en ligne], n° 17 (dossier : loi et contrat), mars 2005, https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/le-contrat-loi-des-parties.
[397] BARREAU (Catherine), art. cit., pp. 74-76.
[398] DE CHARENTENAY (Simon), « Blockchain et Droit : Code is deeply Law », *Blockchain France* [en ligne], 19 septembre 2017, https://blockchainfrance.net/2017/09/19/blockchain-et-droit/.
[399] *Id.*
[400] *Id.*
[401] GODEFROY (Lêmy), « Le code algorithmique au service du droit », art. cit., p. 734.
[402] L. n° 2018-287, 20 avr. 2018, ratifiant l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, *JORF* n° 0093, 21 avr. 2018, texte n° 1.
[403] BENABENT (Alain), *op. cit.*, p. 306.
[404] D'autant plus s'il est précisé qu'il ne peut en outre que constater la résolution et ce, quand bien même il s'agirait d'un manquement d'une extrême légèreté. V. en ce sens, Cass. Civ. 3e, 11 juill. 1977, *Bull. civ.*, III, n° 106.

réformes plus ambitieuses[405]. En effet, en programmant des contrats pour qu'ils déclenchent une réaction lorsqu'une des conditions du code informatique est remplie, il ne serait, en principe, plus indispensable pour une partie de faire constater, par exemple, la défaillance de son cocontractant, puisque ce serait le contrat lui-même qui certifierait ladite défaillance et exécuterait immédiatement l'action prédéfinie correspondante.

Pour autant, l'action en justice n'est en principe pas totalement exclue, puisque le droit d'ester en justice reste un droit fondamental (CPC, art. 31 ; C. consom., art. L. 132-1) et la figure du juge « demeure l'émanation du tiers étatique de confiance »[406]. Seulement, son intervention en ce qui concerne les contentieux d'inexécution se verra profondément diminuée par l'action des *smart contracts*.

Les progrès en matière de programmation des contrats auto-exécutés confirmeront ou démentiront que « le recours au juge ne constitue plus la garantie ultime des accords contractuels »[407]. Mais il n'en demeure pas moins que, en l'état actuel, la technologie a pour effet de troubler les pratiques juridiques traditionnelles en érigeant ce qui semble être un nouveau mode de confiance algorithmique.

Section 2. Vers de nouveaux rapports de confiance

38. Tel qu'il a été mentionné précédemment, *Ethereum* tient une place importante dans le déploiement des *smart contracts via* les *dApps*, applications décentralisées et à vocation universelle[408]. Il est d'ailleurs possible de comparer le système d'exploitation implanté dans les smartphones au code source utilisé par *Ethereum*. Pour autant, elle n'est pas fondée à demeurer la seule. D'autres protocoles spécialisés se développent, notamment *TRON*[409] et ceux de la fondation *Linux*, « *Composer* » *via HyperLedger*[410], et de *Ripple Labs*, « *Codius* »[411], actuellement accessible en version bêta. Les projets mettant en œuvre des *smart contracts* sont trop nombreux pour pouvoir en faire un exposé complet. Il convient alors de retenir que, d'une part, la *blockchain* est capable de donner à la confiance une dimension nouvelle et, d'autre part, moyennant une grande diversité

[405] *Supra* n° 26.
[406] GUERLIN (Gaëtan), art. cit., *loc. cit*.
[407] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 13.
[408] *Supra* n° 8.
[409] Pour plus d'informations sur *TRON* du *TRON development hub*, v. notamment, « Qu'est-ce que TRON - Une monnaie virtuelle ou bienplus ? », *Coin24* [en ligne], 2017, https://coin24.fr/tron/ ; « Java implementation of the Tron whitepaper », *GitHub* [online], 2017, https://github.com/tronprotocol/java-tron#readme.
[410] WEE (David), CHUEN (Kuo), DENG (Robert H.), *op. cit.*, p. 161.
[411] Pour plus de précisions, v. respectivement, https://getcomposer.org/ ; https://codius.org/.

d'approches, elle tend à occuper les aspects les plus courants de la vie. Or, ces caractéristiques, les *smart contracts* les mettent au service de l'effectivité des engagements contractuels à travers des applications aussi nombreuses que diversifiées (§ 1), et notamment dans le domaine assurantiel où de nombreux changements sont en perspective (§ 2).

§ 1. Les diverses applications des *smart contracts* : optimisation des engagements

39. Dans l'objectif d'une optimisation généralisée des relations entre les Hommes, un nombre important de *dApps* ont vu le jour dans divers domaines de la vie courante. Alors que la plupart des utilisations qui en sont faites n'intégraient pas nécessairement le champ habituellement réservé aux relations conventionnelles (A), les autres ont finalement permis de faire évoluer nombre de domaines contractuels traditionnels, en les rendant davantage accessibles (B).

A. De nouveaux domaines de relations conventionnelles

40. Un marché décentralisé et P2P de la puissance de calcul. C'est ainsi qu'a été mise en œuvre, par exemple, *Golem*, une application qui propose à ses utilisateurs, nommés « *providers* » (fournisseurs), de mettre la puissance de calcul inutilisée d'un ordinateur, d'un smartphone ou encore d'un centre de données[412] en commun au sein d'un supercalculateur *open source* et décentralisé[413]. *Golem* repose en effet sur un réseau P2P, rattaché au système de transaction d'*Ethereum*, ce qui lui permet de créer un marché locatif géré en autonomie par les utilisateurs. Moyennant un prix pour la location, un *requestor* (demandeur) peut donc louer à un ou plusieurs *providers* des capacités de calcul[414], qui sont directement mises à disposition sur le réseau, lequel procède au calcul des tâches soumises par le *requestor*[415]. Les programmes informatiques d'animation et d'images de synthèse, par exemple, requièrent d'importantes puissances de calcul. Un apport supplémentaire de puissance de calcul pourrait présenter un intérêt pour les professionnels du milieu artistique qui seraient en mesure de sous-traiter afin de générer plus rapidement des images, des séquences, des animations 3D, des effets spéciaux

[412] V. le site officiel de l'application, https://golem.network/.
[413] « The Golem Project. Crowdfunding Whitepaper », Golem [online], Nov. 2016, p. 3, https://golem.network/crowdfunding/Golemwhitepaper.pdf.
[414] *Id.*
[415] *Ibid*., pp. 4-5.

cinématographiques, etc. Par ailleurs, et à la différence des *Cloud Computing*, le système décentralisé et distribué de partage de la puissance de calcul créé par *Golem* fournit également aux développeurs des outils flexibles et efficaces pour déployer, distribuer et monétiser, directement *via* le réseau, leurs logiciels propriétaires et *open source*, ainsi que leurs *dApps*[416].

41. Des *smart contracts* œuvrant pour le développement durable. Poursuivant la dynamique citoyenne et incitative pour le développement durable et l'intégrité environnementale, en lien avec l'art. 2, § 1, c), de l'Accord de Paris de 2015[417], la banque en ligne Compte CO2 propose à ses clients de mesurer et de réduire leur empreinte carbone lors de leurs divers achats en utilisant une monnaie dédiée, l' « €O2 »[418]. Elle met à leur disposition une carte de paiement, la « carte CO2 », qui produit des réductions d'émissions de CO2 de l'ordre d'un kilo de CO2 pour un €O2 dépensé[419]. En parallèle, l'application propose un bilan carbone personnalisé. Fondée sur une méthodologie de calcul découlant du protocole de Kyōto[420] mise à exécution automatiquement par la *blockchain*, elle calcule, à partir des justificatifs fournis, les émissions du logement et du véhicule du client afin d'établir un seuil d'émissions de référence[421]. À partir de cette dernière, toutes les réductions d'émissions opérées par l'intermédiaire d'achats responsables ou « achats verts » sont immédiatement reversées sous la forme d'€O2. Par exemple, l'achat d'un véhicule électrique permet d'obtenir, environ, deux mille €O2[422]. Des applications basées sur le même principe permettent d'obtenir une récompense sous forme de jetons cryptographiques, échangeables contre des denrées alimentaires lorsque des déchets recyclables, tels que des contenants, canettes ou bouteilles en plastique, ont été collectés dans les mers et océans (*Plastic Bank*)[423], ou sont retournés après utilisation (*RecycleToCoin*)[424], et déposés dans des bornes automatiques installées en Europe et dans le monde.

---

[416] *Ibid.*, p. 6.
[417] Accord Nations Unies Paris, déc. n° 1/CP.21, 12 déc. 2015. – Ratifié par l'UE et entré en vigueur le 4 novembre 2016.
[418] V. le site officiel du projet, https://www.compteco2.com/bilan-co2/.
[419] *Ibid.*, Produit > Carte CO2.
[420] Prot. Nations Unies Kyōto, 11 déc. 1997, à la Convention-cadre des Nations Unies sur les changements climatique, art. 3, § 7.
[421] V., https://www.compteco2.com/bilan-co2/, Produit > Bilan carbone.
[422] *Id.*
[423] KATZ (David), « Plastic Bank : la révolution Social Plastic », *in* « Réinventer l'avenir des plastiques », *La revue de l'Institut Veolia* [en ligne], 2019, pp. 96-99, https://www.institut.veolia.org/fr/plastic-bank-la-revolution-social-plastic. V. également, https://plasticbank.com/.
[424] V., https://steemit.com/crypto/@abraomarcos/bcdc-online-recycle-to-coin.

Démarche également ouverte aux entreprises, il s'agit, à leur niveau, d'optimiser leurs stratégies sociales et, en particulier, environnementales, pour lesquelles elles assument désormais la responsabilité. Initialement axé sur l'engagement volontaire, le droit de la responsabilité sociale et environnementale des entreprises (RSE) a effectivement fait l'objet ces dernières années d'un durcissement, laissant apparaître une tendance à la contractualisation du droit[425]. En s'appuyant sur ce phénomène, les *smart contracts* sont capables d'apporter d'une manière générale aux engagements de toute entreprise (C. civ., art. 1833, al. 2) et, plus particulièrement, aux plans de vigilance imposés à certaines d'entre-elles (C. com., art. L. 225-102-4), un appui non négligeable en ce qui concerne l'identification et la prévention des risques et atteintes graves à l'environnement. Ils représentent en cela des outils à fort potentiel pour diffuser le développement durable dans la chaîne de valeur. C'est sur ce constat qu'Affectio Mutandi et EcoVadis ont décidé d'inclure, dans leurs politiques, des pratiques de contractualisation des enjeux Environnementaux, Sociaux et de Gouvernance (ESG)[426]. Ils envisagent de les traduire en code informatique afin de bénéficier des qualités de la *blockchain* et notamment des *smart contracts*, et ainsi assurer à leurs clients une amélioration des performances et des actions poursuivies en matière de développement durable. En plus de garantir la traçabilité et l'immuabilité des engagements inscrits, la *blockchain* permet indirectement de prouver la fiabilité de leurs clients, tant dans leurs relations *business-to-business* (B2B) que *business-to-consumer* (B2C)[427]. Le *smart contract* est d'autant plus efficace qu'il renforce le contrôle des actions de chaque contractant, tout en laissant la possibilité de prévoir des sanctions automatiques, s'exécutant en principe trois mois après mise en demeure (C. com., art. L. 225-102-4, II). Icertis a ainsi développé, *via* le service *Azure Blockchain*, *Icertis Blockchain Framework*, une application contractuelle à disposition des entreprises qui leur permet d'initier des *smart contracts* pour encadrer leurs relations commerciales avec les fournisseurs et leurs chaînes d'approvisionnement, y compris pour maintenir la conformité avec les programmes sociaux et environnementaux[428]. Selon Mustapha Mekki, si le contrat et la

[425] MEKKI (Mustapha), « L'intelligence contractuelle et numérique au service de la responsabilité sociétale des entreprises », *Actualité juridique. Contrat*, Dalloz, 12 mars 2020, n° 3, pp. 112 et s.

[426] « Le contrat et les clauses RSE, leviers incontournables de vigilance. Étude croisée 2018 acheteurs-fournisseurs sur les clauses contractuelles RSE », Affectio Mutandi et EcoVadis [en ligne], avr. 2018, http://affectiomutandi.com/wp-content/uploads/2018/05/2018_contrat_et_clauses_RSE_ecovadis_affectio_mutandi.pdf.

[427] Le professeur Mustapha Mekki constate en effet que les activités et actions des entreprises en matière de protection de l'environnement intéressent de manière croissante les consommateurs, érigés en « consomm'acteurs », contribuant à faire des objectifs RSE les principaux indicateurs de la bonne ou mauvaise réputation d'une entreprise [MEKKI (Mustapha), « L'intelligence contractuelle et numérique au service de la responsabilité sociétale des entreprises », art. cit.].

[428] Pour plus de précisions, v., https://www.icertis.com, Accueil > The Platform ; Accueil > Ressources.

technologie constituent les deux outils à la fois essentiels et complémentaires à la sécurité juridique des entreprises et au respect des objectifs RSE, la jonction de l'automatisation des *smart contracts* au pouvoir de contrainte de la contractualisation, enrichie de l'éventail de sanctions offert par le droit des contrats et les clauses contractuelles correspondantes[429], ne peut qu'en optimiser l'efficacité[430]. Plus encore, en contribuant ainsi à l'internormativité opérée par l'instrument contractuel[431], il optimise l'effectivité des politiques menées en droit de l'environnement[432], passant progressivement d'un système basé sur l'engagement moral et volontaire à un système de régulation astreignant à la vigilance[433]. Dans le cadre de l'al. 3 de l'art. 1833 du C. civ., une autre application des *smart contracts* pourrait se révéler intéressante en ce qu'elle permettrait d'automatiser les statuts d'une société, et ainsi éventuellement de contrôler le respect de la « raison d'être » de l'entreprise. Il s'agit des Decentralized Autonomous Applications (DAO).

42. Des *smart contracts* pour créer une entreprise sans gérant ? Les *Decentralized Autonomous Applications* (DAO). Découlant directement de la technologie des *smart contracts*, les organisations autonomes décentralisées – ou distribuées – (DAO) ambitionnent de remplacer les plateformes existantes, voire de proposer une alternative à la personnalité morale, et de créer ainsi une nouvelle forme de relation sociale et économique. Il s'agit pour nombre d'auteurs de la finalité de la *blockchain*[434]. La DAO fournit des règles de gouvernance transparentes et immuables à une communauté sans

---

[429] Concernant les bénéfices du contrat auto-exécuté *via blockchain*, *supra* n° 27 et s.

[430] On peut penser, par exemple, que l'inscription par Total de son plan sur une *blockchain*, voire l'utilisation d'un *smart contract*, aurait pu lui éviter des poursuites judiciaires pour « inaction climatique » [DE SÈZE (Cécile), « Total assigné en justice : les entreprises face à leurs responsabilités climatiques », *L'Express* [en ligne], 29 janv. 2020, https://www.lexpress.fr/actualite/societe/justice/total-assigne-en-justice-les-entreprises-face-a-leurs-responsabilites-climatiques_2116624.html].

[431] L'internormativité est définie comme étant un concept constituant « une idée de ce que la normativité peut connaître de sources hybrides en restituant le droit dans sa signification sociologique première » [NOREAU (Pierre), « Belley Jean-Guy (dir.), Le droit soluble. Contributions québécoises à l'étude de l'internormativité, coll. Droit et Société, 1996 [compte-rendu] », *in* GUIBENTIF (Pierre), NIKLAS (Luhmann), « Dossier : L'emploi, l'entreprise : nouvelles normes, nouvelles règles », *Droit et société*, n°41, 1999, pp. 171-172]. Un autre auteur souligne que « Jean Carbonnier entendait désigner par-là "les rapports qui se nouent et se dénouent" entre les différents systèmes normatifs : le droit était ainsi envisagé à travers la relation qu'il entretient avec les autres dispositifs d'encadrement et de normalisation des comportements existant dans la société » [CHEVALIER (Jacques), « L'internormativité », *HAL* [en ligne], 2013, p. 1, hal-01723912]. – V. également, BELLEY (Jean-Guy), « Le contrat comme phénomène d'internormativité », *in* BELLEY (Jean-Guy) (dir.), *Le droit soluble. Contributions québécoises à l'étude de l'internormativité*, LGDJ, 1996, p. 195 ; CARBONNIER (Jean), « Les phénomènes d'inter-normativité », *in European Yearbook in Law and Sociology*, 1977, pp. 42-52.

[432] V., MEKKI (Mustapha), « L'intelligence contractuelle et numérique au service de la responsabilité sociétale des entreprises », art. cit. L'auteur conseille en ce sens de consulter la réglementation des sites pollués, v., MEKKI (Mustapha), « La gestion conventionnelle des risques liés aux sols et sites pollués », *JCP N* 2014, n° 27, p. 1239.

[433] VAN WAEYENBERGE (Arnaud), COLOMBANI (Lorenzo), « Responsabilité sociale des entreprises. Enjeux globaux et technologiques », *Revue française de gestion* 2017/8, n° 269, p. 166.

[434] LEGEAIS (Dominique), *op. cit.*, n°s 60-61.

qu'aucune personne ou organisation ne la contrôle. En d'autres termes, la DAO n'a pas de personnalité juridique, ni de représentant physique, et utilise des fournisseurs *e-services* pour avoir un impact dans le monde réel[435]. Le processus de décision est par conséquent entièrement transparent et neutre. Cette organisation fonctionne en réseau horizontal – contrairement à un modèle d'organisation classique reposant sur une logique verticale[436]. Elle est constituée d'une part, de détenteurs de *tokens*, pouvant être assimilés à des actionnaires auxquels peuvent être rattachés des droits de vote et des pourcentages sur les bénéfices et, d'autre part, d'un ou plusieurs prestataires qui soumettent des projets à financer. Parmi ces parties à la DAO existe un autre protagoniste, nommé « curateur », dont le rôle est non seulement celui d'un contrôleur décentralisé, mais également d'un filtre désintéressé. Sa mission est de vérifier que le projet du prestataire, publié sous la forme d'un *smart contract*, correspond au code source déployé. Si les curateurs s'aperçoivent que les codes sont corrompus, ils peuvent alors décider de les écarter[437]. Un premier exemple d'une telle organisation est « *The DAO* » par l'entreprise slock.it sur la *blockchain Ethereum*, dont l'objectif était de créer une société de financement pouvant décider elle-même de l'utilisation de ses fonds[438]. La DAO qui, d'après certains auteurs a des similitudes avec une fiducie dématérialisée[439], pourrait tout aussi bien, selon le protocole utilisé, se rapprocher de la société créée de fait ou de la société en participation. D'une certaine manière, les DAO poussent à son paroxysme l'idée de désintermédier les intermédiaires de confiance et confirment la capacité des technologies émergentes à coordonner différentes parties à un contrat de société et, *a fortiori*, à tout acte juridique nécessaire tout au long de la vie d'une société, sans avoir besoin de recourir à une instance régulatrice centralisée[440].

Finalement, comme le constate un auteur, « demain, c'est l'ensemble des marchés qui pourrait être dématérialisé au sein d'une *blockchain* »[441], à l'image de la « démocratie liquide » qu'envisageait Vitalik Buterin[442].

---

[435] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., n° 9.
[436] LEGEAIS (Dominique), *op. cit.*, *loc. cit.*
[437] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., *loc. cit.*
[438] POLROT (Simon), « Déploiement de The DAO, "mère de toutes les DAO" », *Ethereum France* [en ligne], 30 avr. 2016, https://www.ethereum-france.com/deploiement-du-projet-the-dao-mere-de-toutes-les-dao/. – The DAO fera l'objet d'une étude détaillée en seconde partie, *infra* n°s 270 et s.
[439] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., *loc. cit.*
[440] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 19.
[441] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., *loc. cit.*
[442] BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », préc.

43. Des applications multiples. Force est de constater que les cas d'usage semblent infinis ou, du moins, ne paraissent cantonnés qu'aux limites des facultés de création de l'Homme, et d'évaluation de la machine. Le déploiement de la technologie ouvre donc le champ d'investigation juridique à de nombreux secteurs d'activité, mais il permet également de faire évoluer les relations contractuelles traditionnellement établies dans des secteurs comme l'immobilier, les assurances, les banques, la santé, l'industrie pharmaceutique, les systèmes de *supply chain* de nombreuses filières (agroalimentaire, diamantaire, automobile, et plus largement de la distribution et du commerce international), l'industrie musicale et culturelle, l'art, la création de sociétés, les administrations publiques[443], etc. Tandis que certains espèrent prochainement faire exécuter des héritages *via smart contracts*[444] ou même remplacer la plateforme de location saisonnière Airbnb[445], d'autres se marient en inscrivant leur contrat de mariage au sein d'un *smart contract* et en déclarant « *Yes, I do* » sur la plateforme *ConsenSys*[446]. D'autres encore perçoivent dans les caractéristiques propres des *smart contracts* un moyen de solutionner diverses difficultés rencontrées dans la pratique contractuelle de certaines activités.

44. Le *smart contract*, un acteur dans la lutte pour la diminution des émissions de carbone ? Les projets de sécurisation et de fluidification des marchés du carbone. Initialement permis par la directive 2003/87/CE du Parlement européen et du Conseil[447],

[443] V. notamment, MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., n° 3 : « À titre d'exemple il est possible d'imaginer la situation d'un ressortissant étranger qui souhaiterait renouveler sa carte de séjour en France. Il devra se procurer toute une série de documents auprès de différents organismes puis les communiquer à l'agent administratif compétent. […] Grâce à la technologie des *blockchains*, censée offrir une sécurité absolue, les documents ne transiteront plus par le demandeur et le document manquant pourra être fourni plus rapidement, sans avoir besoin de fixer un nouveau rendez-vous, et à moindre coût. »

[444] GEIBEN (Didier), JEAN-MARIE (Olivier), VERBIEST (Thibault) *et al.*, *Bitcoin et Blockchain : Vers un nouveau paradigme de la confiance numérique ?*, éd. RB, coll. Les essentiels de la banque et de la finance, 2016, p. 52-53.

[445] Il s'agit de la plateforme *Beenest* [https://www.nest.beetoken.com/], réseau de locations saisonnières accessibles *via Bee Token*. – Pour plus de précisions, v., DEROME (Emma), « Location, achat : quand la blockchain réinvente l'immobilier », *WE Demain* [en ligne], 29 juin 2018, https://www.wedemain.fr/Location-achat-quand-la-blockchain-reinvente-l-immobilier_a3416.html.

[446] WOODS (Tyler), « This couple got married on the blockchain », *Technically Brooklyn* [online], 11 Nov. 2015, https://technical.ly/brooklyn/2015/11/11/couple-got-married-blockchain/.

[447] Dir. (CE) n° 2003/87 du Parlement européen et du Conseil, 13 oct. 2003, établissant un système d'échange de quotas d'émission de gaz à effet de serre dans la Communauté et modifiant la directive 96/61/CE du Conseil (Texte présentant de l'intérêt pour l'EEE), *JOUE* n° L 275 du 25 oct. 2003, pp. 32-46, telle que modifiée par (1) Dir. (CE) n° 2004/101 du Parlement européen et du Conseil, 27 oct. 2004, modifiant la directive 2003/87/CE établissant un système d'échange de quotas d'émission de gaz à effet de serre dans la Communauté, au titre des mécanismes de projet du protocole de Kyoto, *JOUE* n° L 338 du 13 nov. 2004, pp. 18-23, (2) Dir. (CE) n° 2008/101 du Parlement européen et du Conseil, 19 nov. 2008, modifiant la directive 2003/87/CE afin d'intégrer les activités aériennes dans le système communautaire

notamment ses paragraphes 1 et 1 bis de l'art. 25, transposés en droit français à l'art. L. 229-7, II, du C. envir.[448], ainsi que par l'art. 17 du protocole de Kyōto de 1997[449] ratifié en 2005[450] et transposé en droit français à l'art. L. 229-22 du C. envir., l'échange de crédit carbone connaît, depuis, nombre de difficultés portant atteinte à son effectivité, voire à son intégrité.

Certains auteurs regrettent l'absence d'harmonisation des systèmes d'échange de quotas à l'échelle mondiale, notamment en ce qui concerne le prix du carbone[451]. Elle permettrait, d'une part, d'éviter la fragmentation tant des pratiques que des critères d'obtention de quotas lors de la réalisation des projets volontaires de compensation et, d'autre part, le cloisonnement des différents marchés créant, à terme, des déséquilibres entre l'offre et la demande[452]. Par ailleurs, le manque de transparence et de sécurité des pratiques disparates actuelles ont conduit certaines entreprises à polluer davantage afin

d'échange de quotas d'émission de gaz à effet de serre, *JOUE* n° L 8 du 13 janv. 2009, p. 3, (3) Règl. (CE) n° 19/2009 du Parlement européen et du Conseil, 11 mars 2009, portant adaptation à la décision 1999/468/CE du Conseil, *JOUE* n° L 87 du 31 mars 2009, p. 109, et (4) Dir. (CE) n° 2009/29 du Parlement européen et du Conseil, 23 avr. 2009, modifiant la directive 2003/87/CE afin d'améliorer et d'étendre le système communautaire d'échange de quotas d'émission de gaz à effet de serre, *JOUE* n° L 140 du 5 juin 2009, p. 63.

[448] Ord. n° 2004-330, 15 avr. 2004, portant création d'un système d'échange de quotas d'émission de gaz à effet de serre, *JORF* n° 91, 17 avr. 2004, p. 7089, texte n° 46.

[449] Prot. CCNUCC Kyōto, 11 déc. 1997, à la Convention-cadre des Nations Unies sur les changements climatiques.

[450] D. n° 2005-295, 22 mars 2005, portant publication du protocole de Kyoto à la convention-cadre des Nations unies sur les changements climatiques (ensemble deux annexes), fait à Kyoto le 11 décembre 1997 et signé par la France le 29 avril 1998, *JORF* n° 75, 31 mars 2005, p. 5813, texte n° 29.

[451] REY (Hélène), « Le réchauffement climatique n'est plus un sujet "à part" », *Les Echos* [en ligne], 21 nov. 2019, https://www.lesechos.fr/idees-debats/cercle/le-rechauffement-climatique-nest-plus-un-sujet-a-part-1149569 ; XANDRY (Valérie), « Tout comprendre sur le prix carbone en cinq questions », *Challenges* [en ligne], 16 déc. 2015, https://www.challenges.fr/entreprise/energie/tout-comprendre-sur-le-prix-carbone-en-cinq-questions_46369 ; EHKIRCH (Valentin), « COP25 : faut-il fixer un tarif universel du carbone pour sauver la planète ? », *L'Express* [en ligne], 4 déc. 2019, https://www.lexpress.fr/actualite/societe/environnement/cop25-faut-il-fixer-un-prix-du-carbone-pour sauver-la-planete_2109941.html.

[452] « Les marchés du carbone et la réduction des émissions de gaz à effet de serre dans un monde en réchauffement. Évaluation de l'appui du Groupe de la Banque mondiale au financement carbone », IEG [en ligne], 7 avr. 2020, http://documents.banquemondiale.org/curated/fr/787471586280723785/pdf/R%C3%A9sum%C3%A9.pdf. ; GREENFIELD IV (Robert), « Blockchain Enabled Carbon Credit Markets Real considerations to make when tokenizing carbon credits », *Medium* [online], 12 Sept. 2019, https://medium.com/@robertgreenfieldiv/blockchain-enabled-carbon-credit-markets-1a195520f0e1 ; ZURRER (Ryan), « The Carbon Token Ecosystem White Paper: A decentralized P2P self-organizing consensus mechanism and marketplace for carbon offset lifecycle management using blockchain tokens », *Medium* [online], 26 juin 2017, https://medium.com/@rzurrer/the-carbon-token-ecosystem-white-paper-a-decentralized-p2p-self-organizing-consensus-mechanism-and-aa218bdeeb64. – Le prix du quota peut, en effet, suivre les cours des marchés du carbone, régulés par des autorités fixant un plafond aux émissions de gaz à effet de serre (GES), par exemple (pour plus de précisions sur la fixation du prix carbone par les marchés, v., XANDRY (Valérie), art. cit.). Il en va ainsi du modèle de tarification du *Standard Fairtrade* développé par Fairtrade International et Standard (v., https://info.fairtrade.net/fr/product/carbon-credits), ou le *EU Emissions Trading System* (EU-ETS) mis en place depuis 2005 au sein de l'UE. Pour une étude détaillée des différents systèmes de calculs du prix du carbone, outre la fixation par le marché, v. notamment, « Carbon pricing: What is a carbon credit worth? », *Gold Standard* [online], Categories > Blogs, https://www.goldstandard.org/blog-item/carbon-pricing-what-carbon-credit-worth.

de tirer profit de la revente des excédents de quotas reçus[453], ou encore à profiter de certaines failles fiscales, notamment dans le cadre de fraudes dites « carrousel à la TVA »[454], voire à créer un réseau d'activités illégales autour des quotas carbone, comprenant des actes de délinquance financière, d'escroquerie, d'extorsions de fonds ainsi que des assassinats, en bande organisée[455].

Afin de promouvoir un « système fiable de comptabilisation » tout en évitant les problèmes de « double comptage » évoqués par l'art. 6, § 2, de l'Accord de Paris de 2015[456], mais également de fixer le principe d'une tarification du carbone, des auteurs proposent de mettre en œuvre un protocole *blockchain* d'échange P2P de quotas d'émissions, neutre, immuable et transparent[457]. Le groupe indépendant d'évaluation (IEG) encourage d'ailleurs le groupe de la Banque mondiale à identifier et à développer ces politiques et mesures de tarification à travers des approches novatrices[458], dans l'objectif de renforcer la coordination et d'améliorer la complémentarité des initiatives et instruments existants[459], et de créer ainsi la prochaine génération de marchés du carbone[460]. C'est, par exemple, sur ce support que s'est appuyée l'entreprise Play it Open pour créer un marché du carbone sur *blockchain*[461]. Associée à Play it Open, l'entreprise

---

[453] En 2018, des entreprises russes et ukrainiennes (représentant 95 % des quotas émis) ont détourné l'objectif principal de réduction des GES afin de récolter davantage de réductions d'émissions, échangeable au titre des art. 12 et 17 du protocole de Kyoto, menant à une augmentation exponentielle des émissions. En effet, en mars 2015, sur près de 872 millions d'unités de réduction des émissions émises dans le cadre de la mise en œuvre conjointe (MOC), environ 600 millions découlaient des entreprises visées, soit presque 80 % des émissions mondiales. V. notamment, KOLLMUSS (Anja), SCHNEIDER (Lambert), ZHEZHERIN (Vladyslav), « Has Joint Implementation reduced GHG emissions? Lessons learned for the design of carbon market mechanisms (brief) », SEI [online], 24 Aug. 2015, https://mediamanager.sei.org/documents/Publications/Climate/SEI-PB-2015-JI-environmental-integrity.pdf ; « Une grave fraude aux "crédits carbone" exploitée par plusieurs pays pollueurs », *L'Express.fr* [en ligne], 26 août 2015, https://www.lexpress.fr/actualite/societe/environnement/gaz-a-effet-de-serre-une-faille-dans-le-protocole-de-kyoto-a-fait-grimper-les-emissions_1709639.html ; WOLF (Benjamin), KANDZIORA (Kolja), « Le crédit-carbone, un business lucratif », *Arte* [en ligne], 26 août 2015, https://info.arte.tv/fr/le-credit-carbone-un-business-lucratif.

[454] Pour plus de précisions sur le sujet, v., CHENEVIERE (Cédric), « *Fraudes et autres atteintes à l'intégrité du système d'échange de quotas d'émission* », *RLDA* 2011/1, nº 56.

[455] Il s'agit essentiellement de l'affaire dite de la « Mafia du CO2 », dont les actes criminels ont été révélés en 2017. Pour plus de précisions, v. les dossiers : ROBERT-DIARD (Pascale), PIEL (Simon), « L'incroyable histoire de l'arnaque au carbone : le résumé des cinq épisodes », *Le Monde* [en ligne], 14 août 2017, https://www.lemonde.fr/festival/article/2017/08/14/l-incroyable-histoire-de-l-arnaque-au-carbone-le-resume-des-cinq-episodes_5172257_4415198.html ; « La Mafia du CO2 : notre dossier », *Mediapart* [en ligne], nov. 2017, https://www.mediapart.fr/journal/international/dossier/la-mafia-du-co2-notre-dossier.

[456] Accord Nations Unies Paris, déc. n° 1/CP.21, 12 déc. 2015, sur le climat. – Ratifié par l'UE et entré en vigueur le 4 novembre 2016.

[457] GREENFIELD IV (Robert), art. cit. ; ZURRER (Ryan), art. cit.

[458] « Les marchés du carbone et la réduction des émissions de gaz à effet de serre dans un monde en réchauffement. Évaluation de l'appui du Groupe de la Banque mondiale au financement carbone », préc., pp. 22-23.

[459] *Ibid.*, p. 19.

[460] *Ibid.*, p. 6.

[461] PIERRE (Coralie), « Montpellier. Play it Open valorise les démarches RSE par la blockchain », *Mid e-news* [en ligne], 17 nov. 2017, https://www.midenews.com/2017/11/17/montpellier-play-it-open-valorise-demarches-rse-blockchain/.

Pur Projet promeut ainsi le développement durable et l'intégrité environnementale en assistant les entreprises dans leurs stratégies de compensation carbone[462], inscrite au titre des mesures volontaires d'atténuation et d'adaptation des émissions de gaz à effet de serre de l'art. 6 de l'Accord de Paris de 2015, et contribuant à la réalisation des projets fixés par l'UE dans son Pacte Vert[463]. La *blockchain* permet aux entreprises de tracer et de certifier chacune de leurs actions, tout en les accompagnant dans la réduction de leur empreinte carbone par la mise à disposition d'un marché du carbone. L'application mise au point créée et attribue automatiquement des équivalents en jetons (*tokens*) crédits-carbone, échangeables sur la chaîne afin de permettre aux entreprises qui n'ont pas pu réduire leurs émissions d'acheter des quotas à d'autres[464]. Selon l'entreprise, les chiffres pour le fabricant de capsules de café Nespresso, qui a choisi volontairement de compenser ses émissions en investissant dans des projets d'agroforesterie au sein de ses filières de café en Colombie, au Guatemala et en Éthiopie, révèlent que « les 500 000 arbres plantés chaque année sur les champs de café ont la capacité de stocker l'équivalent de l'intégralité de l'empreinte carbone de chaque tasse de café consommée en France »[465]. De nombreuses initiatives similaires ont vu le jour dès 2016, telles que les projets sur *blockchains* de ClimateTrade (*Climate Coin*)[466], Coinbase (*Carboncoin*)[467], ConsenSys (*CarbonX*)[468], Energy-Blockchain Labs et IBM (*Carbon Credit Management Platform*)[469].

Afin de tendre vers un principe de tarification unique du carbone tel que le préconisent nombre d'économistes[470], la Climate Chain Coalition (CCC) est une initiative mondiale ouverte, soutenue notamment par la CCNUCC, visant à encourager la collaboration et l'harmonisation des pratiques entre les membres et les parties prenantes, à savoir environ 200 organisations internationales, comprenant la plupart des *start-ups*

---

[462] V. le site du projet, https://www.purprojet.com/. – Pour plus de précisions sur la compensation carbone, v., la plateforme Info Compensation Carbone, https://www.info-compensation-carbone.com/.
[463] COM(2019) 640 final de la Commission au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions, 11 déc. 2019, Le Pacte Vert pour l'Europe.
[464] https://www.purprojet.com/fr, Insetting > Qu'est-ce que l'Insetting ? > Définition.
[465] « Quand la blockchain permet de certifier le bilan carbone des grandes entreprises », *WE demain* [en ligne], 3 nov. 2016, https://www.wedemain.fr/Quand-la-blockchain-permet-de-certifier-le-bilan-carbone-des-grandes-entreprises_a2257.html. – V. également, https://www.nespresso.com/entreprise/climat/les-arbres-essentiels-pour-un-cafe-de-qualite.
[466] https://climatetrade.com/.
[467] https://www.coinbase.com/.
[468] https://consensys.net/.
[469] https://www-03.ibm.com/press/us/en/pressrelease/51839.wss.
[470] V., notamment, AKERLOF (Georges) (dir.), « Economists' Statement on Carbon Dividends. The Largest Public Statement of Economists in History », *The Wall Street Journal* [online], 17 Jan. 2019, https://clcouncil.org/economists-statement/ ; DELPLA (Jacques), GOLLIER (Christian), « Pour une Banque Centrale du Carbone », Asterion [en ligne], Analyses pour la politique économique, n° 1, 1er oct. 2019, pp. 2-4, https://cdn.website-editor.net/6d83e4db0957400da09979d8cdcf5ee6/files/uploaded/BCC.pdf

précitées[471]. En uniformisant les règles de gouvernance, notamment en standardisant les méthodes de calcul du prix du carbone, et en permettant au système de bénéficier des qualités de la technologie des blocs, le concept doit, en principe, renforcer l'efficacité des dispositions internationales. À terme, cela devrait générer un accroissement de la confiance qui permettra de légitimer et de généraliser son utilisation[472].

Parallèlement, d'autres auteurs s'appuient sur la valeur de l'action pour le climat dévoilée au sein du rapport Quinet de février 2019[473] pour imaginer des *smart contracts* associant automatiquement le système de *tokens* à un objectif de politique publique s'identifiant comme une valeur tutélaire du prix du carbone[474]. De la même manière, il est possible d'imaginer que les *smart contracts* établis puissent, par la suite, automatiser l'exécution des sanctions prévues, comme celles spécifiques au Protocole de Kyoto[475] , à savoir la majoration de 30 % à la suite d'un surplus d'émissions et la suspension des droits de participation au système d'échange de quotas[476]. Le but serait, à terme, de créer un mécanisme de dissuasion.

45. Optimisation des projets de conservation, de gestion durable des forêts et de renforcement des stocks de carbone forestier dans les pays en développement. Partant du constat formulé par l'ONU et selon lequel la protection des forêts est un moyen rentable de fournir un tiers des réductions nécessaires des émissions mondiales de carbone d'ici 2030[477], la *start-up* GainForest s'appuie sur la technologie des *smart contracts* pour encourager les financements internationaux dans la lutte contre la déforestation en

[471] https://www.climatechaincoalition.io/.
[472] GREENFIELD IV (Robert), art. cit. – Sur le prototype *Climate Chain Coalition* et le potentiel des technologies *blockchain* pour accélérer la mise en œuvre de l'Accord de Paris sur le climat, v. également, GEOFFRON (Patrice), VOISIN (Stéphane), « Comment mettre la *Blockchain* au service de la mise en œuvre de l'Accord de Paris sur le climat », *Annales des Mines - Responsabilité et environnement* 2019/2 (avr. 2019), n° 94, pp. 96 à 99.
[473] La valeur de l'action pour le climat, Une valeur tutélaire du carbone pour évaluer les investissements et les politiques publiques, Rapport de la Commission Quinet, fév. 2019.
[474] GEOFFRON (Patrice), VOISIN (Stéphane), « La Blockchain au service d'une tarification du carbone ? », *Connaissance des énergies* [en ligne], 5 nov. 2019, https://www.connaissancedesenergies.org/tribune-actualite-energies/la-blockchain-au-service-dune-tarification-du-carbone#notes.
[475] Accords Nations Unies Marrakech, déc. n° 24/CP.7, 10 nov. 2001, sur les procédures et mécanismes relatifs au respect des dispositions du Protocole de Kyoto.
[476] *Ibid.*, section XV, paragraphe 5.
[477] « FNUF-14: Coup d'envoi de la première session technique du Forum des Nations Unies sur les forêts pour évaluer la mise en œuvre du Plan stratégique 2017-2030 », *Nations Unies* [en ligne], 6 mai 2019, Conseil Économique et Social > Forum des Nations Unies sur les Forêts > Quatorzième Session, 2e Et 3e Séances – Matin & Après-Midi, https://www.un.org/press/fr/2019/envdev1944.doc.htm. – « La nature est l'un des moyens les plus efficaces de lutter contre le changement climatique et devrait faire partie de la stratégie de chaque pays en matière de climat », selon la Directrice exécutive du Programme des Nations Unies pour l'environnement (PNUE), Inger Andersen. V., « La nature est l'un des moyens les plus efficaces de lutter contre le changement climatique », *ONU info* [en ligne], 19 sept. 2019, Thèmes > Changement climatique, https://news.un.org/fr/story/2019/09/1052082.

Amazonie[478]. En application du programme UN-REDD (*Reducing emissions from deforestation and forest degradation*) lancé en 2008 par l'ONU en vertu de la décision 4, i), prise à la 14ème réunion du Conseil d'orientation[479], l'application met en relation les populations autochtones, appelées « gardiens », et des investisseurs internationaux, à travers des *smart contracts*. Selon les termes du contrat, si les gardiens désignés réussissent à protéger la parcelle de forêt pendant la durée fixée, la *blockchain* leur transfère automatiquement la somme conventionnellement prévue[480]. La télédétection, système d'IA utilisant des satellites, directement reliée à la *blockchain*, vérifie la préservation de chaque parcelle de forêt, et déclenche les paiements si les conditions du *smart contract* ont été remplies[481]. En plus d'assurer une forme de sécurité légale des populations locales – ce qui faisait défaut jusqu'alors – en leur fournissant traçabilité et transparence au niveau mondial dans les actions menées sur le terrain, l'application leur offre un moyen de s'autonomiser *via* la sécurité financière d'un financement participatif international[482]. Il s'agit, à travers cette application, de consolider les engagements internationaux en renforçant leur effectivité.

46. Le *smart contract*, libérateur de l'électromobilité ? Les délais de recharge, ainsi que les difficultés pratiques en matière de facturation résultant de l'existence d'une multitude de prestataires de services, constituent un obstacle majeur à l'adoption à grande échelle des véhicules électriques[483]. Face à ces divers problèmes, nombre de *start-ups* ont choisi la technologie des *smart contracts* pour fonder des plateformes transactionnelles mettant en relation les usagers avec les prestataires privés, et éventuellement publiques. Le paiement est effectué automatiquement entre les deux parties au *smart contract*. Il en

---

[478] LEHNIS (Marianne), « These High-Tech Crusaders Are Fighting to Save the Rainforest », *Breaker Mag* [online], 14 Mar. 2019, https://breakermag.com/these-high-tech-crusaders-are-fighting-to-save-the-rainforest/. V. également, https://www.gainforest.app/#/.

[479] https://www.un-redd.org/

[480] LEHNIS (Marianne), art. cit.

[481] *Id.*

[482] Les projets qui autonomisent les communautés autochtones sauvent certaines des forêts du monde et d'autres écosystèmes naturels. Il en va ainsi de la forêt Amazonienne, où les survols du territoire de Kayapo, financés par des ONG, ont permis de repérer à plusieurs reprises la présence illégale de mineurs d'or. Face à l'inaction du gouvernement, les ONG ont mis à disposition des Kayapo le matériel nécessaire (bateaux, moteurs, carburant, GPS, radio, etc.) à une expédition visant à protéger leurs droits sur la terre. De vastes étendues de forêt amazonienne restent intactes aujourd'hui suite aux actions des groupes autochtones, soutenus par des alliances d'ONG telles que Environmental Defence Fund, The Kayapo Project, Instituto Socioambiental, Comissão Pró-Índio de São Paulo, Centro de Trabalho Indigenista, Operação Amazônia Nativa, Planéte Amazone, Conselho Indigenista Missionário. Sur le sujet, v., ZIMMERMAN (Barbara), « Rain Forest Warriors: How Indigenous Tribes Protect the Amazon », *National Geographic* [online], 23 Dec. 2013, https://www.nationalgeographic.com/news/2013/12/131222-amazon-kayapo-indigenous-tribes-deforestation-environment-climate-rain-forest/.

[483] Items International, « Actualités. Blockchain dans le domaine de l'énergie : où en est-on ? », *Think Smartgrids* [en ligne], 7 mars 2019, https://www.thinksmartgrids.fr/actualites/blockchain-domaine-energie.

va ainsi des plateformes *Share&Charge*, développée par Innogy Motionwerk et slock.it, et *Car eWallet* par ZF en Allemagne[484], *Juice Box* par eMotorWerks aux États-Unis en Californie[485], *Everty* par Everty Pty Ltd en Australie[486], et du projet *Alva Energy Consortium* d'Alliander aux Pays-Bas[487].

47. *Smart contracts* et révolution des *Clouds*. Dans un domaine voisin, à l'image de ce qu'avait imaginé Vitalik Buterin pour remplacer les onéreuses *start-ups* spécialisées dans le stockage de fichiers en ligne (*Clouds*, du type *Dropbox*)[488], *Filecoin*[489] permet de mettre en location l'espace-mémoire non-utilisé de son ordinateur, ou inversement d'acheter de l'espace de stockage. Ce service de stockage de fichiers répartis ou « contrats *Dropbox* répartis »[490] repose sur un réseau P2P, entièrement crypté, décentralisé et automatisé[491].

48. Le *smart contract* au service de l'industrie culturelle et de l'art. En réponse à la crise des secteurs de l'industrie culturelle résultant de la généralisation de la distribution d'œuvres sur Internet, des applications basées sur la *blockchain* et les *smart contracts* ont été développées. D'après un auteur, il est possible « d'imaginer une programmation et une exécution automatiques des contrats, qui conduiraient à un partage "équitable" de la

[484] Respectivement, https://shareandcharge.com/ et https://car-ewallet.de/.
[485] https://evcharging.enelx.com/.
[486] « Electric Vehicle Charging for Local Governments », Everty Pty Ltd [online], Aug. 2018, https://citiespowerpartnership.org.au/wp-content/uploads/2018/10/Everty-Council-Document-FINAL-CONTENT-1.pdf.
[487] SÜMMERMANN (Dietrich), « Crossing the Chasm in Blockchain-based Electric Vehicle Charging », *Medium* [online], 20 Apr. 2018, https://medium.com/share-charge/crossing-the-chasm-in-blockchain-based-electric-vehicle-charging-25a6d96ffded#_ftn9.
[488] BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », préc.
[489] https://filecoin.io/.
[490] « Decentralized File Storage » [Trad. : Asseth, préc.], BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », préc.
[491] Vitalik Buterin en explique le fonctionnement, « la clé de voûte d'un tel système serait ce que nous avons appelé le "contrat *Dropbox* réparti". […] Premièrement, les données concernées sont divisées en blocs, chaque bloc étant chiffré pour en assurer la confidentialité, et sont utilisées pour la construction d'un arbre de Merkle. Un contrat est ensuite créé avec une règle stipulant que, à chaque *N* blocs, le contrat choisira un index aléatoire de l'arbre de Merkle (en utilisant l'empreinte du bloc précédent, accessible depuis le code du contrat, comme source aléatoire) et donnera *X ether* à la première entité qui fournira une transaction avec une preuve de possession du bloc situé à cet index dans l'arbre de Merkle. Lorsqu'un utilisateur souhaite re-télécharger un de ses fichiers, il peut utiliser un protocole de canal de micropaiement (par exemple payer 1 *zsabo* par 32 kilo-octets) pour récupérer le fichier ; l'approche la plus économique au niveau des frais consiste pour le payeur à ne pas publier la transaction avant la fin, en remplaçant plutôt la transaction par une autre plus lucrative avec un *nonce* identique après chaque 32 kilo-octets. Une fonctionnalité importante du protocole est que, bien qu'il semble qu'on fasse confiance à plusieurs nœuds aléatoires pour qu'ils ne perdent pas le fichier, on peut quasiment supprimer ce risque en divisant le fichier en de nombreux morceaux par partage secret et en observant les contrats pour vérifier que chaque morceau est toujours hébergé par un ou plusieurs nœuds. Le fait qu'un contrat continue à effectuer un paiement est la preuve cryptographique que quelqu'un héberge toujours le fichier », [trad. : préc.], *id.*

valeur entre créateurs, producteurs, éditeurs, distributeurs, diffuseurs et consommateurs de contenus numériques et à une rémunération des ayants droit reflétant la consommation au téléchargement ou à l'écoute près »[492]. La plateforme *Inmusik*[493] ou encore la *dApp UjoMusic*[494] proposent en effet aux artistes de placer leurs titres sur la *blockchain* et de prévoir le paiement, sans intermédiaires, des *royalties* et autres droits d'auteurs (CPI, art. L. 131-8, L. 214-1, L. 311-1 et s.) en indiquant, pour chaque fragment des titres correspondant, le ou les propriétaires des droits et destinataires des futures transactions. D'ailleurs, pour faciliter l'identification des œuvres au niveau mondial, trois sociétés de gestion collective du droit d'auteur, à savoir ASCAP aux États-Unis, PRS for Music au Royaume-Uni et la Sacem en France, collaborent avec IBM depuis avril 2017 afin de rapprocher les codes ISRC et ISWC, spécifiques au secteur de la musique enregistrée[495] en s'appuyant sur le projet « *Hyperledger Fabric* »[496] de la fondation *Linux*[497].

Sur le même concept de transparence et d'effectivité des droits de propriété intellectuelle, la plateforme d'art numérique *Ascribe* met à disposition des artistes des *smart contracts* leur permettant de sécuriser leurs droits sur une œuvre numérique[498]. Le *smart contract* attaché à une création numérique trace les utilisations de celles-ci et réclame automatiquement les redevances légalement dues pour les reverser à l'auteur en vertu des art. L. 111-1 et 121-1 du CPI.

49. En dehors du domaine des données, de l'énergie, ou de la culture, les *smart contracts* intéressent également le secteur assurantiel.

§ 2. Le fonctionnement des assurances « blockchaînées » : perspectives de changements

50. En 2017, la plupart des études de satisfaction client indiquaient que les assureurs rencontraient certaines difficultés dans leurs relations avec les consommateurs, en raison notamment d'un parcours client jugé mauvais. Par exemple, l'étude proposée par

[492] PONS (Jérôme), « La mise en œuvre de la blockchain et des smart contracts par les industries culturelles », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), pp. 81-90.
[493] V., http://www.InMusik.co.
[494] V., https://ujomusic.com/.
[495] Pour plus de précisions sur ce sujet, v., PONS (Jérôme), art. cit., pp. 89-90.
[496] V. les sites officiels, https://www.hyperledger.org/projects/fabric ; https://www.ibm.com/blockchain/fr-fr/hyperledger/.
[497] « Blockchain : la Sacem, Ascap et PRS for Music s'allient pour une meilleure identification des œuvres », *Société Sacem* [en ligne], communiqué de presse du 7 avr. 2017, http://societe.sacem.fr/actualites/innovation/blockchain--la-sacem-ascap-et-prs-for-music-sallient-pour-une-meilleure-identification-des-oeuvres.
[498] V., https://www.ascribe.io/.

l'AFNOR révélait que, d'une manière générale, les clients étaient peu satisfaits de leur expérience avec leur assureur, à laquelle ils attribuaient, en moyenne, la note de 5/10[499]. L'étude sur la Valeur de l'Expérience Client Assurance (VEC-A) de Teleperformance et GN Research dévoilait d'ailleurs que, d'une part, concernant les assurances destinées à garantir les biens (assurances IARD, « Incendie, Accidents et Risques Divers »), 40 % des souscripteurs avaient « vécu la gestion du sinistre comme un effort important », pour un taux de 52 % de satisfaction globale et, d'autre part, concernant les assurances santé, 60 % des souscripteurs avaient « vécu [la réclamation] comme un effort important », et 57 % se disaient devenus « détracteurs de la marque » d'assurances à laquelle ils étaient liés[500]. L'intégration des NTIC au sein des parcours client a nettement contribué à améliorer l'expérience client. D'après une étude réalisée par Bain & Company pour l'année 2018, 52 % des français, et particulièrement les profils âgés entre 18 et 34 ans (80 %), auraient délaissé leur assurance traditionnelle pour souscrire des polices d'assurance auprès des nouveaux acteurs des *InsurTechs*[501], jugées « plus adaptées à leurs besoins », et 14% affirment envisager sérieusement un changement[502].

Face à une jeune et puissante concurrence née de l'union d'Internet et des nouvelles technologies qui outrepassent les frontières nationales, à la mutation constante des exigences et des comportements des consommateurs ainsi que leur relation avec le risque, et à des demandes contradictoires de rentabilité, de sécurité et de fluidité, les compagnies d'assurances sont contraintes de maintenir leurs efforts en matière d'innovation. Très tôt, le secteur assurantiel a donc mené de nombreuses études et investissements sur les impacts des technologies du numérique, et en particulier des

[499] L'étude a été menée à partir des réponses à un questionnaire de satisfaction retournées par 3 008 clients de 40 compagnies différentes. V., LEGOFF (Éloïse), « Satisfaction client : peut mieux faire ! », *L'Argus de l'assurance* [en ligne], 1er juin 2017, https://www.argusdelassurance.com/acteurs/satisfaction-client-peut-mieux-faire.119162 ; https://indiko.afnor.org/wp-content/uploads/2017/08/Infographie-EXPERIENCE-CLIENT-Assurance.pdf.

[500] L'étude a été menée à partir des réponses à un questionnaires sur la perception des expériences vécues avec les assureurs, obtenues auprès de 6 000 personnes âgées de 18 ans et plus, évaluant plus de 4 000 expériences assurés IARD et 4 000 expériences Santé vécues auprès de 26 assureurs différents. V., « L'étude 2017 "La Valeur de l'Expérience Client" Assurance est disponible », *Teleperformances* [en ligne], 17 oct. 2017, https://fr.teleperformanceblog.com/strategic-thinking/letude-2017-la-valeur-de-lexperience-client-assurance-est-disponible/.

[501] DESOMBRE (Nicolas), DUVERNE (Denis), DE MONTCHALIN (Amélie), « Les stratégies d'internationalisation en assurances », *Rev. éco. fin.* 2017/2, n° 126, pp. 51-64.

[502] GOOSSENS (Camille), « Rapport annuel Bain & Company sur les Comportements et la Loyauté des Clients dans l'Assurance (chiffres 2018 pour la France) », *in* GOOSSENS (Camille), « 80 % des Millennials seraient prêts à souscrire une assurance auprès d'un nouvel acteur », *Bain & Company* [en ligne], 10 oct. 2018, https://www.bain.com/fr/a-propos-de-bain/media-center/communiques-de-presse/france/2018/rapport-annuel-bain--company-sur-les-comportements-et-la-loyaute-des-clients-dans-lassurance/ ; FAURÉ (Virginie), « Comment augmenter la satisfaction client dans le secteur de l'assurance ? », *WizVille* [en ligne], 25 mars 2019, https://wizville.fr/blog/satisfaction-client-assurance/.

blockchains, sur leurs activités[503]. Cette forte implication a abouti, d'une part, à des programmations de type *business-to-business* (B2B) ayant vocation à renforcer leurs relations professionnelles avec les entreprises et, d'autre part, à réaliser un état des lieux des avantages du *smart contract* dans la relation entre l'assuré, consommateur d'un produit d'assurance, et l'assureur (B2C)[504]. Différentes stratégies s'appuyant sur les capacités de la technologie des *blockchains* à optimiser la relation client ont été élaborées. Parmi ces cas d'usages, les applications mettant en œuvre des mécanismes d'exécution automatisés des dispositions contractuelles ont mené les assureurs vers une solution avantageuse tant pour l'assureur que pour l'assuré, destinée à réinstaurer un lien de confiance dans les assurances traditionnelles (A). En parallèle, des réseaux de consommateurs tentent de s'affranchir de ce cadre traditionnel en créant, *via* des *smart contracts* et même des DAO, de véritables systèmes d'assurance P2P autonomes, distribués et décentralisés (B).

A. Réinstaurer le lien de confiance dans les assurances traditionnelles

51. Les attentes des assureurs et des consommateurs de produits d'assurance. Aujourd'hui, les assurés réclament davantage de fluidité dans leurs relations avec leur assureur[505]. Dans la pratique, les clients insatisfaits soulèvent un manque de réactivité et de rapidité dans le traitement de leurs dossiers (les assurés déclarent devoir contacter en moyenne cinq fois leur assureur avant de réussir à le joindre et à obtenir les renseignements souhaités[506]). Les clients interrogés évoquent également des difficultés quant à l'exécution du contrat, dont certaines conditions ne sont pas toujours pleinement comprises bien qu'inscrites en toutes lettres, et quant aux démarches administratives à accomplir[507], notamment en raison de la complexité du langage assurantiel[508]. Au-delà de l'accessibilité de l'assureur, la clarté des contrats souscrits fait également partie de leurs exigences, lesquels auraient tout intérêt à bénéficier d'une présentation plus ergonomique. Cette situation représente irrémédiablement une source avérée de défiance, mais identifie également les variables à privilégier dans le cadre d'une refonte des parcours clients.

---

[503] « Blockchain, catalyseur de nouvelles approches en assurance. Volume 2 : Quelles mises sur le marché concrètes et quelles évolutions pour 2019 ? », PwC [en ligne], 2018, p. 1, https://www.pwc.fr/fr/assets/files/pdf/2018/09/pwc-blockchain-3-catalyseur-de-nouvelles-approches-en-assurance-2018.pdf.
[504] BARBRY (Éric), art. cit., p. 79.
[505] *Id.*
[506] « L'étude 2017 "La Valeur de l'Expérience Client" Assurance est disponible », préc.
[507] FAURÉ (Virginie), art. cit.
[508] LEGOFF (Éloïse), art. cit.

Partant du constat que la satisfaction du client a un impact économique considérable, en ce sens qu'elle contribue à fidéliser la clientèle – les études démontrent d'ailleurs qu'il est plus difficile et plus coûteux pour les assureurs d'acquérir de nouveaux clients que de conserver les clients actuels[509] –, et qu'elle influence directement l'image de la marque, les assureurs ont montré un intérêt croissant dans l'investissement de la *blockchain*. En dehors des questions d'amélioration des parcours client, de fidélisation et d'image de marque, les spécificités de la technologie pourraient leur permettre également de détecter et de réduire les risques de fraude à l'assurance, dont les pertes potentielles annuelles s'élèvent à plus de 12 milliards d'euros toutes assurances comprises, avec 2,5 milliards d'euros de fraudes identifiées en IARD en 2015, et 1 demi-milliard d'euros en 2018[510].

52. Automaticité et garanties réciproques. Assurés et assureurs manifestent un besoin de confiance réciproque, et la *blockchain* paraît être une solution à ne pas négliger. Outre les importants bénéfices découlant de sa fonction de base de données étendue, sécurisée, décentralisée et infalsifiable[511], l'auto-exécution des *smarts contracts* permet d'automatiser une multitude de processus de polices d'assurance pour une efficacité opérationnelle et un accompagnement des consommateurs de la souscription de la police à la potentielle déclaration de sinistre. Comme le constate Virginie Fauvel, *Member of Management Board* chez *Allianz France*, « dans cinq à dix ans, les processus des assureurs seront très différents de ce qu'ils sont aujourd'hui. La *blockchain* aura tout changé. Elle va modifier le métier, aussi bien dans les interactions entre assureurs que dans les interactions avec les clients »[512]. Nombreux sont les professionnels du secteur qui investissent la question[513].

Programmés pour s'exécuter directement sur la *blockchain*, sans intermédiaires, les termes du contrat d'assurance lient l'assuré et son assureur par une convention synallagmatique immuable. Pour cela, ces termes déterminent, dès la souscription, l'intégralité des conditions d'application et d'exécution du contrat, à savoir les éléments permettant de qualifier chaque évènement pris en compte par le contrat et l'énumération des exclusions de manière formelle et limitée (C. ass., art. L. 113-1, al. 1er), la durée du

[509] FAURÉ (Virginie), art. cit.
[510] http://www.alfa.asso.fr/fr/content/la-fraude, La fraude à l'assurance > Chiffres clés.
[511] VERBIEST (Thibault), « Blockchain : une révolution juridique ? », art. cit., *loc. cit.*
[512] THEVENIN (Laurent), « Les assureurs s'engouffrent dans la blockchain », *Les Echos* [en ligne], 31 oct. 2016, https://www.lesechos.fr/31/10/2016/LesEchos/22309-122-ECH_les-assureurs-s-engouffrent-dans-la-blockchain.htm.
[513] « L'innovation numérique, enjeu clé de l'assurance pour 2020 », *CXP Group* [en ligne], 2018, https://www.sigma.fr/solutions-services/linnovation-numerique-enjeu-cle-de-lassurance-pour-2020/.

contrat (C. ass., art. L. 113-12, al. 1er), les franchises, les modalités de déclaration de sinistre (C. ass., art. L. 113-2, 3° et 4°), et les actions associées telles que les prestations, leurs montants et modalités de règlement[514]. Il se pourrait même que le *smart contract* souscrit soit constitué de « sous-*smart contracts* » destinés à être appelés par le contrat principal en cas de réclamation ou, d'une manière générale, à l'occasion de la survenance d'un sinistre. Au-delà de l'accessibilité de l'assureur, l'intelligibilité des contrats souscrits serait ainsi améliorée. Dans un objectif de simplification des démarches administratives, l'automatisation permettrait aux assurés d'être remboursés des pertes et dommages garantis, sans même avoir à remplir directement de déclaration de sinistre[515]. En effet, puisque cette déclaration n'est soumise à aucune condition de forme[516] excepté la condition de l'envoi en recommandé (C. ass., art. L. 113-2, 3°) à laquelle la *blockchain* peut, par ailleurs, répondre (C. ass., art. L. 111-12)[517], rien n'empêche en principe qu'elle soit effectuée par un procédé de traitement instantané, dans le délai fixé par le contrat (C. ass., art. L. 113-2, 3° et 4°). Il suffirait alors qu'un accident, explicitement identifié au sein du *smart contract* de l'assuré, survienne pour que l'indemnisation d'assurance lui soit immédiatement versée, sans l'attente de traitement et *a fortiori* d'aval de la part de l'assureur[518].

Réciproquement, chaque déclaration et indemnisation de sinistre étant enregistrées de manière immuable sur la *blockchain*, l'assuré qui aurait déjà perçu une indemnisation pour un sinistre identifié ne pourrait tenter d'en solliciter une nouvelle auprès d'un autre établissement[519]. Le *smart contract* pourrait même être programmé pour procéder à ces vérifications automatiquement et rejeter toute demande frauduleuse au moment de sa validation. Par ailleurs, l'assuré, mauvais payeur, qui n'honorerait pas le paiement d'une prime dans le temps imparti recevrait automatiquement une mise en demeure, et verrait sa garantie suspendue par la *blockchain* dans les trente jours et jusqu'à paiement effectif de ses cotisations d'assurance, sans même requérir de l'assureur de constater le non-paiement (C. ass., art. L. 113-3).

Finalement, le caractère automatisé du *smart contract* assure le respect des droits de chaque partie, pour une meilleure expérience et satisfaction client. Les relations assuré-

---

514 MARRAUD DES GROTTES (Gaëlle), « La blockchain : un secteur encore en phase d'exploration, mais très prometteur », *RLDI* 2017/2, n° 138.
515 *Id*.
516 Cass. Civ. 1ère, 4 juin 1945, *RGAT* 1945, p. 151.
517 Sur la fiabilité des systèmes de signatures électroniques *via blockchain*, *infra* n°s 95 et s.
518 RODA (Jean-Christophe), art. cit., *loc. cit*.
519 KEMP (Leanne), « Blockchain applications in assurance », Deloitte LPP [online], 2016, pp. 1-2, https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-deloitte-blockchain-app-in-insurance.pdf.

assureur seraient ainsi simplifiées et fluidifiées, à raison d'une gestion rapide et efficace des demandes – tant de souscription que d'indemnisation – et des versements des indemnités[520]. À terme, l'exécution automatisée des tâches permettra aux assureurs de réduire les coûts d'investissements initiaux et les dépenses de structure et de gestion administrative[521], économies qui se répercuteront en principe sous la forme d'une réduction des primes d'assurances et d'une amélioration de la compétitivité.

Dans un objectif de satisfaction client, il pourrait être envisagé de programmer le *smart contract* pour qu'il exécute la clause de dépannage d'une police d'assurance automobile. Ainsi, dès qu'un accident surviendrait, l'assuré activerait le *smart contract*, qui prendrait directement contact avec les services de dépannages pour leur fournir les informations nécessaires à la constitution du dossier[522]. L'assuré conviendrait ensuite personnellement d'une date pour effectuer les réparations convenues. Selon l'importance des réparations, le *smart contract* pourrait également permettre une mise à disposition automatique d'un véhicule de prêt *via*, par exemple, la fourniture d'un code d'activation temporaire du véhicule[523]. Il faudrait, pour cela, que le *smart contract* fixe un seuil de déclenchement sous la forme d'une condition de montant ou d'une liste énumérant limitativement les dommages matériels menant à une telle garantie, par exemple. Le recours à une assistance médicale ou à une ambulance, ainsi que le paiement automatique des frais afférents (frais médicaux ou frais de transport sanitaire) pourraient également être programmés et auto-exécutés par la *blockchain*[524]. En programmant des *smart contracts* pour qu'ils s'exécutent en fonction, d'une part, de la parution au Journal Officiel, par zone, par type d'évènement et par périodes, d'arrêtés de reconnaissance de catastrophe naturelle, et, d'autre part, de la localisation des biens de l'assuré, la garantie d'indemnisation des dommages matériels en cas de catastrophe naturelle pourrait être également optimisée.

53. Domaines actuels d'application. Les *smart contracts* ont ainsi vocation à se développer dans les secteurs de la gestion de sinistre et de l'indemnisation des assurés[525], et en particulier à s'appliquer aux contrats d'assurance de dommages « de masse », c'est-à-dire les assurances habitation et automobile, en raison de la facilité à les traduire sous

[520] DENIS (Bénédicte), HEGEDUS (Orsolya), LAREDO (Anne), SOLERANSKI (Louis), « La Blockchain dans le secteur de l'assurance », *RLDA* 2017/12, n° 132.
[521] *Id.*
[522] GRYNBAUM (Luc), LE GOFFIC (Caroline), MORLET-HAÏDARA (Lydia), *Droit des activités numériques*, éd. Dalloz, 1ère édition, 2014, n°s 288 et s.
[523] VERBIEST (Thibault), « Blockchain : une révolution juridique ? », art. cit., *loc. cit.*
[524] DENIS (Bénédicte), HEGEDUS (Orsolya), LAREDO (Anne), SOLERANSKI (Louis), art. cit.
[525] VERBIEST (Thibault), « Blockchain : une révolution juridique ? », art. cit., *loc. cit.*

forme d'algorithmes[526]. D'après un rapport du Capgemini's Digital Transformation Institute de 2016, l'automatisation *via* l'utilisation de *smart contracts* permettrait aux compagnies d'assurances automobiles d'économiser environ 21 milliards de dollars sur les coûts annuels au niveau mondial[527].

C'est par exemple sur ce concept que le consortium Blockchain Insurance Industry Initiative (B3i) conçoit des applications logicielles fondées sur les technologies *blockchains* et *smart contracts*, permettant à la fois d'améliorer la qualité des données utilisées par les entreprises et d'automatiser certaines procédures dans un objectif de célérité et d'efficacité[528]. La première application, *B3i Cat XoL*, a été développée et mise sur le marché en septembre 2019 pour le secteur de la réassurance[529]. Elle permet aux clients et aux assureurs de négocier facilement et à moindre coût les conditions et le prix des primes, de conclure les contrats d'assurance et d'automatiser les paiements[530].

La *start-up* Monuma s'appuie sur la *blockchain Bitcoin* pour proposer un « expert 24/24 » pour, d'une part, simplifier les démarches de constatation et d'estimation, et *a fortiori* d'indemnisation, et, d'autre part, écourter les délais de traitement des dossiers[531]. L'application met à disposition des assurés d'Allianz France, Moonshot et Valoo, un registre décentralisé sur lequel ils sont invités à lister leurs biens, accompagnés d'une photo et d'une preuve d'achat afin de pouvoir prouver leur existence, leur propriété et leur valeur en cas de sinistre. La valeur d'usage des biens est ensuite actualisée automatiquement chaque année en fonction du coefficient de vétusté inscrit dans le contrat[532], conformément à l'art. L. 121-1, al. 1er, du C. ass. En moyenne, ce système permet d'obtenir en trois jours, au lieu d'un mois traditionnellement, un constat d'état ou une expertise, ce qui permet indirectement de réduire les coûts de fonctionnement[533].

Appliquée actuellement au secteur maritime, la plateforme *Insurwave* propose pour sa part de moderniser les procédures administratives de traitement des informations des assureurs et courtiers d'assurances afin de les rendre plus efficaces et plus adaptées

---

[526] DENIS (Bénédicte), HEGEDUS (Orsolya), LAREDO (Anne), SOLERANSKI (Louis), art. cit.
[527] « Smart Contracts in Financial Services: Getting from Hype to Reality », CapGemini Consulting [online], 2016, p. 12, https://www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/08/smart_contracts_paper_long_0.pdf.
[528] WOOD (Charlie), « B3i deploys latest Cat XoL product », *Reinsurance News* [online], 15 Oct. 2019, https://www.reinsurancene.ws/b3i-deploys-latest-cat-xol-product/ ; https://b3i.tech/what-we-do.html.
[529] *Id.*
[530] *Id.*
[531] « Blockchain, catalyseur de nouvelles approches en assurance. Volume 2 : Quelles mises sur le marché concrètes et quelles évolutions pour 2019 ? », préc., p. 9.
[532] https://www.monuma.fr/qui-sommes-nous-fr.
[533] *Id.*

aux besoins des assurés[534]. Développée par Ernst & Young en collaboration avec l'entreprise Guardtime, elle met à disposition des assureurs et des transporteurs maritimes un système assurantiel automatisé capable de gérer le risque dynamique[535]. La base de données distribuée et immuable (*ledger*) constitue un accès sécurisé à une seule version de la vérité, et permet ainsi aux *smart contracts* mis en place de remplacer avec sécurité et transparence de nombreux processus manuels chronophages, tout en proposant aux transporteurs d'obtenir, à chaque étape du transport, une évaluation du risque. Sous la forme d'un outil d'aide à la décision, la plateforme les informe instantanément de l'étendue de leur garantie, ainsi que la nature de la couverture, le coût de la surprime, etc., en fonction des risques pris et des décisions à prendre[536]. Cet outil procure une garantie « en temps réel » et une possibilité d'adapter la traversée en pleine connaissance des coûts encourus, sans nécessiter de négociations ou renégociations *a posteriori*[537]. En contrepartie, en plus d'engendrer des économies d'argent et de temps sur le plan administratif, le système permet aux assureurs d'améliorer la gestion de leur exposition aux risques et de proposer un accompagnement adapté aux besoins réels et immédiats des assurés[538]. Les développeurs d'*Insurwave* travaillent actuellement sur une adaptation du protocole aux industries et entreprises de BTP[539].

D'autres prototypes sont actuellement en phase d'expérimentation[540]. Des mécanismes de gestion similaires à ceux des entreprises captives d'assurance fondés sur le transfert de risques automatisé et l'auto-exécution des transactions associées (C. ass., art. L. 350-2, 1° et 2°) sont en cours de développement chez Allianz, en partenariat avec Nephila[541]. Des projets portent encore sur des systèmes d'assurance anti-pollution (Axa) qui permettront aux personnes sensibles à la qualité de l'air, telles que les personnes atteintes de maladies pulmonaires, de souscrire une garantie pour couvrir les risques liés à un niveau de pollution établi (impossibilité immédiate de se rendre sur son lieu de travail, frais supplémentaires pour des besoins impérieux, etc.)[542]. La Caisse des dépôts

---

[534] REMY (Morgane), « La blockchain au service de l'assurance maritime », *L'argus de l'assurance* [en ligne], 8 nov. 2018, https://www.argusdelassurance.com/tech/la-blockchain-au-service-de-l-assurance-maritime.136654.

[535] https://insurwave.com/ ; « Better-working insurance: moving blockchain from concept to reality », EY et Guardtime [online], 2017, p. 1, https://media.voog.com/0000/0044/6548/files/5.%20Product%20-%20InsurWave%20-%20ebook.pdf.

[536] *Id.*

[537] REMY (Morgane), art. cit.

[538] « Better-working insurance: moving blockchain from concept to reality », préc., pp. 4, 6.

[539] *Ibid.*, p. 9 ; REMY (Morgane), art. cit.

[540] Pour une étude détaillée, v., LOIGNON (Stéphane), *Big Bang Blockchain. La seconde révolution d'internet*, éd. Tallandier, 2017.

[541] Pour plus de précisions, v., https://www.agcs.allianz.com/about-us/digital-transformation-and-insurance/blockchain.html, About Us > Digital Transformation > Embracing Blockchain Technology.

[542] LOIGNON (Stéphane), *op. cit., loc. cit.*

et consignation envisage de créer *Labchain*, un système d'assurance décès connecté au Répertoire national d'identification des personnes physiques (RNIPP), automatisant les indemnisations[543]. Toutefois, bien que la mise en place d'une *blockchain* semble intéressante dans le cadre de l'art. L. 132-8, al. 7, du C. ass.[544], nombre d'auteurs s'y opposent[545]. Parmi les arguments avancés figure, par exemple, le manque de pertinence d'un *smart contract* versant le capital ou la rente d'un contrat au bénéficiaire alors même que la correcte identification dudit bénéficiaire est en pratique délicate[546]. Or l'importance de cette identification semble conduire ces auteurs à penser qu'une erreur ne ferait que retarder encore davantage les délais de traitement[547]. Il est en effet essentiel d'évaluer et d'identifier la pertinence du cas d'usage avant son déploiement et son utilisation. Certains auteurs constatent en ce sens que, « tout au plus cela permettrait […] à l'assureur vie de déclencher une alerte avec une obligation de recherche du bénéficiaire »[548]. Cependant, il semble *a priori* que la programmation des conditions qui justifieraient la mise en place automatisée des mesures conservatoires de l'art. L. 631-2-1, 5° ter, du CMF[549] pourrait contribuer à renforcer le dispositif de prévention des risques de crise financière et la stabilité du système financier[550].

54. Optimisation des contrats et confiance : l'exemple des assurances paramétriques. Force est de constater que c'est en matière d'assurances paramétriques[551]

---

[543] « LaBChain, l'initiative de place lancée par la Caisse des Dépôts, dévoile son premier cas d'étude », Caisse des dépôts Groupe [en ligne], 18 juill. 2016, https://www.caissedesdepots.fr/sites/default/files/medias/cp_et_dp/cp_labchain.pdf.

[544] Conformément aux exigences de l'art. 13, VI, de la L. n° 2014-617, 13 juin 2014, relative aux comptes bancaires inactifs et aux contrats d'assurance vie en déshérence, *JORF* n° 0137, 15 juin 2014, p. 9951, texte n° 1.

[545] VERBIEST (Thibault), « Blockchain : une révolution juridique ? », art. cit., *loc. cit.* ; BIGOT (Rodolphe), « La blockchain et l'assurance, la blockchain ou l'assurance ? », *RLDI* 2017/11, n° 142 ; DELZANNO (Clémentine), « Nouveaux process pour les gestionnaires de patrimoine », *Dr. & patr. Mensuel*, 1er oct. 2016, n° 162 ; BIGOT (Rodolphe), « L'assurance, le droit et le digital : un mauvais remake du "bon, la brute et le truand" ? », *RGDA* janv. 2018, n° 115h0, p. 8 ; GRYNBAUM (Luc), LE GOFFIC (Caroline), MORLET-HAÏDARA (Lydia), *op. cit.*, nos 288 et s.

[546] BIGOT (Rodolphe), « L'assurance, le droit et le digital : un mauvais remake du "bon, la brute et le truand" ? », art. cit., *loc. cit.*

[547] GRYNBAUM (Luc), LE GOFFIC (Caroline), MORLET-HAÏDARA (Lydia), *op. cit., loc. cit.*

[548] *Id.*

[549] Il s'agit de prendre des mesures permettant de « a) Limiter temporairement l'exercice de certaines opérations ou activités, y compris l'acceptation de primes ou versements ; b) Restreindre temporairement la libre disposition de tout ou partie des actifs ; c) Limiter temporairement, pour tout ou partie du portefeuille, le paiement des valeurs de rachat ; d) Retarder ou limiter temporairement, pour tout ou partie du portefeuille, la faculté d'arbitrages ou le versement d'avances sur contrat ; e) Limiter temporairement la distribution d'un dividende aux actionnaires, d'une rémunération des certificats mutualistes ou paritaires ou d'une rémunération des parts sociales aux sociétaires ».

[550] L. n° 2016-1691, 9 déc. 2016, relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (dite « Loi Sapin 2 »), *JORF* n° 0287, 10 déc. 2016, texte n° 2, art. 49, b).

[551] L'assurance paramétrique consiste en une garantie fondée sur un indice généré par un organisme extérieur et donc indépendant, permettant une indemnisation transparente. Il en va ainsi, par exemple, des

que les projets de *smart contracts* sont, d'une manière générale, plus facilement programmables. Partant du constat que nombre d'assurés ne connaissent pas toujours le contenu exact des clauses de leur police d'assurance et, par conséquent, manquent de réclamer ou d'exercer leurs droits – en particulier à l'indemnisation en cas de retard de livraison ou de transports[552] –, la compagnie française AXA a développé et expérimenté dès septembre 2017 un système d'assurance-retard de vol entièrement automatisé[553]. Nommée « *Fizzy* » et développée en collaboration avec la *start-up* Utocat, l'application permettait un remboursement automatique des billets d'avion en cas de retard constaté[554]. Les *smart contracts* souscrits sur *Ethereum* fixaient un prix variant selon le « risque de retard », et étaient directement reliés aux bases de données des fournisseurs mondiaux de trafic aérien *Flighstats* et *Official Airline Guide* (OAG)[555]. Par conséquent, dès lors qu'un retard de plus de deux heures était observé sur *Flighstats*, le contrat s'exécutait instantanément, sans requérir de déclaration de sinistre[556], et le protocole procédait au versement de l'indemnité prévue – en général, il s'agissait du tiers du prix du billet[557]. Dans une interview, le directeur de la R&D chez AXA soulignait le fait qu' « AXA ne [décidait] plus s'il [devait] indemniser ou non le consommateur. C'est le *smart contract* dans la *blockchain* qui [déclenchait] le paiement. L'intérêt, c'est que cela [apportait] de la confiance au consommateur »[558]. Après une centaine d'assurés indemnisés et des projets de déploiement dans d'autres secteurs des transports[559], AXA a décidé au bout de deux

polices d'assurances basées sur des indices météorologiques qui, en pratique, prennent en compte des données satellites de haute précision de mesure de l'humidité.

[552] BARBRY (Éric), art. cit., p. 80.

[553] « AXA se lance sur la Blockchain avec fizzy », *AXA* [en ligne], 13 sept. 2017, https://www.axa.com/fr/newsroom/actualites/axa-se-lance-sur-la-blockchain-avec-fizzy.

[554] Pour une analyse détaillée sur cette technologie, *infra* n° 54.

[555] THEVENIN (Laurent), « Assurance : les premières offres fondées sur la blockchain font leur apparition », *Les Echos* [en ligne], 18 sept. 2017, https://www.lesechos.fr/18/09/2017/lesechos.fr/030578479297_assurance---les-premieres-offres-fondees-sur-la-blockchain-font-leur-apparition.htm.

[556] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., n° 25 ; CUNY (Delphine), « Retard d'avion : Axa lance une assurance automatique sur la Blockchain », *La Tribune* [en ligne], 14 sept. 2017, https://www.latribune.fr/entreprises-finance/banques-finance/retard-d-avion-axa-lance-une-assurance-automatique-sur-la-blockchain-750202.html : « L'assuré n'a pas de justificatif à fournir, il sait à l'avance la somme qui lui sera remboursée (en fonction du dommage qu'il a souhaité garantir à la souscription), le prix de la police est calculé en fonction du risque de retard (d'après les statistiques), tandis que l'assureur n'a pas de déclaration de sinistre à traiter. Le remboursement est instantané sur le compte de la carte bancaire qui a servi au paiement du billet. »

[557] RAYNAL (Juliette), « Axa lance une assurance contre les retards d'avions avec la blockchain Ethereum », *L'Usine Digitale* [en ligne], 18 sept. 2017, https://www.usine-digitale.fr/article/axa-lance-une-assurance-contre-les-retards-d-avions-avec-la-blockchain-ethereum.N588233.

[558] THEVENIN (Laurent), art. cit.

[559] « AXA se lance sur la Blockchain avec fizzy », art. cit. ; VITARD (Alice), « Axa arrête Fizzy, son assurance contre les annulations et retards d'avion utilisant la blockchain », *L'usine digitale* [en ligne], 8 nov. 2019, https://www.usine-digitale.fr/article/axa-arrete-fizzy-son-assurance-contre-les-annulations-et-retards-d-avion-utilisant-la-blockchain.N902129.

ans d'interrompre l'expérimentation[560]. 11 000 polices ont été souscrites la première année, cependant, bien que ces hypothèses n'aient pas été confirmées par la compagnie, il semble que cette dernière n'ait pas atteint le retour sur investissement escompté à raison d'une « commercialisation plus difficile qu'envisagée » d'un produit novateur[561]. Dans son rapport « *Predicts 2019 : Future of Supply Chain Operations* », Gartner évaluait d'ailleurs une évolution croissante des offres en matière de *blockchain* jusqu'en 2021, évoquant un effet d'obsolescence rapide pour les projets mis précocement sur le marché[562].

C'est sur le même support que l'assureur Allianz s'est appuyé pour réaliser des expérimentations dans le cadre des obligations catastrophes (*cats bonds*)[563] en cas de catastrophes naturelles[564]. Le protocole *Allianz Risk Transfer* (ART) exécute automatiquement les transferts d'argent convenus entre les parties dès lors qu'un évènement remplit les conditions prédéfinies au sein du contrat[565]. La compagnie estime qu'en plus d'accroître la négociabilité des obligations catastrophes, le traitement transactionnel et le règlement entre assureurs et investisseurs seront considérablement accélérés et simplifiés[566].

55. Au-delà des solutions d'exécution automatisées proposées par les assureurs, certains acteurs réfléchissent à réinstaurer le lien de confiance dans les assurances à travers des systèmes d'assurances P2P autonomes et décentralisés, prenant la forme de

---

[560] V., https://fizzy.axa/ : « Désolé, mais l'expérience fizzy est terminée ! Les polices achetées en amont restent bien sûr valides. Nous tenons à vous remercier pour ces 3 années et pour tout ce que nous avons appris à vos côtés. L'équipe fizzy passe à autre chose mais nous nous reverrons bientôt. »

[561] RAYNAL (Juliette), « Clap de fin pour Fizzy, l'application phare d'Axa dans la Blockchain », *La Tribune* [en ligne], 8 nov. 2019, https://www.latribune.fr/entreprises-finance/banques-finance/assurance/clap-de-fin-pour-fizzy-l-application-phare-d-axa-dans-la-blockchain-832676.html.

[562] PRADHAN (Alex), STEVENS (Andrew), TITZE (Christian) *et al.*, « Predicts 2019 : Future of Supply Chain Operations », *Gartner* [online], 29 Nov. 2018, https://www.gartner.com/en/documents/3894387/predicts-2019-future-of-supply-chain-operations ; COSTELLO (Katie), « Gartner Predicts 90 % of Current Enterprise Blockchain Platform Implementations Will Require Replacement by 2021 », *Gartner* [online], 3 Jun. 2019, https://www.gartner.com/en/newsroom/press-releases/2019-07-03-gartner-predicts-90--of-current-enterprise-blockchain.

[563] Les obligations dites catastrophes ou « cats » sont des instruments financiers qui transfèrent un ensemble spécifique de risques – en règle générale, il s'agit des risques de catastrophe naturelle – d'un assureur aux investisseurs ou à d'autres assureurs, en fonction de conditions se déclenchant selon des paramètres définis. En pratique, l'assureur conclue un contrat en vertu duquel plusieurs parties assument le risque financier de certains événements en investissant. Si un évènement se produit et répond aux critères de déclenchement prédéfinis, les investisseurs perdent tout ou partie du capital qu'ils ont investi. Dans le cas contraire, ils reçoivent des intérêts sous forme de paiement périodique, ainsi que le retour de leur investissement principal à l'échéance du contrat.

[564] V., https://www.agcs.allianz.com/about-us/digital-transformation-and-insurance/blockchain.html, About Us > Digital Transformation > Embracing Blockchain Technology.

[565] *Id.*

[566] « Blockchain technology successfully piloted by Allianz Risk Transfer and Nephila for catastrophe swap », Allianz [online], 15 Jun. 2016, https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/migration/media/press/document/Press_Release_ART_Blockchain_pilot_final.pdf.

coopératives d'assurés organisés en réseaux de consommateurs. Autrement dit, le système serait géré par et pour les assurés.

B. Affranchir les systèmes traditionnels de mutualisation des risques à travers les assurances P2P

56. Entre encouragements à l'utilisation des possibilités de dématérialisation de la relation avec le client et concepts d'assurances décentralisées et distribuées. Le législateur encourage la dématérialisation dans le secteur de l'assurance, en particulier avec l'ordonnance n° 2017-1433 du 4 octobre 2017, relative à la dématérialisation des relations contractuelles dans le secteur financier[567], en arguant la nécessité de « favoriser, *via* un cadre juridique rénové, la pleine exploitation du potentiel des supports numériques et outils de dématérialisation, qui sont de nature à améliorer, faciliter et fluidifier les échanges entre les organismes du secteur financier et leurs clients »[568]. Des *start-ups* tentent toutefois de s'affranchir du cadre traditionnel majoritairement opaque en créant des systèmes assurantiels en P2P. La *blockchain* deviendrait donc un outil de contractualisation et de mutualisation transparente des risques directement entre assurés.

C'est, par exemple, sur ce principe, que s'est appuyée la *start-up* californienne (USA) Lemonade Insurance, pour mettre à disposition de ses clients une solution d'assurance habitation, responsabilité civile et dommages aux biens P2P[569]. Bénéficiant de la rapidité de la *blockchain*, *Lemonade* permet de souscrire une assurance en moins d'une minute, et être indemnisé en moyenne en trois minutes[570]. Fondée sur des *smart contracts*, l'application rassemble les primes mensuelles versées par les assurés afin de les reverser en cas de réclamation, dès lors que les conditions des contrats d'assurance sont remplies[571]. 20% de ces primes sont retenus par Lemonade Insurance pour la gestion et notamment pour souscrire de son côté des contrats de réassurance destinés à garantir le

[567] Ord. n° 2017-1433, 4 oct. 2017, relative à la dématérialisation des relations contractuelles dans le secteur financier, *JORF* n° 0233, 5 oct. 2017, texte n° 21, prise sur le fondement de l'art. 104 de la L. n° 2016-1321, 7 oct. 2016, pour une République numérique, *JORF* n° 0235, 8 oct. 2016, texte n° 1, donnant habilitation au gouvernement de prendre les mesures concernant les supports dématérialisés se substituant aux documents écrits sur support papier.

[568] Rapp. au Président de la République relatif à l'ord. n° 2017-1433, 4 oct. 2017, relative à la dématérialisation des relations contractuelles dans le secteur financier, *JORF* n° 0233, 5 oct. 2017, texte n° 20.

[569] TEQUI (Clément), HIAULT (François), DELLA CHIESA (Martin), *Blockchain : Vers de nouvelles chaines de valeur*, éd. Eyrolles, 2019, pp. 231-232.

[570] https://www.lemonade.com/, Home > Policy 2.0.

[571] TURCOTTE (Michel), « L'assurance sans assureur ou le P2P », Assurances et gestion des risques / Insurance and Risk Management [en ligne], 84 (n°s 1-2), 2017, p. 83, https://www.erudit.org/fr/revues/agr/2017-v84-n1-2-agr03256/1041821ar.pdf.

système en cas de réclamations importantes[572]. Les *smart contracts* assurant la gestion du capital des primes collectées sont programmés pour, chaque fin d'année, transférer la part du capital non utilisée à des associations caritatives[573]. De cette manière, il s'agit pour la *start-up* de dissuader la fraude par l'existence d'une cause sociale[574].

De la même manière, les *start-ups* Guevara au Royaume-Uni[575] et Friendsurance en Allemagne[576], proposent à leurs clients de mutualiser leurs primes afin de réduire leur montant et de rembourser annuellement les primes excédentaires, à condition pour les assurés de Friendsurance de n'avoir eu aucun sinistre à déclarer[577]. Depuis 2015, 90% des utilisateurs de la plateforme *Guevara* ont ainsi pu réduire leurs primes d'assurance automobile[578].

Il en va ainsi également d'*InsurChain* de XLAB Foundation LTD., une application singapourienne de micro-assurances à la demande, flexible et instantanée, et d'indemnisation automatique *via smart contracts*[579]. Les canadien et français Deloitte et Sratumn se sont fondés sur le même concept pour créer leur plateforme *LenderBot*. Cette dernière permet plus spécifiquement de garantir entre assurés chaque utilisateur/emprunteur à l'occasion du prêt ou de la location d'objets tels que des appareils photo, smartphones, tablettes, etc., avec un paiement et une indemnisation automatisés avec LemonWay[580].

À l'instar de *Fizzy*, la plateforme américaine *INsurETH* est basée sur le protocole *Ethereum* pour fournir une assurance de retard et d'annulation de vols à déclaration et indemnisation automatiques à partir des primes versées pour chaque contrat conclu sur la chaîne[581].

Jusqu'en 2018, la *start-up* française Inspeer.me mettait à disposition un mécanisme de mutualisation des franchises d'assurances automobiles, relatives aux

---

[572] https://www.lemonade.com/, Home > Legal Stuff.
[573] *Id.*
[574] TEQUI (Clément), HIAULT (François), DELLA CHIESA (Martin), *op. cit.*, *loc. cit.*
[575] https://heyguevara.com/.
[576] https://www.friendsurance.com/.
[577] *Id.*
[578] Terry (Hugh), « Guevarra Peer to Peer car insurance », *The Digital Insurer* [online], 2017, https://www.the-digital-insurer.com/dia/guevara-peer-to-peer-car-insurance/.
[579] V., le livre blanc de l'application, « InsurChain: A Decentralized Insurance Blockchain Ecosystem », *github* [online], 19 Sept. 2018, https://github.com/InsurChain/whitepaper/blob/master/en/whitepaper_en.md ; http://www.insurchain.org/.
[580] « Deloitte partners with Stratumn and presents a micro-insurance proof-of-concept built on the blockchain », *Stratumn* [online], 5 Jul. 2016, https://www.stratumn.com/press/deloitte-partners-with-stratumn-and-presents-a-micro-insurance-proof-of-concept-built-on-the-blockchain/ ; MERTZ (Victor), « Lemon Way s'allie avec Deloitte et Stratumn pour démocratiser la micro-assurance via la blockchain », *Lemonway* [en ligne], 22 sept. 2016, https://www.lemonway.com/fr/communiques/lemon-way-deloitte-stratumn-lenderbot-democratiser-micro-assurance-via-blockchain/.
[581] FELL (Grace), « The 4 Insurtech Blockchain Disruptors To Know », *Foresight Factory* [online], 15 Jun. 2017, https://www.foresightfactory.co/2017/06/15/4-insurtech-blockchain-disruptors-know/.

dommages, à la responsabilité, à la location de batterie et au remorquage, pour les véhicules électriques au sein d'une communauté d'assurés[582]. Anciennement InsurePal, la *start-up* slovène VouchForMe propose un système comparable de mutualisation des franchises en cas de sinistre en matière d'assurance automobile, bien que la plateforme ne mutualise les risques qu'entre membres d'un même réseau (famille et amis). Fondée sur un objectif de société auto-régulée et responsable, le montant de la prime d'assurance repose sur l'obtention d'une « preuve sociale » (*Social Proof*) de fiabilité, évaluée par le biais d'un système de notation par les pairs (*Social Proof Trustcore*)[583]. L'indemnisation d'une franchise est ensuite répartie entre assurés d'un même groupe social, au prorata des primes de chacun[584].

57. Vers une complète autonomie dans la gestion du risque ? Le recours à la DAO et à la responsabilisation vis-à-vis du groupe. Certaines *start-ups* ont décidé de poursuivre l'expérimentation dans l'objectif d'aboutir à une complète gestion par les assurés et ainsi former des coopératives d'assurés. Ce modèle d'assurance est fondé sur trois éléments constitutifs, à savoir, une plateforme de produits d'assurance, des utilisateurs à la fois associés et bénéficiaires de ces produits, et aucun intermédiaire. Pour gérer une telle plateforme mettant à disposition des mécanismes quasi-autonomes de gestion des imprévus[585] et associant les participants aux décisions, les assurés ont eu recours à une forme de *smart contracts*[586], les DAO (*Decentralized Autonomous Organizations*). Programmées dans un objectif assurantiel, ces organisations fonctionnent comme des entités autonomes au sein de la *blockchain* et *a fortiori* sans aucune personnalité ni aucun statut juridique exprès. Elles peuvent être créées pour mettre en place un groupement d'associés sur le modèle P2P, dont les modalités de fonctionnement sont inscrites directement dans le protocole de la *blockchain*. Volontairement décentralisée, aucun organe central ne contrôle la chaîne, ce qui garantit aux assurés la sécurité d'une maîtrise collective. De manière générale, en tant que système orienté vers une réalisation collaborative et coopérative, des mécanismes de vote sont programmés afin de permettre à la communauté d'assurés de modifier, *via* un consensus collectif, les

[582] BASSANI (Joël), « Inspeer.me et l'assurance collaborative affinitaire », *jinnbee* [en ligne], 24 janv. 2018, https://insurtechs.jinnbee.com/inform/inspeer-me-assurance-collaborative-affinitaire-1334/.
[583] TEQUI (Clément), HIAULT (François), DELLA CHIESA (Martin), *op. cit.*, *loc. cit.*
[584] https://vouchforme.co/.
[585] Blockchain France, « Blockchain et assurances », *Blockchain France* [en ligne], 17 févr. 2016, https://blockchainfrance.net/2016/02/17/assurances-et-blockchain/.
[586] Définition *supra* n° 42.

règles en cours de fonctionnement[587]. Sous réserve des règles propres à chaque DAO, les primes collectées auprès des assurés sont automatiquement versées au solde d'un capital global représentant les fonds disponibles de la DAO[588]. Le montant des primes est ainsi directement fonction du besoin en capital disponible et donc du comportement de chacun[589], ce qui pourrait inciter à une plus grande responsabilisation des membres. À la différence des compagnies d'assurances classiques et des *start-ups* supervisant des mécanismes d'assurance P2P précédemment présentées, les utilisateurs – à la fois associés et assurés – peuvent également décider collectivement du versement ou non des indemnisations, au cas par cas, après examen des preuves du sinistre. Ainsi, dès qu'une indemnisation est validée, celle-ci est transférée au bénéficiaire à partir du capital commun de la DAO. Étant donné que l'utilisation d'une DAO entraîne irrémédiablement un allègement des frais de structure et d'administration, les assurés peuvent prévoir, dans le *smart contract* de l'organisation, de redistribuer automatiquement à chaque fin d'année contractuelle la part de capital non-utilisée[590]. Prenant la forme d'un avantage économique individuel, cette dernière fonction représente souvent une garantie supplémentaire de fiabilité.

Contrairement aux offres d'assurances P2P « basiques », seules quelques initiatives de DAO appliquées au secteur assurantiel sont aujourd'hui proposées sur le marché.

C'est, par exemple, sur ce support, que s'est appuyée la plateforme *open source* non-lucrative française wekeep.io pour proposer un système d'auto-assurance, à la fois financé par les primes des assurés et géré par chacun d'entre eux au sein de « groupes de mutuelles », remboursant annuellement les surplus de primes nommés « gains du contrat »[591]. En cas de sinistre, les *smart contracts* vérifient que les conditions de garantie prédéfinies sont remplies et soumettent, le cas échéant, l'indemnisation au vote du groupe correspondant[592]. Les *start-ups* russe et britannique Teambrella et Nexus Mutual[593] sont fondées sur un modèle assurantiel similaire. Teambrella, par exemple, met à disposition, au Pérou, aux Pays-Bas, en Argentine et en Allemagne, une plateforme d'assurance P2P autonome permettant de mutualiser les risques et de décider des indemnisations par

[587] HONIGMAN (Philippe), « Qu'est-ce qu'une DAO ? », *Ethereum France* [en ligne], 9 juill. 2019, https://www.ethereum-france.com/quest-ce-quune-dao/.
[588] FERRON (Antoine), SAUZADE (Adrien), « Blockchain », *Institut des actuaires* [en ligne], 15 mars 2017, p. 34, https://www.institutdesactuaires.com/global/gene/link.php?doc_id=9971&fg=1.
[589] WALTZ-TERACOL (Bélinda), « Blockchain et assurance : entre mythe et désillusion », *RGDA* nov. 2019, n° 116x8, p. 5.
[590] FERRON (Antoine), SAUZADE (Adrien), art. cit.
[591] *Id.*
[592] *Id.*
[593] https://nexusmutual.io/.

équipe (*teams*) en matière de dommages aux vélos et aux animaux, et prochainement d'assurance pour animaux de compagnie aux États-Unis et d'assurance automobile en Russie [594]. En pratique, les équipes s'accordent au préalable sur les conditions générales des polices d'assurance et, en cas de sinistre, les membres procèdent à un vote pour accorder ou non le paiement et déterminer son plafond[595].

La *start-up* américaine Dynamis permet pour sa part aux petites entreprises, *via* une offre d'assurance chômage complémentaire entièrement autonome, de mutualiser le versement des indemnités en cas de licenciement ou de démission de leurs employés[596]. La *dApp* dédiée, *Dynamisapp*, permet aux entreprises participantes de programmer le versement des primes au solde du capital de la DAO, qui crée automatiquement des comptes au nom de chacun de leurs employés sous la forme de *smart contracts* individuels[597]. En fonction du nombre de réclamations, les primes peuvent diminuer avec le temps[598]. Reliée au réseau professionnel *LinkedIn*, et *a fortiori* aux profils renseignés par leurs clients, *Dynamisapp* est informée dès qu'un changement de statut d'emploi survient et, en cas de licenciement, les salariés perçoivent directement leurs indemnités, sans l'intervention d'un organe central[599].

58. Un état des lieux de l'assurance P2P. Certains auteurs soulignent que, si les règles de fonctionnement de la technologie ont la faculté d'optimiser de nombreux processus et polices d'assurance, cette faculté serait limitée[600]. D'après eux, les polices d'assurance jugées complexes, à savoir celles concernant « la responsabilité civile professionnelle, [la] responsabilité civile produits, [les] contrats d'assurance dommages et pertes d'exploitation industriels ou tertiaire », « ne sauraient être entièrement automatisées par le biais de *smart contracts*, car ils peuvent nécessiter une appréciation et/ou une prise de décision » qu'il est impossible, en l'état de l'art, de programmer[601].

Force est de constater qu'il découle, malgré tout, de ces différentes initiatives une multitude de bénéfices. La désintermédiation permise par la technologie s'accompagne en effet d'une réduction des coûts de gestion, donc des tarifications, et d'une amélioration

---

[594] https://teambrella.com/.
[595] *Id.*
[596] TERRY (Hugh), « Dynamis – Ethereum-Based DAO for Distributed P2P Insurance », *The Digital Insurer* [online], 2016, https://www.the-digital-insurer.com/dia/dynamis-ethereum-based-dao-for-distributed-p2p-insurance/.
[597] *Id.*
[598] FERRON (Antoine), SAUZADE (Adrien), art. cit., p. 35.
[599] V., http://www.dynamisapp.com/ ; https://www.civic.com/ ; HUCKSTEP (Rick), « Dynamis – If Insurance, Then Blockchain », *The Digital Insurer* [online], 3 Mar. 2016, https://www.the-digital-insurer.com/blog/insurtech-dynamis-if-insurance-then-blockchain/.
[600] DENIS (Bénédicte), HEGEDUS (Orsolya), LAREDO (Anne), SOLERANSKI (Louis), art. cit.
[601] *Id.*

de la transparence des opérations. Plus encore, les *smart contracts*, et en particulier lorsqu'ils sont organisés en DAO, ne sont programmées pour collecter les primes que pour améliorer la situation des assurés et leur permettre de se prémunir contre les risques, sinon de payer les pertes. Alors que le défaut de confiance entre souscripteurs représente l'un des premiers risques que l'assureur traditionnel est amené à maîtriser, les diverses qualités de la technologie *blockchain*, notamment sa neutralité et son immuabilité, pourraient lui permettre de réinstaurer le lien de confiance dans les assurances tout en s'affranchissant de son caractère impératif[602], pour une re-concentration sur la personne de l'assuré[603]. Mais, ces qualités seront-elles suffisantes ?

Quid en effet des informations erronées ou frauduleuses ? Une auteure constate en ce sens qu'une DAO d'assurés ne peut prospérer « qu'en présence d'assurés en nombre limité, car pour qu'il y ait une confiance réciproque entre eux il faut qu'ils se connaissent »[604]. Cependant, un tel système aspirant à une application à tous types de polices d'assurance doit être en mesure de garantir chaque demande d'indemnisation, y compris pour des risques importants. Or, à défaut d'augmenter le montant des primes, une DAO devra, pour détenir une capacité financière suffisante, ouvrir son offre à un nombre plus importants d'assurés[605]. Le système collaboratif parviendra-t-il à surmonter cet obstacle ?

59. Limites réglementaires et défis futurs. Bien que le législateur préconise de « [privilégier] aussi souvent que possible la possibilité de dématérialisation de la relation avec le client, sauf opposition de sa part »[606], un double obstacle s'élève face aux assurances P2P. Il s'agit, d'une part, du cadre strictement fixé par les autorités concernant les obligations légales d'assurance[607] et, d'autre part, de la nécessité d'obtenir un agrément pour pouvoir exercer, du moins, en France et dans toute l'UE, des opérations d'assurance[608]. Plus encore, il convient d'après certains auteurs de se demander si les systèmes de *partage* – et non de *transfert* – du risque inhérents aux assurances P2P fondées sur des DAO, qui constituent des entités sans personnalité juridique,

[602] *Id.*
[603] Blockchain France, « Blockchain et assurances », art. cit.
[604] WALTZ-TERACOL (Bélinda), « Blockchain et assurance : entre mythe et désillusion », art. cit.
[605] MAYAUX (Luc), « Voyage au pays de l'assurance collaborative », *RGDA* juin 2017, n° 114r3, p. 337.
[606] Rapp. au Président de la République relatif à l'ord. n° 2017-1433, préc.
[607] Par exemple, concernant l'assurance obligatoire s'appliquant aux propriétaires de véhicules automobiles, v., C. route, art. L. 424-1 et L. 424-2 ; C. pén., art. D. 45-3 à D. 45-21 ; C. ass., art. L. 211-4 à L. 211-7. – V. également, les règles propres à l'assurance conclue à distance, GRYNBAUM (Luc), LE GOFFIC (Caroline), MORLET-HAÏDARA (Lydia), *op. cit.*, n°s 288 et s.
[608] C. assur., L. 321-1 ; C. mut., art. R. 211-2 ; CSS, art. L. 931-4. – V. également, VERBIEST (Thibault), « Blockchain : une révolution juridique ? », art. cit., *loc. cit.*

correspondent à ce que la définition traditionnelle entend par « assurance »[609]. Pourtant, le problème semble davantage concerner la qualification des parties à la DAO, et en particulier de distinguer le « professionnel/entreprise régi(e) par le code des assurances » des « consommateurs », celle-ci donnant lieu à l'application des régimes de protection notamment introduits en droit de la consommation pour la conclusion des contrats à distance (C. consom., art. L. 211-1, L. 222-1 et s.).

Par conséquent, les projets actuels d'assurances collaboratives n'en sont qu'à leurs balbutiements et constituent un nouveau champ d'investigation juridique. Alors que d'après certains auteurs, l'émergence de modèles d'assurance P2P entièrement décentralisés est, en raison de leurs propres limites, très peu probable[610], d'autres constatent qu'ils pourraient se développer massivement dans le domaine des assurances facultatives[611]. Le succès rencontré par les différentes initiatives évoquées témoigne du potentiel de la technologie à améliorer les rapports entre les assurés et leurs systèmes d'assurance, mais il sera essentiel pour les acteurs du secteur de parvenir à identifier les potentielles failles tant juridiques que techniques avant tout déploiement. Par exemple, *quid* de l'assuré qui déclarerait un sinistre alors que le solde du compte commun de la DAO serait vide ? Cette interrogation fait partie de celles qui ont mené certains acteurs, tel que la *start-up* Otherwise, DAO proposant une « complémentaire santé collaborative »[612], à collaborer avec les assureurs traditionnels afin d'enrichir leurs offres respectives. Ainsi confronté à l'émergence de ces nouveaux acteurs de l'économie collaborative décentralisée, BNP Paribas manifeste son intérêt pour les demandes de transparence et de participation active au processus de mutualisation de ses clients[613]. Tout en alimentant le mécanisme de sa stabilité financière en cas de sinistres importants, l'entreprise a délégué une partie de ses processus opérationnels au sein d'un système collaboratif d'assurance[614].

Il s'agira donc pour ces nouveaux acteurs du secteur assurantiel de réussir à cibler les offres commercialisables et réellement vectrices de confiance, de la souscription à l'indemnisation[615].

---

609 V., notamment, MAYAUX (Luc), art. cit. ; GRYNBAUM (Luc), art. cit., *loc. cit.* ; WALTZ-TERACOL (Bélinda), art. cit.
610 TURCOTTE (Michel), art. cit. ; BIGOT (Rodolphe), « La blockchain et l'assurance, la blockchain ou l'assurance ? », art. cit.
611 DENIS (Bénédicte), HEGEDUS (Orsolya), LAREDO (Anne), SOLERANSKI (Louis), art. cit.
612 https://otherwise.fr/.
613 BERGER (Raphaël), « Otherwise : le premier courtier d'assurance collaboratif », *BNP Paribas* [en ligne], 17 nov. 2016, https://group.bnpparibas/actualite/otherwise-premier-courtier-assurance-collaboratif.
614 *Id.*
615 DENIS (Bénédicte), HEGEDUS (Orsolya), LAREDO (Anne), SOLERANSKI (Louis), art. cit.

60. Par ailleurs, l'avancée technologie permise avec les objets connectés et/ou intelligents a contribué ces dernières années à profondément renforcer l'efficacité des processus opérationnels des polices d'assurance[616]. Il s'avère que l'alliance de la technologie *blockchain* et de ces objets pourrait étendre leurs capacités respectives d'application et permettre, d'une manière générale aux relations contractuelles, de renforcer davantage la force donnée aux obligations consenties. De nouvelles opportunités s'ouvrent pour le juriste.

[616] *Id.* ; KEMP (Leanne), préc., p. 2.

Chapitre 2. Amplifier l'efficacité de la force contractuelle : l'interconnectivité comme mise à exécution instantanée

61. Les interactions, d'une part, entre machines et, d'autre part, entre la machine et l'Homme, tiennent une place de plus en plus importante et offrent de nouvelles possibilités d'expérimentation du monde environnant. Poursuivant son office de « *trust machine* »[617], l'exécution automatique proposée par la *blockchain* a ainsi tout à gagner à une interconnexion des technologies. Appliquée aux relations contractuelles, cette interactivité pourrait imprégner les contrats des bénéfices que les entités retirent les unes des autres.

C'est donc en investissant un nouvel environnement que la « *blockchain* des objets » – issue d'une combinaison de la technologie des *smart contracts* et des technologies de l'univers de l'IoT (*Internet of Things*, ou Internet des Objets (IdO)) – édifie un pont entre monde physique et monde virtuel (Section 1), de sorte que la réactivité, la simplicité et la fluidité découlant de son utilisation ont pour effet de renforcer de manière dynamique la force du contrat. Mais il s'agira également de constater que cette interconnexion de technologies opère une mutation des interactions entre l'Homme et la machine, ce qui a pour effet de transformer les relations contractuelles traditionnelles en relations fondées sur un ensemble d'interactions diverses entre machines, et entre l'Homme et les machines (Section 2).

Section 1. Une combinaison de technologies : connexion entre mondes physique et virtuel

62. Avant d'évaluer les apports mutuels d'une interconnexion de dispositifs ou équipements électroniques et de *smart contracts* (§ 2), il convient d'en appréhender la nature technique par une présentation des notions et technologies associées au projet de « *smart contract* 2.0 » (§ 1).

[617] « The promise of the blockchain: The trust machine », *The Economist* [online], 31 Oct. 2015, https://www.economist.com/leaders/2015/10/31/the-trust-machine.

§ 1. Présentation des notions et technologies du projet « *smart contract* 2.0 »

63. Les notions d'objets « intelligents », « connectés » et « communicants », définies par certains auteurs comme l' « apparence concrète et séductrice de ce qui pourrait n'être qu'une surenchère commerciale, devançant la réalité technologique »[618], et celle de l'IoT, sont intimement liées les unes aux autres. Il s'agira d'abord de présenter le fonctionnement de ces dispositifs électroniques dotés de capacités de perception de l'environnement, d'auto-adaptation et de communication (A), avant d'évoquer les systèmes d'interconnexion existants, en particulier l'IoT, les systèmes *Machine to Machine* (M2M), et les Oracles de la technologie *blockchain* (B).

A. Fonctionnement des dispositifs de perception de l'environnement, d'auto-adaptation et de communication

64. Le dispositif électronique doté de capacités de perception de son environnement, d'auto-adaptation, voire d'action sur le réel. Selon la Commission Nationale de l'Informatique et des Libertés (CNIL), un objet « intelligent » correspond à « l'adjonction de trois capacités : des capteurs, de la puissance de calcul et des communications réseau »[619]. Cette définition n'est toutefois pas suffisante pour appréhender l'étendue des fonctionnalités de la technologie dite « intelligente ». D'autant plus que, comme le constate Nathalie Nevejans, « un objet peut être intelligent sans être connecté, et un objet connecté peut parfaitement ne pas être intelligent »[620]. L'auteure suggère notamment de prêter attention aux attributs fonctionnels permettant au dispositif ou à l'équipement électronique de percevoir son environnement et de s'y adapter de lui-même[621]. Elle précise d'ailleurs que si le dispositif électronique est doté d'une « architecture, c'est-à-dire d'articulations lui donnant une structuration et lui permettant d'agir dans le réel en recevant les différents organes, on passe plutôt à la catégorie

[618] PRIVAT (Gilles), « Des objets communicants à la communication ambiante », *Les Cahiers du numérique*, 2002/4, vol. 3, pp. 23-44.
[619] CNIL, *Rapport d'activité de 2015*, éd. La Documentation Française [en ligne], 2016, p. 84, https://www.cnil.fr/sites/default/files/atoms/files/cnil-36e_rapport_annuel_2015_0.pdf.
[620] NEVEJANS (Nathalie), « Une introduction juridique à l'Objet Intelligent », communication au colloque « L'objet intelligent : normes, usages et responsabilités » de l'Institut d'électronique et des Systèmes (Université de Montpellier R 5214) et l'Unité Dynamiques du droit (Université de Montpellier R 5815) – Centre National de la Recherche Scientifique, Montpellier, Université de Montpellier, non publié, 6 nov. 2015.
[621] *Id.*

"robot" »[622]. Il apparaît ainsi que le robot dispose de caractéristiques techniques supplémentaires, de sorte que le qualificatif de « robot » représenterait le *summum* de l'objet « intelligent ». Dans son *Traité de droit et d'éthique de la robotique civile*, Nathalie Nevejans propose une définition générale du robot[623]. Pour constituer un robot, six conditions fondamentales doivent selon l'auteure être cumulativement remplies par la machine, à savoir, une existence matérielle (ou physique)[624], une alimentation en énergie[625], une capacité à agir sur le réel[626], une capacité de perception de son environnement[627], une capacité de décision[628], et enfin une capacité d'apprentissage – dont le premier niveau correspond à la programmation de la machine par le spécialiste[629]. Cette définition suggère en outre une certaine rigueur dans le processus de qualification. En effet, un dispositif ou un équipement électronique peut être considéré comme étant un robot, mais la catégorie des robots en tant que telle n'inclut pas nécessairement les objets dotés de fonctionnalités dites « intelligentes », ou à tout le moins dotés d'attributs de perception de leur environnement et d'auto-adaptation. Force est de constater que, dans l'univers de la robotique, il est finalement difficile de « proposer une définition […] qui constitue un outil manipulable par le droit, tout en conservant une pertinence scientifique »[630].

En ce qui concerne la *blockchain*, il apparaît qu'au-delà de la question de la qualification du dispositif électronique, l'interconnexion opérée par le projet de « *blockchain* des objets » nécessite surtout des technologies dotées de facultés de perception de l'environnement et d'action sur le réel – ce qui supposerait qu'elles soient capables d'analyser les données recueillies et finalement d'agir en conséquence.

Il est donc essentiel qu'elles disposent de capteurs, c'est-à-dire « des organes sensoriels [leur] permettant de percevoir [leur] environnement »[631], soit l'équivalent en robotique d'attributs consistant à « construire une représentation du monde physique à partir de données perçues »[632] ou encore à « détecter et [à] enregistrer des signaux

[622] *Id.*
[623] NEVEJANS (Nathalie), *Traité de droit et d'éthique de la robotique civile*, éd. LEH éditions, coll. Science, éthique et société, 2017, pp. 100-131.
[624] *Ibid.*, pp. 101-109.
[625] *Ibid.*, pp. 109-115.
[626] *Ibid.*, pp. 115-118.
[627] *Ibid.*, pp. 118-122.
[628] *Ibid.*, pp. 122-125.
[629] *Ibid.*, pp. 125-131.
[630] *Ibid.*, p. 87.
[631] NEVEJANS (Nathalie), « Une introduction juridique à l'Objet Intelligent », art. cit.
[632] « Le développement industriel futur de la robotique personnelle et de service en France », Ministère de l'économie [en ligne], p. 12, https://www.entreprises.gouv.fr/files/files/en-pratique/etudes-et-statistiques/dossiers-de-la-DGE/robotique.pdf.

physiques »[633] en fonction des informations nécessaires[634]. La CNIL indique en effet que ces capteurs peuvent être d'origines variées et reliés entre eux afin de permettre à un dispositif ou équipement électronique de prélever et de rassembler en continu un ensemble de données physiques, provenant de son environnement proche[635], à l'image de ce que sont les organes des sens chez l'homme. Un capteur peut, par exemple, mesurer la température, la luminosité, la distance, les vibrations, le bruit, le son, ou encore la pollution[636]. Une auteure précise qu'en robotique il s'agit pour la machine « d'acquérir et d'interpréter les données sur son environnement ou sur elle-même » *via* des capteurs qui les transforment ensuite « en une information, le plus souvent un signal électrique, qui est alors utilisable »[637]. Cette information peut effectivement être utilisée, soit par l'utilisateur – auquel elle est directement transmise après avoir été convertie dans une forme compréhensible[638] –, soit par la partie analyse du dispositif électronique. Dans ce dernier cas, le dispositif doit être pourvu d'un processeur exécutant une série d'instructions prédéfinies et décrites dans son algorithme[639]. Chargé avec les données captées et enregistrées en mémoire, le processeur consiste en « un circuit électronique qui exécute les instructions machine des programmes informatiques et qui effectue les opérations arithmétiques et logiques » sans intervention tierce[640]. Les décisions prises par le dispositif à la suite de l'analyse des informations transmises ne sont, cependant, que le résultat final généré à partir de l'exécution stricte du programme. Les calculs effectués par le processeur ne peuvent dépasser les limites du cadre prédéfini, en ce sens que le dispositif électronique n'a, en principe, ni capacités de raisonnement et de décision[641], ni capacités d'apprentissage en dehors de celles consistant à lui permettre de se situer dans son environnement et de s'adapter à lui sans l'intervention de l'Homme[642]. C'est la raison

---

633 « Éthique de la recherche en robotique. Rapport n° 1 de la CERNA, Commission de réflexion sur l'Éthique de la Recherche en sciences et technologies du Numérique d'Allistene », CERNA [en ligne], nov. 2014, p. 12, http://cerna-ethics-allistene.org/digitalAssets/38/38704_Avis_robotique_livret.pdf.

634 NEVEJANS (Nathalie), *Traité de droit et d'éthique de la robotique civile*, *op. cit.*, p. 120.

635 CNIL, *Rapport d'activité de 2015*, préc., p. 84.

636 BOUJAT (Gérard), ANAYA (Patrick), *Automatique industrielle en 20 fiches*, éd. Dunod, 2013, pp. 40-49.

637 NEVEJANS (Nathalie), *Traité de droit et d'éthique de la robotique civile*, *op. cit.*, pp. 119-120.

638 Pour un exemple concret d'objet intelligent, v. le fonctionnement des « montres intelligentes », GOULOUMES (Romain), « Comment marche un objet intelligent ? », *20 Minutes* [en ligne], 10 oct. 2013, https://www.20minutes.fr/magazine/secoacher-mag/2422103-20130426-comment-marche-un-objet-intelligent.

639 Définition *supra*, note 253 sous n° 11.

640 NEVEJANS (Nathalie), « Une introduction juridique à l'Objet Intelligent », art. cit. – V. également, « L'Internet des objets, ou la connexion d'objets intelligents via l'Internet ou l'Intranet », *Ciscomag*, mars 2009, n° 25 ;

641 Sur la notion d'autonomie, et la distinction entre « autonomie opérationnelle » et « autonomie décisionnelle », v., NEVEJANS (Nathalie), *Traité de droit et d'éthique de la robotique civile*, *op. cit.*, pp. 133-139.

642 Sur la notion d'apprentissage, v., « Éthique de la recherche en robotique », Rapport n° 1 de la CERNA, Commission de réflexion sur l'Éthique de la Recherche en sciences et technologies du Numérique d'Allistene [en ligne], nov. 2014, p. 44, http://cerna-ethics-

pour laquelle il s'agit davantage d'un dispositif auto-adaptatif plutôt que véritablement autonome. Une fois les données sur son environnement analysées et les instructions algorithmiques exécutées, le processeur crée un signal électrique correspondant, ordonnant au dispositif électronique de matérialiser sa décision par la production d'une action, telle qu'un mouvement.

Ce sont les actionneurs qui vont permettre au dispositif électronique d'agir dans le monde réel. C'est pourquoi il est également primordial que le dispositif en soit doté. Un actionneur est un organe chargé de convertir l'énergie en une action[643]. D'une manière relativement similaire, le § 3.1 de la norme NF EN ISO 8373 spécifiant le vocabulaire relatif aux robots et composants robotiques depuis 2012 définit la notion d'actionneur comme un « organe de puissance capable de produire un mouvement du robot ». En pratique, il s'agit le plus souvent de moteurs, de vérins, etc. Caractéristique accessoire à sa capacité d'action sur le réel, il est essentiel, pour que le dispositif puisse fonctionner sans l'intervention de son utilisateur, qu'il dispose d'une certaine autonomie énergétique, qu'elle provienne de ressources classiques ou d'une énergie auto-créée, tel que le précise la définition donnée par Nathalie Nevejans dans le domaine de la robotique[644].

C'est par exemple le cas du « robot aspirateur » de son nom commercial, qui rassemble à la fois les instructions du programme enregistré dans sa mémoire et les informations qu'il collecte *via* ses différents capteurs pour adapter sa trajectoire en fonction de son environnement et prendre des décisions préprogrammées telles que « continuer tout droit », « tourner », « faire demi-tour », se matérialisant sous la forme d'un déplacement de l'objet[645].

Au-delà des attributs fonctionnels permettant aux dispositifs de capter des données et finalement d'agir en conséquence, l'interconnexion opérée par le projet de « *blockchain* des objets » nécessite également des technologies dotées d'une capacité de communication.

65. Le dispositif électronique doté de capacité de communication des données captées. Le déploiement de l'objet dit « connecté » a été la première étape d'une succession d'évolutions du web contribuant à la création d'un monde

allistene.org/digitalAssets/38/38704_Avis_robotique_livret.pdf. – V. également, NEVEJANS (Nathalie), *Traité de droit et d'éthique de la robotique civile, op. cit.*, pp. 125-131.

643 NEVEJANS (Nathalie), « Une introduction juridique à l'Objet Intelligent », art. cit.

644 Pour plus de précisions sur la condition d'une « nécessaire source d'énergie », v., NEVEJANS (Nathalie), *Traité de droit et d'éthique de la robotique civile, op. cit.*, pp. 109-115.

645 LOCQUENEUX (Cédric), DARRIEUMERLOU (Serge), *Le guide de la maison et des objets connectés : Domotique, smart home et maison connectée*, éd. Eyrolles, 2016, p. 205.

« hyperconnecté »[646] fondé sur un objectif de « mise en relation dynamique de [multiples] entités »[647]. Tel que le souligne Nathalie Nevejans, la capacité de communication d'un dispositif électronique lui permet de « recevoir, échanger, ou diffuser des informations »[648]. L'auteure constate par ailleurs que cette interaction peut survenir tant entre un dispositif ou équipement communicant et son utilisateur, qu'entre dispositifs électroniques lorsqu'aucun humain n'intervient en tant qu'intermédiaire[649]. Dans l'état de l'art, le dispositif ou l'équipement électronique requiert le plus souvent ce qui consiste en un centre de contrôle[650], tel qu'un smartphone ou un ordinateur, qui puisse tenir lieu d'interface d'accès entre lui et l'utilisateur. Le cas échéant, se ralliant au rapport rédigé par la CNIL[651], la Commission de Régulation de l'Énergie (CRE) définit la capacité de communication comme la faculté de « communiquer avec un ordinateur, un smartphone ou une tablette via un réseau sans fil » à l'instar des réseaux Internet, *Wi-Fi*, *Bluetooth*, de téléphonie mobile, radio à longue portée de type *Sigfox* ou *LoRa*[652].

Finalement, un auteur propose une définition de l'objet communicant fondée sur quatre caractéristiques complémentaires dérivées des fonctions de traitement, de communication et d'interaction[653]. Il serait donc possible de qualifier un dispositif ou un équipement électronique d' « objet communicant » s'il intègre conjointement les capacités d'acquisition d'informations sur lui-même ou sur son environnement, de traitement et de stockage des informations collectées, d'émission des informations vers d'autres objets et, inversement, de réception d'informations transmises par d'autres objets, et enfin de réalisation d'actions en retour « sur son état physique propre, ou, le cas échéant, sur l'environnement »[654]. Partant de cette définition générale, l'auteur suggère de considérer les facultés d'interaction mais aussi et surtout de communication banalisée associée au protocole de l'objet comme étant les deux caractéristiques fondamentales à la qualification d'un dispositif ou d'un équipement électronique « communicant »[655]. En mettant l'accent sur la mise en réseau, une telle interprétation permet d'étendre son champ de qualification et d'inclure les dispositifs dotés de capacités communicantes, quel que soit leur niveau d'interaction, tels qu' « un capteur passif en réseau, ou un actionneur

[646] SCHWAB (Klaus), *La quatrième révolution industrielle*, éd. Dunod, 2017.
[647] NEVEJANS (Nathalie), *Traité de droit et d'éthique de la robotique civile*, *op. cit.*, p. 139.
[648] NEVEJANS (Nathalie), « Une introduction juridique à l'Objet Intelligent », art. cit.
[649] *Id.*
[650] CNIL, *Rapport d'activité de 2015*, préc., p. 85.
[651] *Ibid*., p. 84.
[652] CRE, « Dossier : Les objets connectés », *Smart Grids* [en ligne], 6 mars 2017, http://www.smartgrids-cre.fr/index.php?p=objets-connectes-introduction.
[653] PRIVAT (Gilles), art. cit.
[654] *Id.*
[655] *Id.*

physique trivial mais commandable en réseau, comme un interrupteur ou une ampoule ». C'est ainsi que la CRE distingue deux catégories d'objets communicants, à savoir, « les objets destinés à la collecte et l'analyse de données », et « les objets qui répondent à une logique de contrôle-commande » et qui permettent de déclencher une action à distance[656].

Un auteur constate qu'en entendant la fonction de communication au sens large, cela permet de surcroît de bénéficier de la « propriété de composabilité spontanée » propre à tout objet communicant, y compris les « objet[s] doté[s] uniquement de capacité d'interface physique en entrée et de transmission banalisée », qui leur permettent de constituer des « fédérations d'objets »[657].

B. Fonctionnement des systèmes d'interconnexion des objets

66. Relier les mondes physique et virtuel avec des données : l'interconnexion entre Internet et objets. Comme le constate une auteure, « si l'objet communicant est, par la force des choses, nécessairement connecté, il ne l'est pas forcément à Internet »[658]. Néanmoins, lorsqu'il l'est, ses attributs fonctionnels et les diverses informations qu'il capte sont mis au service d'un ensemble plus grand contribuant à créer un réseau d'objets capable de « faire le lien entre logiciel et objets »[659], et ainsi d'optimiser la relation entre monde virtuel et monde physique. L'Internet des Objets désigne la connexion des objets à un réseau plus large, local ou Internet, sans requérir l'intervention de l'utilisateur. Il peut s'agir d'une communication directe, par *Wi-Fi* par exemple. Mais il peut également s'agir d'une communication par l'intermédiaire du smartphone de l'utilisateur, exécutant, cette fois, la fonction de périphérique passerelle entre l'objet et le réseau, le plus souvent *via* une connexion *Bluetooth*, sinon par l'intermédiaire des protocoles de communication propres aux objets[660].

L'expression « *Internet of Things* » a été imaginée en 1999 au Royaume-Uni par Kevin Ashton pour qualifier le lien qui existe entre la technologie RFID (*Radio Frequency Identification*), utilisée dans de nombreux badges comportant des puces d'identification, et Internet[661], qu'il proposait d'utiliser pour optimiser la gestion de la

[656] CRE, « Dossier : Les objets connectés », préc.
[657] PRIVAT (Gilles), art. cit.
[658] NEVEJANS (Nathalie), « Une introduction juridique à l'Objet Intelligent », art. cit.
[659] *Id.*
[660] BENSOUSSAN (Alain), FORSTER (Frédéric), *Droit des objets connectés et télécoms*, éd. Bruylant, coll. Lexing - Technologies avancées & Droit, 2017, pp. 13-18.
[661] SYLVAIN (Geoffray), « [Infographie] Histoire de l'internet des objets au fil du temps », *ARUCO* [en ligne], 11 août 2014, https://aruco.com/2014/08/infographie-internet-objets/.

chaîne d'approvisionnement de l'entreprise Procter & Gamble[662]. S'agissant d'un concept en évolution constante, l'*Internet of Things* ne dispose pas d'une définition standardisée. Une majorité des auteurs s'accorde sur l'idée d'un « réseau de réseaux qui permet, *via* des systèmes d'identification électronique normalisés et unifiés, et des dispositifs mobiles sans fil, d'identifier directement et sans ambiguïté des entités numériques et des objets physiques et ainsi de pouvoir récupérer, stocker, transférer et traiter, sans discontinuité entre les mondes physiques et virtuels, les données s'y rattachant »[663]. Dix ans après sa présentation à Procter & Gamble, Kevin Ashton est revenu sur la notion d' « IoT » pour en préciser les fondements, sans prétendre néanmoins à l'uniformisation, ni du concept, ni des pratiques[664]. Il a ainsi développé les motivations et l'idée sous-jacente de l'expression IoT en soulignant que, si la structure d'Internet requiert pour fonctionner des milliards d'équipements interconnectés – incluant des serveurs, des routeurs, etc. –, l'élément essentiel demeure l'information et donc, indirectement, l'Homme[665]. Il constate toutefois que, d'une part, les données produites par l'Homme sont limitées, à la fois en termes de quantité et de qualité, et que, d'autre part, les différents capteurs des objets communicants peuvent y remédier[666]. Le principe initial était donc de mettre à disposition des systèmes informatiques des moyens de recueillir, par eux-mêmes, les informations dont ils ont besoin, afin qu'ils ne soient pas influencés par les propres limites de temps, d'attention et de précision de l'être humain. Finalement, l'IoT correspond à l'expansion d'Internet à des choses ou objets et à des lieux dans le monde physique, permettant aux objets d'évoluer en quasi-autonomie et avec des informations aussi efficaces que suffisantes.

Le dispositif ou l'équipement électronique dans l'univers de l'IoT est celui qui, lié à Internet, capte des informations, les analyse à un certain degré, souvent peu élevé, et

---

662 « Kevin Ashton : Il Ya 20 Ans Il A Inventé La Désignation "Internet Of Things" », *Territorial Challenges* [en ligne], 11 nov. 2019, https://territorialchallenges.com/2019/11/11/kevin-ashton-il-ya-20-ans-il-a-invente-la-designation-internet-of-things/84100/. – Pour plus de précisions, v., ASHTON (Kevin), « That "Internet of Things" Thing. In the real world, things matter more than ideas », *RFID Journal* [online], 22 Jun. 2009, http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf ; GERSHENFELD (Neil), KRIKORIAN (Raffi), COHEN (Danny), « The Internet of Things: The principles that gave rise to the Internet are now leading to a new kind of network of everyday devices, an "Internet-0" », *Scientific American* [online], Oct. 2014, https://www.scientificamerican.com/article/the-internet-of-things/ ; ZHANG (Ying), « Technology framework of the Internet of Things and its application », *in 2011 International Conference on Electrical and Control Engineering*, IEEE, Yichang, 16-18 Sept. 2011, pp. 4109-4112.

663 BENGHOZI (Pierre-Jean), BUREAU (Sylvain), MASSIT-FOLLEA (Françoise), *L'Internet des objets : Quels enjeux pour l'Europe*, éd. Éditions de la Maison des sciences de l'homme, coll. praTICs, 2012, pp. 15-16. – V. également, BENSOUSSAN (Alain), FORSTER (Frédéric), *op. cit.*, p. 17.

664 ASHTON (Kevin), art. cit.

665 *Id.*

666 *Id.*

les transmet, à l'image de ce que font les bracelets, montres, ampoules ou encore volets connectés.

67. De la communication des données à l'interaction entre objets. Des confusions peuvent naître concernant le système « *Machine-to-Machine* » (M2M) et la notion d'IoT. Bien qu'ils proposent chacun des « solutions d'accès à distance à des objets ou des capteurs » et qu'ils permettent des échanges d'informations entre dispositifs ou équipements communicants, la CRE souligne que le M2M consiste essentiellement en un « système fermé utilisé dans le cadre d'une tâche spécifique », alors que l'IoT est « un système libre dans lequel chaque objet est identifié et communique avec une plateforme de stockage de données, qui s'intègre dans un réseau mondial »[667]. Toutefois, plus qu'une relation d'opposition, ce sont en réalité deux approches complémentaires qui peuvent tout à fait cohabiter. D'autant plus si un objet présente tout à la fois des capacités de communication, d'interaction et d'analyse (ou traitement) des données.

68. Interconnexion entre objets et *blockchain* : l'utilisation du système d' « Oracle ». La *blockchain Bitcoin* utilise une forme rudimentaire de langage de programmation[668] nommée *Script* ou *Scripting*[669], qui lui permet d'inscrire des transactions sur les blocs de la chaîne et qui repose sur la notation postfixée[670] et, en particulier, sur la notion de pile appliquant le principe anglais « *last in, first out* » (LIFO), soit « le dernier entré, le premier sorti »[671]. Les résultats issus des opérations de *Script*

[667] CRE, « Dossier : Les objets connectés », préc.
[668] CNRTL [en ligne], v° Langage, https://www.cnrtl.fr/definition/langage : « Langage de programmation. "Langage préétabli utilisé pour écrire les programmes d'un ordinateur déterminé" (MESS. Télém. 1979). Langage symbolique. "Langage de programmation utilisant des codes mnémoniques pour représenter les instructions machines" (Informat. 1972). [Langage symbolique :] code intermédiaire entre le langage machine et les langages externes (langues naturelles ou langages documentaires), et permettant au programmeur de communiquer aisément avec l'automate. C'est pourquoi les langages symboliques sont aussi appelés langages de programmation (COYAUD, Introd. ét. lang. docum.,1966, p. 14). »
[669] Le langage spécifiquement utilisé pour *Bitcoin* est dérivé du langage *Forth*, inventé dans les années 1960 par Charles H. Moore. Il compte parmi les premiers langages de programmation à pile. – V., IBNOUHSEIN (Issam), « Programmation des blockchains et "smart contracts" », *Quantmetry* [en ligne], 31 mai 2016, https://www.quantmetry.com/single-post/2017/05/31/Programmation-des-blockchains-et-%E2%80%9C smart-contracts%E2%80%9D.
[670] Schématiquement, la notation postfixée – ou post-fixée –, appelée parfois notation polonaise inverse en comparaison à la notation polonaise (notation unaire) inventée par le polonais Jan Łukasiewicz, permet d'écrire de façon non-ambiguë les expressions arithmétiques sans avoir besoin de connaître la priorité des opérateurs, donc sans avoir besoin d'utiliser de parenthèses. Contrairement à la notation polonaise, l'opérateur est ici placé à la suite de ses opérandes (c'est-à-dire des valeurs de l'opération). À titre d'exemple : 14 + 4 (en notation infixe) s'écrit : + 14 4 (notation unaire), 14 4 + (notation postfixée). – Pour davantage de précisions sur le sujet, v., ANTONOPOULOS (Andreas M.), *Mastering Bitcoin*, ed. O'Reilly, 2nd edition, 2017, pp. 16-19.
[671] Schématiquement, ce concept ressemble à la fonction « Presse-papier » des smartphones, de sorte que lorsqu'est « copié-collé » un extrait de texte, c'est celui-ci qui apparaît en premier dans la liste du presse-

sont, par conséquent, limités à deux types de sorties (*outputs*), à savoir, « vrai » (*True*) ou « faux » (*False*). C'est la raison pour laquelle le langage de *Script* utilisé dans *Bitcoin* est « *non-Turing Complete* » ou « Turing-incomplet ». Or, lorsque l'exécution du *smart contract* ne fait appel qu'à des données inscrites au sein de la *blockchain*, la vérification est automatique et ne requiert aucune instruction spécifique. En revanche, si le contrat n'est censé s'exécuter qu'après vérification de données inscrites en dehors de la chaîne, la *blockchain* ne pourra exécuter ce type d'instruction sans l'utilisation d'un langage Turing-complet.

Le « *Turing Completeness* » est un concept mathématique qui mesure la compatibilité d'un langage de programmation. Un langage *non-Turing Complete* signifie essentiellement que le langage est conçu sans constructions complexes, telles que, par exemple, des boucles et des conditions, ce qui a pour conséquence de limiter sa capacité à créer des programmes à usage général.

En ce qui concerne *Ethereum*, la *blockchain* utilise « *Solidity* », un langage Turing-complet[672]. Cette caractéristique lui permet notamment de coder des programmes simples comme complexes[673], d'utiliser l'intégralité des fonctions calculables, mais également de traduire et reformuler n'importe quel autre langage informatique[674], et donc de pouvoir recourir à des données externes en temps réel afin de déclencher une action prédéfinie dans la chaîne de blocs. En pratique, il s'agit pour le *smart contract*, par exemple, d'obtenir une information concernant le suivi d'un colis sur un site de livraison (« Le colis *X* est en cours de livraison ; a été livré »). Il peut encore, par exemple, se connecter directement à un dispositif ou à un équipement électronique communicant pour obtenir une information spécifique récoltée par ses capteurs et mettre à jour l'état d'exécution du contrat, ou pour donner un ordre aux actionneurs, et ce, sans intervention humaine. Ce système de données externes sollicité par la *blockchain* est nommé « Oracle » par l'écosystème *Ethereum*[675]. Proche du langage *JavaScript*[676], *Solidity* est également un langage de programmation de haut-niveau[677]. Cette seconde caractéristique

papier. – V., IBNOUHSEIN (Issam), art. cit. – V. également, Annexe n° 4. Schéma simplifié du principe du langage à pile, p. 436.

672 LEE (David), CHUEN (Kuo), DENG (Robert H.), *Handbook of Blockchain, Digital Finance, and Inclusion: vol. 2:ChinaTech, Mobile Security, and Distributed Ledger*, ed. Academic Press, 2017, p. 155.

673 *Id.*

674 RODRIGUEZ (Philippe), *La révolution blockchain : Algorithmes ou institutions, à qui donnerez-vous votre confiance ?*, éd. Dunod, 2017, p. 143.

675 Pour une analyse plus détaillée de l'Oracle, *infra* n° 335.

676 *JavaScript*, ou JS, est un langage de programmation dynamique complet qui permet d'intégrer une interactivité dynamique sur les sites web. Il s'agit, par exemple, des animations web, des jeux 2D ou 3D, ou encore de la fonction permettant de remplir les champs d'un formulaire à remplir en ligne en « un clic ».

677 D'abord proposé en août 2014 par Gavin Wood puis développé par l'équipe *Solidity* du projet *Ethereum* dirigé par Christian Reitwiessner. L'équipe était notamment composée de Gavin Wood, Christian Reitweissner, Alex Beregszaszi, Yoichi Hirai et d'autres collaborateurs d'*Ethereum*.

permet à la *blockchain* de supporter la mise en œuvre d'un système dynamique d'inscription d'actes auto-exécutants[678] et donc de développer des applications adaptées à la logique « auto-application » requise par les *smart contracts* pour consolider des transactions, en particulier avec des appels d'Oracles[679]. Bien qu'il soit étiqueté comme étant un langage de « haut-niveau » – ce qui signifie en principe qu'il est facilement compréhensible par un humain et doit permettre de coder en utilisant à la fois des mots usuels des langues naturelles (l'anglais étant le plus souvent utilisé) et des symboles mathématiques familiers – *Solidity* demeure assez complexe pour les non spécialistes et demande certaines compétences en programmation.

69. Finalement, dans le cadre d'une interconnexion entre *blockchain* et objets, il s'agirait, d'une part, de donner le rôle d'Oracle à l'objet et, d'autre part, de confier à la *blockchain* la partie commande du dispositif électronique – et éventuellement l'autonomie opérationnelle de l'objet – par le biais de l'algorithme programmé d'un *smart contract*. Cela consisterait pour le processeur de l'objet à procéder à l'exécution des instructions machines à partir du programme informatique inscrit dans la chaîne de blocs dédiée[680].

§ 2. Apports réciproques entre technologies du concept « *smart contract 2.0* »

70. Force est de constater que les algorithmes d'exécution sont la clé de voûte des *smart contracts*. En incluant des dispositifs électroniques, qu'ils soient communicants et/ou dotés de capacités de perception de leur environnement, d'auto-adaptation, voire d'action sur le réel, dans la relation contractuelle, ceux-ci permettent aux *smart contracts* de disposer d'informations supplémentaires sur leur exécution, voire de déclencher une action automatique dans le monde physique sans intervention humaine, et finalement de

[678] Vitalik Buterin précise à ce sujet que « le code EVM permet d'effectuer des boucles de deux manières. Premièrement, l'instruction *JUMP* permet au programme de revenir à un point précédent dans le code, tandis que l'instruction *JUMPI* permet d'effectuer un saut conditionnel, permettant des déclarations comme w*hile x < 27 : x = x * 2.* Deuxièmement, les contrats peuvent appeler d'autres contrats, permettant potentiellement une boucle à travers la récursivité. » [Trad. : Asseth (Stéphane Roche, Jean Zundel, Frédéric Jacquot, Alexandre Kurth et Etienne Jouin), v., http://www.asseth.fr/2016/11/09/traduction-whitepaper-ethereum/], BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », *github* [liens de publication originaux supprimés] [online], Nov. 2013, https://github.com/ethereum/wiki/wiki/White-Paper].

[679] Sur le sujet, v., KAROCYT, « Introduction aux Smart Contracts », *GitHub* [en ligne], 1er juin 2017, solidity-fr > docs > introduction-to-smart-contracts.rst, github.com ; PHUC (Morgan), « Caractéristiques de Solidity », *Bit Conseil* [en ligne], 22 août 2019, https://bitconseil.fr/solidity-langage-ethereum/.

[680] Sur les notions de processeur, d'instructions machines et d'autonomie opérationnelle, *supra* n° 64.

bénéficier d'une mise à exécution matérielle instantanée (A). S'il est dans un premier temps évident que l'IoT est une opportunité de développement pour la technologie *blockchain* et les *smart contracts*, il faut pourtant remarquer que sans la *blockchain*, et en particulier sans la décentralisation qu'elle opère, il ne pourrait mettre en œuvre une interconnexion fiable et sécurisée entre les différents objets (B). C'est la raison pour laquelle l'un et l'autre sont complémentaires.

A. Une mise à exécution matérielle instantanée

71. Matérialisation de la dimension temporelle dans le contrat. Un des apports de cette association de technologies est de rendre matériellement exécutable le contenu des stipulations contractuelles[681]. En pratique, il s'agit d'initier un *smart contract* consentant un accès à la chose-objet du contrat à un instant *t*, fixé de manière précise par les parties et immuable, et retirant automatiquement et instantanément cette autorisation d'accès à un autre instant *t'*, terme extinctif prédéfini de son exécution[682]. À l'instar des verrous automatiques, permettant de verrouiller/déverrouiller l'accès à une multitude d'objets mis en location[683], cette alliance instantanéise matériellement le début et la fin de la relation contractuelle.

Nombreuses entreprises se sont spécialisées dans le domaine depuis les années 2010-2011 avec l'objectif de créer une « *Blockchain of Things* ». Il en va ainsi, par exemple, de la *blockchain* d'origine allemande *Tangle* d'IOTA[684], de *Filament* développée par la *start-up* Everywhere à Reno dans l'Oregon (États-Unis) et appliquée au secteur automobile[685], et d'*IBMWatson IoT*, un projet de l'allemand IBM[686]. Concernant ce dernier projet, IBM s'appuie sur la programmation de systèmes hybrides reliant différents objets à une *blockchain* pour proposer de multiples applications automatisant la location, la maintenance, la vente, l'achat, le réapprovisionnement, et même le partage d'objets communicants au sein d'un réseau P2P grâce à une interface

[681] HAEHNSEN (Erick), « La Blockchain part à la conquête de l'Internet des objets », *La Tribune* [en ligne], 1er févr. 2012, https://www.latribune.fr/technos-medias/la-blockchain-part-a-la-conquete-de-l-internet-des-objets-550006.html.
[682] MEKKI (Mustapha), « Blockchain : l'exemple des smart contracts », *blog mekki.fr* [en ligne], 25 mai 2018, p. 8, http://www.mekki.fr/files/sites/37/2018/05/Smart-contracts.pdf.
[683] Sur la *smart property*, *infra* nos 78 et s.
[684] POPOV (Serguei), « The Tangle : White Paper IOTA », [online], 30 Apr. 2018 (1.4.3 version), https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf ; LEHUGER (Stéphanie), « Présentation de IOTA et Tangle », *Medium* [en ligne], 21 août 2017, https://medium.com/iota-et-tangle/presentation-iota-tangle-2d6e63e3a70.
[685] https://filament.com/.
[686] https://www.ibm.com/internet-of-things.

utilisateur intuitive[687]. Il s'agirait, par exemple, d'un réfrigérateur qui, enregistrant l'absence d'un produit *y*, serait programmé pour se réapprovisionner automatiquement et en commanderait une nouvelle quantité directement auprès du commerçant désigné[688].

72. Amplification de l'effet dissuasif de la sanction automatique pour manquement contractuel. L'automatisation de la sanction pour inexécution contractuelle[689] concerne en particulier l'exception d'inexécution de l'art. 1219 du C. civ. En dehors des cas de l'allocation de dommages et intérêts (C. civ., art. 1217, al. 2 et 1231 et s.) et de réduction du prix (C. civ., art. 1223, al. 1er), dès lors que le débiteur n'a pas honoré dans les temps impartis ses engagements, tel le paiement d'un loyer ou d'une facture, le *smart contract* a donc pour instruction de délivrer réciproquement le créancier de ses propres obligations. En interconnexion avec des objets présents tout au long du cycle d'exécution du contrat, il va ainsi pouvoir physiquement verrouiller l'élément-objet de la location à l'aide d'un objet communicant, telle une serrure de porte par exemple[690], ou annuler automatiquement la commande effectuée auprès des préparateurs et livreurs du commerçant. La sanction, même non-pécuniaire, est rendue par ce biais immédiatement exécutable. Plus encore, en créant ainsi un pont instantané entre virtualité et réalité, le code informatique introduit une nouvelle dimension aux solutions de *Contract Lifecycle Management* (CLM, Gestion du Cycle de Vie des Contrats)[691] tout en optimisant d'une manière générale la force de la sanction pour inexécution contractuelle et, *a fortiori*, la force du contrat.

Il faudra toutefois prêter une attention particulière à la programmation de la résolution pour inexécution (C. civ., art. 1224 et s.), dont les effets, après mise en demeure infructueuse (C. civ., art. 1225, al. 2), divergent selon que le contrat soit à exécution instantanée (C. civ., art. 1111-1, al. 1er) ou à exécution successive (C. civ., art. 1111-1, al. 2), à durée déterminée[692] ou indéterminée. Il s'agira pour cela d'identifier la qualification juridique de chaque contrat exécuté par un *smart contract* afin que celui-ci se conforme aux règles légales et jurisprudentielles correspondantes. Si la résolution d'une vente, y compris d'un bien futur, ou d'un échange, se résout en principe par la disparition

[687] LEGEAIS (Dominique), « Blockchain », *JCl. Sociétés Traité*, fasc. 2160, n° 57.
[688] Sur la *smart home*, *infra* n°s 85 et s.
[689] Sur l'automatisation comme dissuasion à l'inexécution, *supra* n°s 33 et s.
[690] GODEFROY (Lêmy), « Le code algorithmique au service du droit », *D.* 2018, pp. 734 et s.
[691] Sur les *Contract Lifecycle Management*, *supra* n° 31.
[692] Cass. Civ. 1ère, 28 avr. 1971, n° 69-13.775, *Bull.* 1971, I, n° 136 (« le contrat à exécution successive à durée déterminée doit s'analyser comme un contrat dont le fractionnement dans le temps ne peut être considéré que comme le mode d'exécution d'une seule et même convention »).

rétroactive du contrat[693] et la restitution des prestations de chaque partie dans les conditions prévues aux art. 1352 à 1352-9 du C. civ.[694], la résolution d'un contrat de location opère ses effets au jour de l'inexécution, pour prendre la forme d'une résiliation sans restitution (C. civ., art. 1229, al. 3), sous réserve de l'application de l'obligation de préavis[695].

B. Une interconnexion d'objets décentralisée

73. La création d'une « *blockchain* des objets » : la solution de la décentralisation. L'interconnexion des *smart contracts* avec les objets et systèmes d'IoT devient ainsi la clé d'une interaction avec le monde physique, permettant d'envisager des applications plus sophistiquées que ce que l'IoT ou les dispositifs électroniques pris isolément permettaient jusqu'ici[696]. D'ailleurs, selon un rapport de la société IBM, il est impossible pour une entité centralisée de gérer une telle architecture[697]. Au risque de compromettre à elle seule l'ensemble de l'expérience, elle ne peut tout à la fois neutraliser les tentatives d'intrusions malveillantes et autres cyberattaques – auxquelles les objets communicants sont particulièrement exposés[698] –, corriger ses potentielles défaillances, veiller à la conformité juridique et fournir une prestation de service de qualité[699]. En parallèle, l'informatisation croissante du quotidien avec le développement des objets communicants et/ou « intelligents » – tels que, dans le domaine de la santé avec les montres connectées, le télé-suivi, les systèmes de partage des dossiers patients et les projets sur la médecine spécialisée[700] –, est également une source de difficultés du point

[693] Cette règle découle d'une jurisprudence constante issue de l'arrêt Cass. Civ., 4 mai 1898, *D. P*. 98, I, n° 457.
[694] V. également, Cass. Civ. 1ère, 15 mai 2007, n° 05-16.926, *Bull*. 2007, I, n° 193 ; Cass. Civ. 1ère, 19 févr. 2014, n° 12-15.520, *Bull*. 2014, I, n° 26.
[695] Concernant l'obligation de préavis précédant la résiliation unilatérale d'un contrat à durée indéterminée, v., Cass. Civ. 1ère, 6 mars 2001, n° 98-20.540 (sous condition du respect d'un « préavis d'usage ») ; Cass. Civ. 1ère, 16 mai 2006, n° 03-10.328 (ou d'un « délai de préavis raisonnable ») ; Cass. Civ. 1ère, 2 févr. 1999, n° 97-12.964, *Bull*. 1999, I, n° 38 (« seule la gravité du comportement du cocontractant pouvant justifier une rupture sans préavis »).
[696] GENESTIER (Philippe) *et al*., « Blockchains et Smart Contracts : des perspectives pour l'Internet des objets (IoT) et pour l'e-santé », *Annales des Mines – Réalités industrielles* 2017/3 (août 2017), p. 70.
[697] « Device democracy Saving the future of the Internet of Things », IBM [online], Jul. 2015, https://www-935.ibm.com/services/multimedia/GBE03620USEN.pdf.
[698] BERGOUNHOUX (Julien), « Le retour des botnets ou pourquoi les objets connectés sont un danger pour l'Internet », *L'usine digitale* [en ligne], 24 oct. 2016, https://www.usine-digitale.fr/article/le-retour-des-botnets-ou-pourquoi-les-objets-connectes-sont-un-danger-pour-l-internet.N454382 ; KALLENBORN (Gilbert), « Pourquoi les objets connectés peuvent casser le web (et comment les en empêcher) », *BFMTV* [en ligne], 24 oct. 2016, https://hightech.bfmtv.com/securite/pourquoi-les-objets-connectes-peuvent-casser-le-web-et-comment-les-en-empecher-1051648.html.
[699] « Device democracy Saving the future of the Internet of Things », préc.
[700] JUANALS (Brigitte), « Protection des données personnelles et TIC au cœur des enjeux de société et de la mondialisation : les mécanismes d'un contrôle distribué », *TIC&société* [en ligne], vol. 8, 2014, n°s 1-2, https://journals.openedition.org/ticetsociete/pdf/1475.

de vue juridique. Comme le constate Philippe Genestier, elle « génère des préoccupations croissantes en termes de respect de la vie privée, de sécurité, en plus des contraintes réglementaires à prendre en compte par les acteurs du secteur »[701]. En effet, les entreprises doivent le plus souvent choisir entre, d'une part, construire un système fermé et sécurisé mais très limité dans sa capacité à intégrer d'autres applications ou machines que celles utilisées et, d'autre part, construire un système ouvert, performant, et intégré aux nuages IoT, mais s'exposant *de facto* à un accès par des tiers[702]. L'approche actuelle fondée sur Internet s'avère relativement inadaptée, si bien que la *blockchain* constitue un procédé fiable d'interconnexion, compte tenu de ses caractéristiques d'entité décentralisée, transparente et sécurisée.

74. La solution de la décentralisation : endiguer les cyberattaques et protéger les utilisateurs. Comme en témoigne les multiples attaques ayant utilisé le *malware Mirai*[703] pour pirater nombre de grands groupes internationaux, tels que Amazon, Netflix, Twitter, Reddit, Spotify ou Tumblr en octobre 2016[704], par le biais de 1,5 millions de dispositifs infectés, l'IoT est particulièrement exposé aux cyberattaques. Ces risques avérés d'intrusions malveillantes mettent en exergue les faiblesses inhérentes de la centralisation de l'interopérabilité actuelle des dispositifs électroniques communicants[705]. Afin de satisfaire aux exigences de sécurité et de protection des données incombant aux services en ligne[706], les objets communicants – et en particulier l'architecture réseau mise en place pour les relier à Internet – doivent, d'une manière générale, être munis de deux choses[707]. D'une part, ils doivent présenter des propriétés de résistance, qui correspondent à la

[701] GENESTIER (Philippe) *et al.*, art. cit., p. 70.
[702] NEVEJANS (Nathalie), *Traité de droit et d'éthique de la robotique civile*, *op. cit.*, pp. 143-144.
[703] Le malware *Mirai* est un logiciel malveillant capable de prendre le contrôle de n'importe quel appareil – qu'il s'agisse d'ordinateurs ou, en l'espèce, d'objets connectés – en forçant les codes d'accès avec des listes de codes usuellement utilisés, tels que « admin/admin », « admin/password », « admin/123456 », etc. [v., KALLENBORN (Gilbert), art. cit.]. Il les transforme ensuite en *bots* afin de lancer des attaques virtuelles à grande échelle appelées déni de service distribué (*DDoS*), ce qui rend momentanément indisponible un service en ligne pour ses utilisateurs.
[704] Pour plus de précisions sur les attaques, v., BERGOUNHOUX (Julien), art. cit.
[705] Un auteur souligne que la « faiblesse […] dévoilée [est] la trop grande dépendance des services web vis-à-vis des prestataires Internet. La résilience de l'Internet est basée depuis son origine sur son architecture décentralisée, qui évite que la panne d'un serveur entraîne beaucoup d'autres dans sa chute. Or, Dyn est devenu aux États-Unis *de facto* un fournisseur unique de services DNS pour un grand nombre de sites web » [KALLENBORN (Gilbert), art. cit.].
[706] Notamment des données personnelles, v., L. n° 2018-493, 20 juin 2018, relative à la protection des données personnelles, *JORF*, 21 juin 2018, portant modification de la L. n° 78-17, 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, *JORF*, 6. janv. 1978, art. 34, al. 2 ; Règl. (UE) n° 2016/679 du Parlement européen et du Conseil, 27 avr. 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (dit « Règlement Général sur la Protection des Données », ou RGPD), *JOUE* L 119, 4 mai 2016, pp. 1-88.
[707] GENESTIER (Philippe) *et al.*, art. cit., p. 71.

capacité à endiguer les pannes – accidentelles ou provoquées – pour permettre aux utilisateurs de continuer d'utiliser le service. D'autre part, ils doivent disposer de propriétés de résilience, qui correspondent à la capacité parallèle à mettre en œuvre des stratégies pour corriger les pannes et reprendre un fonctionnement normal. Ces deux caractéristiques sont le propre de la *blockchain*. La moindre activité algorithmiquement anormale est automatiquement repérée par le protocole, et se voit par conséquent écartée par le biais d'un refus de validation des nœuds. C'est la raison pour laquelle la *blockchain* apparaît comme une solution à un déploiement tant généralisé que sécurisé de l'IoT[708]. Alors que l'écosystème des objets sans la *blockchain* se révèle désarmé au sein d'un environnement naturellement hostile, l'application des *smart contracts* permettrait de faire renaître la confiance nécessaire à leur expansion. C'est sur ce concept que s'est appuyé, par exemple, l'entreprise allemande Porshe, en collaboration avec la *start-up* Xain, afin d'assurer la protection du conducteur lors du déverrouillage des portes du véhicule[709]. Partant du constat que les voitures munies de dispositifs communicants subissent de nombreuses cyberattaques, le constructeur a introduit un dispositif permettant au seul propriétaire de déclencher le *smart contract* associé au système de verrouillage.

75. La solution de la décentralisation : assurer l'interopérabilité. Face à l'absence de normes communes et à l'indépendance des constructeurs – conduisant à des systèmes hétérogènes, complètement isolés les uns des autres, et finalement non-interopérables[710] – seules des plateformes capables de fournir des moyens de communication entre les objets pourront dépasser les divers enjeux techniques engendrés[711]. À l'image de *Fog Computing*[712], en s'érigeant traductrice des différents protocoles, la *blockchain* permettrait le développement de plateformes multi-agents.

---

[708] *Id*.

[709] « Blockchain: the key technology of tomorrow », *Porsche* [online], 1st Nov. 2019, Porsche Newsroom > Company > Blockchain: the key technology of tomorrow, https://newsroom.porsche.com/en/company/porsche-blockchain-technology-opportunities-digitization-16800.html.

[710] NEVEJANS (Nathalie), « L'usine connectée : l'usine à l'ère du numérique sous le prisme du droit », *in* CHÉRIGNY (Florence), ZOLLINGER (Alexandra) (dir.), *Les objets connectés. Colloque "30 ans du magistère en droit des TIC" Vendredi 23 septembre 2016*, éd. Presses Universitaires juridiques de Poitiers, coll. Actes et colloques de la Faculté de Droit et des Sciences sociales, 2018, p. 37.

[711] GENESTIER (Philippe) *et al.*, art. cit., p. 72.

[712] CUNNINGHAM (Talyana), « Blockchain et Fog computing, le duo gagnant », *Cisco* [en ligne], 28 juin 2018, https://gblogs.cisco.com/fr/iot/blockchain-et-fog-computing-le-duo-gagnant/.

76. Associée aux 28 milliards d'objets communicants et/ou « intelligents » attendus pour 2021[713], la *blockchain* pourrait permettre la concrétisation de projets de plus en plus automatisés, tout en accompagnant la redéfinition tant des relations contractuelles en une économie du partage basée sur une interaction Homme-objets, que du rôle de certains acteurs[714]. Il est possible d'imaginer que dans les années à venir des voitures autonomes seraient dotées, *via* une association avec la technologie des *smart contracts*, d'un capital de crypto-actifs découlant des diverses locations ou covoiturages réalisés, et seraient programmées pour s'acquitter des factures de carburant, et peut-être même des places de parking, en toute autonomie. Des projets émergent d'ores et déjà en ce sens, à l'image du consortium MOBI (*Mobility Open Blockchain Initiative*) piloté par les entreprises BMW, General Motors, Ford et Renault[715] ou du constructeur Porsche[716]. Il faudra toutefois s'assurer qu'une pareille prédisposition à la passation d'une succession de contrats de prestation de services ayant pour objectif initial de faciliter le quotidien des utilisateurs ne devienne pas le prétexte d'un débat sur l'octroi de la personnalité juridique à des dispositifs électroniques[717].

À ce stade de la réflexion, un état des lieux de cette « *blockchain* des objets » peut se révéler intéressant.

---

[713] PARET (Dominique), *Objets communicants sécurisés : Applications, conceptions et concrétisation*, éd. ISTE Group, 2017, p. 34.

[714] GENESTIER (Philippe) *et al*., art. cit., pp. 70-71. – V. également, GARESSUS (Emanuel), « La blockchain promet une nouvelle révolution », *Le Temps* [en ligne], 6 nov. 2015, https://www.letemps.ch/economie/blockchain-promet-une-nouvelle-révolution.

[715] https://dlt.mobi/. – V. également, Nexity, « Avec la blockchain, la voiture devient (vraiment) autonome », *Envies de villes* [en ligne], 18 oct. 2018, https://www.enviesdeville.fr/penser-la-ville/avec-la-blockchain-la-voiture-devient-vraiment-autonome/.

[716] « Blockchain: the key technology of tomorrow », art. cit.

[717] V. sur le sujet (en particulier concernant la « personnalité juridique » des robots) : Direction Générale des Politiques Internes du Parlement Européen, PE 571.379, étude sur les règles européennes de droit civil en robotique, Département thématique C : droits des citoyens et affaires constitutionnelles, affaires juridiques [en ligne], oct. 2016, p. 16, https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_FR.pdf, (incongruité de la personnalité juridique du robot en matière de responsabilité) ; NEVEJANS (Nathalie), « Le statut juridique du robot doit-il évoluer ? », *La Jaune et la Rouge* [en ligne], n° 750, déc. 2019, https://www.lajauneetlarouge.com/le-statut-juridique-du-robot-doit-il-evoluer/ ; NEVEJANS (Nathalie), RAJA (Chatila), GLASA (Joseph) *et al.*, « Open Letter to the European Commission Artificial Intelligence and Robotics », *Robotics* [online], Oct. 2018, http://www.robotics-openletter.eu/, (la lettre ouverte a rassemblé 285 signataires dans toute l'UE) [version initiale en français, NEVEJANS (Nathalie), « Lettre ouverte à la Commission européenne sur l'intelligence artificielle et la robotique », *Sido Lyon* [en ligne], 24 oct. 2018, https://www.sido-lyon.com/blog/2018/10/24/lettre-ouverte-a-la-commission-europeenne-sur-lintelligence-artificielle-et-la-robotique/.

Section 2. Une mutation des relations Homme-machine : transformation des relations contractuelles traditionnelles

77. En initiant une mutation de la relation Homme-machine la chaîne de blocs se révèle capable de renouveler la façon dont les échanges sont conduits entre les Hommes. En témoigne le déploiement des systèmes de *smart property* (§ 1) et de *smart home* (§ 2), qui contribuent, chacun à leur niveau, à optimiser le processus d'exécution des contrats.

§ 1. Le fonctionnement de la *smart property*

78. La notion de *smart property* consiste en un écosystème capable de lier le propriétaire à la chose sur laquelle il détient des droits de propriété par un lien à la fois immuable et dynamique (A), capable de s'adapter à un changement de possesseur légitime par la programmation d'un mécanisme autonome de mise à disposition de la chose (B) selon les termes du contrat inscrits au sein du *smart contract.*

A. Établissement d'un droit immuable et dynamique de disposition d'un bien

79. Désintermédier les relations contractuelles portant sur des choses par le biais des objets. La grande majorité des individus est familiarisée avec l'interaction Homme-machine, qu'elle conçoit comme un outil permettant de déléguer une tâche ou d'obtenir un service. C'est notamment de cette idée qu'est né le concept de « *slock* », un système de verrou connecté développé par la *start-up* slock.it. Il s'agit de payer une serrure de porte « intelligente » pour qu'elle donne accès, par exemple, à un appartement, ou de payer un verrou de vélo « intelligent » pour pouvoir utiliser les vélos mis à disposition du public, ou encore de payer une prise d'alimentation « intelligente » pour être autorisé à alimenter un appareil[718]. Aux États-Unis, mais également à Bordeaux et dans quelques villes d'Italie et d'Espagne, la *start-up* Helbiz met à disposition des trottinettes (*HelbizGO*) et des vélos (*HelbizBike*) électriques qui, après avoir été géolocalisés par le biais d'une application dédiée, peuvent être loués[719]. L'utilisateur scanne le *QR-code* présent sur l'appareil, l'application vérifie les informations de l'utilisateur et un *smart*

[718] PRISCO (Giulio), « Slock.it to Introduce Smart Locks Linked to Smart Ethereum Contracts, Decentralize the Sharing Economy », *Bitcoin Magazine* [online], 5 Nov. 2015, https://bitcoinmagazine.com/articles/slock.it-to-introduce-smart-locks-linked-to-smart-ethereum-contracts-decentralize-the-sharing-economy-1446746719/.
[719] https://www.helbiz.com/.

contract est instantanément inscrit sur la chaîne[720]. Ce contrat entre le loueur et le propriétaire fixe les modalités de location, notamment en ce qui concerne la tarification applicable, et la souscription d'une assurance facultative[721]. Subséquemment, la clé numérique déverrouillant le véhicule est envoyée au téléphone de l'utilisateur qui peut alors prendre possession de l'appareil[722]. Le *smart contract* reste actif jusqu'à la fin de la location et en recueille automatiquement le paiement dès lors que l'utilisateur manifeste sa volonté de mettre un terme au contrat par l'inscription sur la chaîne d'une photographie de l'appareil à l'endroit de son nouveau stationnement[723]. La désintermédiation permet à la fois de simplifier et d'accélérer le processus contractuel, et de réduire les coûts de fonctionnement liés à la prestation, donc de diminuer les tarifications. Plus encore, force est de constater que dans ces situations, les tiers ne seraient en principe plus nécessaires pour veiller à la bonne application des dispositions contractuelles, ni même le propriétaire lui-même.

Quel que soit son domaine d'application, la *smart property* consiste en des systèmes de gestion digitalisés de la propriété mobilière ou immobilière[724], permettant d'effectuer des transactions particulières de ces biens, en particulier les transferts de droit de jouissance d'un bien, sans recourir à des sociétés ou à des sites d'intermédiation, tels qu'*Airbnb*, afin de conclure puis d'assurer le respect du contrat de location entre les parties. La *smart property* fondée sur la technologie *blockchain* constitue une extension des *smart contracts* en ce sens qu'elle institue une auto-gestion de sa disposition en interaction directe avec son utilisateur[725], et transcende ainsi la relation Homme-machine traditionnelle.

80. Renforcer les droits détenus par chaque partie sur une chose. La *smart property via blockchain* fonde une version interactive des contrats de location, permettant par l'auto-exécution de joindre indirectement le propriétaire à la relation contractuelle, tout en lui assurant à distance un renforcement de ses droits de propriété sur le bien[726]. En 1997, Nick Szabo soulignait que « les *smart contracts* font référence à cette propriété

[720] *Id.*
[721] *Id.*
[722] *Id.*
[723] *Id.*
[724] KERIKMÄE (Tanel), RULL (Addi), *The Future of Law and eTechnologies*, ed. Springer, 2016, pp. 137-138.
[725] ACHESON (Noelle), « Smart property: what does that mean for the blockchain? », *FinTech Blue* [online], 9 Dec. 2015, http://www.fintechblue.com/2015/12/smart-property-what-does-that-mean-for-the-blockchain/.
[726] SZABO (Nick), « Formalizing and Securing Relationships on Public Networks », [online], 1st Sept. 1997, http://firstmonday.org/ojs/index.php/fm/article/view/548/469.

sous une forme dynamique, [et] donneraient le contrôle des clés cryptographiques pour l'exploitation de la propriété à la personne qui possède légitimement cette propriété, selon les termes du contrat »[727]. En définitive, l'ensemble des droits, même temporaires en ce qui concerne le loueur, s'avèrent consolidés par l'usage de la *blockchain*.

81. L'exemple du *slock* pour « louer, partager ou vendre facilement tout ce qui peut être verrouillé »[728]. Depuis juin 2015[729], la *start-up* allemande mettait à disposition l'application mobile « *slock.it* » en version bêta, disponible dans l'*App Store* pour les appareils *Android* et *Apple* allemands[730]. Désormais, slock.it met à disposition un kit de développement logiciel, l' « *Incubed SDK* », fourni avec des outils et des interfaces normalisées, ainsi que des méthodes d'interaction, de contrôle d'accès, de sécurité, etc., permettant de connecter n'importe quel dispositif communicant avec la *blockchain* et d'en automatiser l'accès[731]. Un réseau de partage universel, nommé *Universal Sharing Network* (USN)[732], au sein d'une DAO créée sur la plateforme *Ethereum*, relie les appareils à la *blockchain*. L'USN détenu par le propriétaire permet de verrouiller et de déverrouiller le verrou « intelligent » (*slock*) automatiquement, en fonction des conditions fixées dans le *smart contract* conclu entre le propriétaire et l'utilisateur. Le contrat peut être fondé sur une variable déterminée, telle que la durée d'utilisation ou le nombre de kilomètres parcourus.

Finalement, il semble que slock.it matérialise l'idée initialement évoquée par Nick Szabo de *smart contracts* embarqués dans des dispositifs électroniques compatibles. Il convient à présent d'analyser le fonctionnement en lui-même du système automatisé.

---

[727] « *Smart contracts reference that property in a dynamic, (often proactively enforced form, and provide much better observation and verification where proactive measures must fall short.)* [These protocols] *would give control of the cryptographic keys for operating the property to the person who rightfully owns that property, based on the terms of the contract.* » [notre trad.], SZABO (Nick), « Formalizing and Securing Relationships on Public Networks », préc.

[728] « *If you can lock it, we will let you rent, sell or share it.* » [notre trad.], https://slock.it/.

[729] PRISCO (Giulio), « Slock.it to Introduce Smart Locks Linked to Smart Ethereum Contracts, Decentralize the Sharing Economy », préc.

[730] La version « bêta » désigne une version test, une pré-version en quelques sortes.

[731] V., https://slock.it/, Products > Incubed SDK.

[732] V., https://slock.it/, Products > Universal Sharing Network (USN). – JENTZSCH (Christoph), « Slock.it IoT Layer: Enabling the economy of things », *Medium* [online], Nov. 2015, https://blog.slock.it/slock.it-iot-layer-f305601df963 : « *It's a nice vision to use blockchain technology for* IoT *devices. And yet, how can you securely connect a device to the blockchain?* [...] *Our team at Slock.it got together to brainstorm different options. We wanted to have a secure solution which removes the need to trust a single server and we didn't want to spend time synchronizing the chain. Neither did we want to store anything beyond the software itself. We also wanted it to work with all EVM-based blockchains, have minimal bandwidth requirements, and it was supposed to only communicate when it was actually needed. We found the answer, and called it INCUBED (IN³)! A trustless incentivized remote node network. In short, a network of remote nodes, which are incentivized to always give you the right response*. »

82. « *Slock smart* » et location de biens. Lorsque qu'une personne acquiert un *slock* dans le but de verrouiller/déverrouiller un bien, cela consiste à connecter le bien directement à la *blockchain Ethereum via* un contrat appelé « *slock smart* »[733]. Par le biais du *slock smart*, le propriétaire fixe un prix pour la location de sa propriété, désignée par le contrat « *smart property* », et incidemment un montant de dépôt de garantie[734], conformément aux art. 1713 et s. du C. civ. L'utilisateur potentiel devra donc payer ce dépôt par une transaction sur la *blockchain Ethereum* ou toute autre chaîne basée sur l'EVM (*Ethereum Virtual Machine*) indépendamment de la plateforme de slock.it pour obtenir l'accès au bien[735]. Techniquement, *Incubed SDK* agit comme un pare-feu et contrôle l'intégralité des messages entrants et sortants, qui doivent être impérativement signés cryptographiquement[736]. De cette manière, dès lors que la signature est validée par l'interface, l'appareil se connecte à la *blockchain* et demande l'autorisation d'accès[737]. Une seule signature, découlant d'un identifiant unique nommé « clé privée » en langage cryptographique[738], peut accéder au *slock smart* de l'objet. Le propriétaire définit les conditions d'attribution d'une clé au sein du contrat *slock smart*[739], de sorte qu'une fois ces conditions réunies, l'utilisateur obtient instantanément une clé privée pour accéder à la propriété verrouillée[740].

En parallèle, le *slock smart* peut également être programmé pour appliquer le principe selon lequel le propriétaire n'a accès au bien, durant toute sa période de location, que sur autorisation du locataire, en vertu des art. 9 du C. civ. et 226-4 du C. pén.[741]. À l'instant où le contrat s'exécute, le *slock* ne permet alors plus au propriétaire de pénétrer dans les lieux, à moins qu'il ne détienne l'accord du preneur sous la forme d'une clé privée valide.

---

[733] PRISCO (Giulio), « Slock.it to Introduce Smart Locks Linked to Smart Ethereum Contracts, Decentralize the Sharing Economy », préc.
[734] *Id.*
[735] *Id.*
[736] V., https://slock.it/, Products > Incubed SDK.
[737] *Id.*
[738] Définition *infra* n° 99.
[739] LEGEAIS (Dominique), *op. cit.*, n° 55.
[740] JENTZSCH (Simon), « Share&Charge Smart Contracts: the Technical Angle », *Medium* [online], 1st May 2017, https://blog.slock.it/share-charge-smart-contracts-the-technical-angle-58b93ce80f15.
[741] Le principe veut que le propriétaire n'ait plus accès au logement du locataire sans son autorisation en vertu des art. 9 du C. civ. (respect de la vie privée du locataire) et 226-4 du C. pén. (éventuellement infraction de violation de domicile).

En pratique, la transaction financière entre le locataire et le propriétaire est suspendue jusqu'à ce que le locataire décide de retourner la clé virtuelle en envoyant une nouvelle transaction à la chaîne de blocs. À l'instar d'une caution, la somme initialement déposée sous forme de transaction est alors immédiatement débloquée, et conformément aux dispositions du *slock smart* conclu, l'équivalent du montant de la location à verser, débitée du solde du prix en cas d'acompte et du dépôt de la location, est envoyé au propriétaire du *slock*[742]. L'intérêt étant que l'intégralité de ces opérations s'exécutent sans l'intervention d'un tiers ni même des parties directement.

Il est également possible d'imaginer que diverses situations pouvant survenir durant la location soient initialement prévues dans le contrat. Il s'agirait, par exemple, de programmer que l'irrespect des engagements pris par chacune des parties entrainerait une indemnisation ou une résiliation automatique selon le cas. L'algorithme fixerait alors un délai avant verrouillage du bien par le *slock* qu'il porterait à la connaissance du preneur *via* une notification à travers l'interface *Incubed SDK* (C. civ., art. 1741). Il en irait ainsi en cas de perte pour le locataire résultant de vices ou défauts rendant inutilisable la chose louée (C. civ., art. 1721), ou au contraire s'il s'avérait que le locataire « n'use pas de la chose louée raisonnablement ou emploie la chose louée à un autre usage que celui auquel elle a été destinée, ou dont il puisse résulter un dommage pour le bailleur » (C. civ., art. 1729), conditions qui nécessiteront des mentions claires et précises au sein du *smart contract* dédié. En toute logique, il sera toutefois important pour chacune des parties d'être en mesure ensuite de prouver le bienfondé de leur décision en cas de contentieux.

83. Domaines d'application. S'agissant des biens immeubles, en raison de l'automaticité du verrouillage du bien à la fin de la relation contractuelle, l'ensemble de ces programmations semblent plus particulièrement convenir aux contrats de location saisonnière entre particuliers plutôt qu'aux contrats de baux d'habitation classiques. Or, comme tout contrat écrit, le *slock smart* semble pouvoir lui aussi prendre en compte, *via* la programmation des règles de droit au sein du *slock smart*, les exigences légales. Il en va ainsi de l'obligation de préavis fixée, d'une manière générale, par l'art. 15 de loi n° 89-462 du 6 juillet 1989[743], en parallèle de l'art. L. 412-6 du CPC exéc. établissant les

[742] PRISCO (Giulio), « Slock.it to Introduce Smart Locks Linked to Smart Ethereum Contracts, Decentralize the Sharing Economy », préc.

[743] L. n° 89-462, 6 juill. 1989, tendant à améliorer les rapports locatifs et portant modification de la L. n° 86-1290 du 23 décembre 1986, *JORF*, 8. juill. 1989, et modifiée par la L. n° 2014-366, 24 mars 2014, pour l'accès au logement et un urbanisme rénové, *JORF* n° 0072, 26 mars 2014, texte n° 1, art. 1-25-2. V., notamment, l'art. 2, al. 2, selon lequel la loi s'applique aux « locations de locaux à usage d'habitation ou à usage mixte professionnel et d'habitation, et qui constituent la résidence principale du preneur, ainsi qu'aux garages, aires et places de stationnement, jardins et autres locaux, loués accessoirement au local principal

conditions d'expulsion durant la trêve hivernale, ou encore de l'obligation de respect des engagements réciproques due, tant par le bailleur que par le locataire en ce qui concerne, par exemple, les art. 6 et 7 de la loi du 6 juillet 1989. Les parties devront alors prendre leurs dispositions pour rendre le contrat « blockchaîné » conforme à la loi en vigueur, d'autant plus que ces dispositions sont d'ordre public[744]. Par ailleurs, il est également possible d'imaginer la mise en place d'un tel dispositif afin de simplifier la mise à disposition d'un bien immobilier dans le cadre d'une indivision, qu'elle soit d'origine légale ou conventionnelle. Un *slock smart* pourrait ainsi automatiser l'accès, par périodes prédéfinies, de chaque couple ayant fait l'achat, en indivision, d'une résidence de vacances, par exemple, voire de chaque indivisaire d'une résidence secondaire transmise à la suite d'un partage de succession (C. civ., art. 815-815-1 et 1873-1 et s.).

S'agissant des biens meubles, les serrures intelligentes pourraient également contrôler l'accès aux voitures – sous réserve de programmation et d'application des règles spéciales telles que l'obligation d'assurance pour la location de véhicule terrestre à moteur (C. assu., art. L211-1) –, aux bicyclettes et même aux unités de stockage. Dès lors que le bien dispose d'un dispositif communicant, il peut être relié au cœur de ce système et faire l'objet d'un *slock smart* de location ou même de partage, organisant la mise à disposition automatique du bien entre les différents propriétaires. Ainsi, par exemple, les voitures pourraient être garées dans les rues de la ville en attendant le prochain client. Celui-ci louerait à l'heure l'une d'elles, qu'il géolocaliserait et déverrouillerait instantanément à l'aide d'une application de téléphone envoyant une requête « payer la serrure » à une *blockchain*, puis utiliserait, et enfin garerait à nouveau la voiture pour qu'un autre utilisateur puisse s'en servir[745]. Lors de sa présentation à la *DevCon 1* de Londres en novembre 2015[746], le fondateur de slock.it Christoph Jentzsch évoquait une « technologie promettant d'habiliter n'importe qui à louer, partager ou vendre facilement tout ce qui peut être verrouillé »[747], et imaginait une voiture électrique qui, ayant besoin d'être rechargée, conclurait un contrat d'achat d'électricité par induction avec d'autres véhicules à un feu rouge[748]. Il proposait ainsi de créer une véritable coopération entre

par le même bailleur. », ainsi que l'art. 3 concernant les exceptions d'application. En vertu de l'art. 25-3, elle est également applicable aux « contrats de location de logements meublés tels que définis à l'article 25-4 dès lors qu'ils constituent la résidence principale du locataire au sens de l'article 2. »

[744] L. n° 89-462, préc., modifiée par la L. n° 2014-366, préc., art. 2, al. 2.

[745] JENTZSCH (Christoph), « Slock.it IoT Layer: Enabling the economy of things », préc.

[746] V. le site officiel, http://devcon.london/. – JENTZSCH (Christoph), « slock.it DAO demo », *in* Fondation Ethereum, *DevCon1 Ethereum*, Developer Conference [video online], London, 9-13 Nov. 2015, not published,https://www.youtube.com/watch?v=uy6P5_WQoUI.

[747] « *If you can lock it, we will let you rent, sell or share it*. » [notre trad.], https://slock.it/.

[748] JENTZSCH (Christoph), « Slock.it IoT Layer: Enabling the economy of things », art. cit. – V. également, JENTZSCH (Christoph), « Presentation "Blockchain" », *CEBIT d!talk* [video online], https://www.youtube.com/watch?v=nyEfBua469E.

machines, formant un système d'échanges de valeurs, au-delà des échanges d'informations traditionnels[749]. D'après Nick Szabo, les *smart contracts* pourraient, à terme, « [intégrer] des contrats dans toutes sortes de biens de valeur, contrôlés par des dispositifs numériques »[750]. Selon un auteur, le secteur automobile et, plus largement, la sphère sociale et économique, sont sur le point de connaître une transformation profonde, et souligne que « les voitures de locations disposant de "serrures intelligentes" pourront également se conduire seules jusqu'à leurs prochains clients », menant, aux termes des innovations, à « modifier radicalement la vie urbaine »[751]. Finalement, il semble qu'*Airbnb*, *Uber* et les autres intermédiaires d'accès aux biens et services soient sur le point de se faire disrupter à leur tour[752].

84. L'interconnexion des technologies offre de nouvelles possibilités d'expérimentation des interactions, d'une part, entre la machine et l'Homme et, d'autre part, entre machines. Pourtant, il n'y a pas que sur les routes que les modes de vie risquent de changer.

§ 2. La nouvelle *smart home* décentralisée

85. De l'application effective au simple projet en cours d'expérimentation, la nouvelle *smart home* décentralisée épouse de multiples formes et investit divers champs juridiques. Du partage automatisé d'énergie dans des écosystèmes d'autoconsommation (A) à la perspective d'une auto-gestion des centaines de milliards d'objets présents dans les habitations (B), la *blockchain* et les *smart contracts* constituent la clé de la réussite de l'interconnexion des objets communicants entre eux.

---

[749] JENTZSCH (Christoph), « Slock.it IoT Layer: Enabling the economy of things », préc. : « *In order for machines to be part of an economy of things, they need to cooperate with each other on a different level beyond just transferring data. They need to exchange values, and, most importantly, they need to be able to enter into complex agreements. Not too far into the future we will also see machine to human interactions. So if we have an autonomous car, it needs someone to change the tires. Not for free. The car itself will pay someone to do this.* »

[750] « [Smart contracts] *embed contracts in all sorts of property that is valuable and controlled by digital means* » [notre trad.], SZABO (Nick), « Formalizing and Securing Relationships on Public Networks », préc.

[751] PRISCO (Giulio), « Slock.it to Introduce Smart Locks Linked to Smart Ethereum Contracts, Decentralize the Sharing Economy », préc.

[752] ALLISON (Ian), « Airbnb has no plans to move into blockchain », *International Business Times* [online], 14 Apr. 2016, https://www.ibtimes.co.uk/airbnb-has-no-plans-move-into-blockchain-1554743.

86. Une application particulière en matière de partage d'énergie au sein des *smart homes* ou entre *smart homes* : les *smart grids*. Fondée sur les principes d'économie du partage en P2P et de renouvellement de l'énergie, *TransActive Grid* de LO3 Energy et ConsenSys proposent de la même manière aux auto-producteurs d'énergie, notamment solaire, de collectiviser les ressources inutilisées. Expérimentée en 2016 dans un lot d'appartements de Brooklyn aux États-Unis, elle permet aux résidents de vendre et d'acheter des crédits d'énergie en toute sécurité entre voisins en multipliant les réseaux locaux intelligents – ou *smart grids* – *via* la création de mini-communautés énergétiques autonomes[753]. Prenant la forme d'une *dApp* développée sur *Ethereum*, elle est reliée à des capteurs qui enregistrent un historique de la création d'énergie solaire de chaque résident sur la *blockchain*. Les *smart contracts* de l'application mettent ensuite en œuvre les règles d'utilisation et de partage de cette énergie, ainsi que la grille de tarifs des producteurs[754]. En pratique, les compteurs électriques négocient automatiquement la fourniture d'énergie supplémentaire avec les autres compteurs et contractualise l'achat/vente sans aucune intervention humaine[755], conformément aux directives de la Commission européenne concernant le paquet « Une énergie propre pour tous les Européens »[756] et mises en œuvre par la loi n° 2019-1147 du 8 novembre 2019 relative à l'énergie et au climat (C. énergie, art. L. 315-1 et s.).

C'est sur ce support que s'est appuyé le consortium français Eurêka Confluence et l'Opérateur Energie Lyon Living Lab, pour mettre en œuvre le premier axe « ville efficiente » de sa stratégie de développement durable lors de la construction de l'écoquartier La Confluence dans la ville de Lyon[757]. Partant du constat selon lequel les

---

[753] Il s'agit plus exactement d'une « *Ethereum-enabled Community Energy Market Sharing Economy for Microgrids* » [ORISINI (Lawrence), « Transactive Grid: A Decentralized Energy Management Solution », *in* Fondation Ethereum, *DevCon1 Ethereum*, Developer Conference [video online], London, 13 Nov. 2015, not published, https://www.youtube.com/watch?v=kq8RPbFz5UU]. – V. également, http://lo3energy.com/ ; https://consensys.net/.

[754] NAUDIN (Iris V.), « TransActive Grid, le réseau d'énergie intelligent à Brooklyn », *Medium* [en ligne], 22 mars 2017, https://medium.com/le-lab/transactive-grid-le-r%C3%A9seau-d%C3%A9nergie-intelligent-%C3%A0-brooklyn-ead550918cc2.

[755] TELLENNE (Cédric), « L'énergie, vecteur de développement et de puissance des États », *Géopolitique des énergies*, 2021, p. 9.
PETRUCCI (Mélissa), « Qu'est-ce que la blockchain peut apporter aux Smart Grids ? », *lesmartgrids.fr* [en ligne], 2 oct. 2017, https://les-smartgrids.fr/blockchain-apporter-smart-grids/.

[756] COM(2015) 80 final de la Commission au Parlement européen, au Conseil, au Comité économique et social européen, au Comité des régions et à la Banque européenne d'investissement, 25 févr. 2015, sur le Cadre stratégique pour une Union de l'énergie résiliente, dotée d'une politique clairvoyante en matière de changement climatique.

[757] « Opérateur global de services urbains. Lyon Living Lab Confluence – fiche projet », Ministère de la transition écologique et solidaire, Ministère de la cohésion des territoires [en ligne], juin 2017, http://www.divd.logement.gouv.fr/IMG/pdf/lyon_living_lab_confluence_fiche_projet_divd_a4_9_light.p

dispositifs de stockage actuels de l'énergie présentent malgré eux des pertes, l'objectif du projet est de construire des territoires à énergie positive, c'est-à-dire des « morceaux de ville […] qui, en sus de consommer peu d'énergie, en produisent » et, à terme, de réussir à suffisamment autonomiser les quartiers pour qu'aucune énergie ne soit stockée[758]. C'est sur cette idée de flux tendu énergétique qu'a été implanté le démonstrateur Eurêka et le *Smart Grid* de Lyon Confluence, qui mutualise l'énergie produite par les panneaux solaires photovoltaïques d'une douzaine de bâtiments mixtes comprenant des logements, des commerces, des bureaux et des équipements publics[759]. En plus de sécuriser les échanges d'énergie produite, la plateforme « *Blockchain as a Service* » de Microsoft Azure, développée par Stratumn et Energisme, met à disposition des riverains, en plus d'un mécanisme de transactions automatisés, un outil d'information du taux de consommation d'énergie locale, dont les données sont sécurisées par un système implanté sur une *blockchain*[760]. Conformément à sa stratégie de développement durable et son objectif de réduction de la consommation énergétique, le consortium a doté les bâtiments de divers capteurs de température, de ventilation, d'éclairage ou encore d'émissions de CO_2[761]. L'opération d'autoconsommation collective a été légalisée en France dès l'entrée en vigueur de la loi n° 2017-227 du 24 février 2017 ratifiant les ordonnances n° 2016-1019 du 27 juillet 2016 relative à l'autoconsommation d'électricité et n° 2016-1059 du 3 août 2016 relative à la production d'électricité à partir d'énergies renouvelables et visant à adapter certaines dispositions relatives aux réseaux d'électricité et de gaz et aux énergies renouvelables[762] et du décret d'application n° 2017-676 du 28 avril 2017[763]. Cependant, contrairement au *TRansActive Grid* de Brooklyn, la loi française ne s'applique qu'aux modèles mettant en œuvre une fourniture d'électricité effectuée entre un ou plusieurs producteurs et un ou plusieurs consommateurs finaux liés entre eux au sein d'une personne morale (C. énergie, art. L. 315-2).

---

df. – V. également, GOURDON (Jessica), « La "blockchain" ouvre le champ des possibles pour la "smart city" », *Le Monde* [en ligne], 27 sept. 2017, https://www.lemonde.fr/smart-cities/article/2017/09/27/la-blockchain-ouvre-le-champ-des-possibles-pour-la-smart-city_5192463_4811534.html.

[758] MAZOYER (Éric), « Point de vue d'Eric Mazoyer (Bouygues Immobilier) : Construire un bâtiment à énergie positive », *CRE.fr* [en ligne], 2 mai 2018, Accueil > Tous les dossiers > La blockchain appliquée à l'énergie, http://www.smartgrids-cre.fr/index.php?p=blockchain-bouygues.

[759] *Id.*

[760] PETRUCCI (Mélissa), art. cit.

[761] *Id.*

[762] L. n° 2017-227, 24 févr. 2017, ratifiant les ordonnances n° 2016-1019 du 27 juillet 2016 relative à l'autoconsommation d'électricité et n° 2016-1059 du 3 août 2016 relative à la production d'électricité à partir d'énergies renouvelables et visant à adapter certaines dispositions relatives aux réseaux d'électricité et de gaz et aux énergies renouvelables, *JORF* n° 0048, 25 févr. 2017, texte n° 4, modifiée par la L. n° 2019-1147, 8 nov. 2019, relative à l'énergie et au climat, *JORF* n° 0261, 9 nov. 2019, texte n° 1.

[763] Décr. n° 2017-676, 28 avr. 2017, relatif à l'autoconsommation d'électricité et modifiant les articles D. 314-15 et D. 314-23 à D. 314-25 du code de l'énergie, *JORF* n° 0102, 30 avr. 2017, texte n° 6.

À l'instar des *smart grids*, la filiale Vertuoz d'Engie, a conçu une infrastructure *blockchain* sur un réseau de capteurs d'eau et d'électricité connectés qui permet de surveiller et de piloter à distance les installations, ainsi que d'effectuer les opérations de maintenance nécessaires[764]. Par le biais de *smart contracts*, le réseau propose, par exemple, de contacter automatiquement un dépanneur en cas de fuite et de planifier son intervention[765], de mettre en œuvre des stratégies d'économies d'énergie auto-exécutées, et en particulier d'initier des opérations d'autoconsommation individuelles ou collectives sur le principe des art. L. 315-1, et L. 315-1 et s. du C. énergie. Un projet annexe, « Flexigazelec », vise d'ailleurs à expérimenter l'autoconsommation collective d'électricité dans quatre-vingt-seize logements de la ville de Nice à partir de chaudières à co-génération, dont la partie contractuelle concernant les échanges P2P et les excédents de production d'énergie récupérés par le réseau est auto-gérée par une *blockchain*[766].

87. Le projet d'un *smart grid* international. Alors que nombreuses expérimentations d'autoconsommation voient le jour à travers le monde (*RENeW Nexus* en Australie, *Jouliette* aux Pays-Bas, *Conjoule* en Allemagne, *WePower* à Gibraltar, etc.[767]), l'organisation mondiale à but non-lucratif *Energy Web Fondation* travaille actuellement sur un projet d'interopérabilité des solutions de *smart grids* au niveau international[768]. En mutualisant les ressources financières et techniques de la plupart des

[764] V. notamment, « Imaginer aujourd'hui les solutions smart de demain au service de l'efficacité énergétique », *Engie* [en ligne], Menu > Solutions innovantes > Dossiers thématiques, https://www.engie-cofely.fr.

[765] Pour plus de détails, v., blockchain-studio.com ; Futurs, « Futurs et Engie lancent Blockchain Studio à #VivaTech », *Medium* [en ligne], 22 mai 2018, https://medium.com/futurs-io/futurs-et-engie-lancent-blockchain-studio-%C3%A0-vivatech-8c31e02d8a60.

[766] V. notamment, « Faire décoller l'auto-consommation électrique grâce à un bon pilotage ! », *Engie Vertuoz* [en ligne], 7 juin 2019, https://www.engie-vertuoz.fr/blog/autoconsommation-bon-pilotage/ ; « Quand l'énergie se connecte à la blockchain ! », *Engie Vertuoz* [en ligne], 7 juin 2019, https://www.engie-vertuoz.fr/blog/energie-connexion-blockchain/.

[767] Pour une présentation des projets existants en la matière et déployés en collaboration avec Energy Cities, v., « Blockchain et transition énergétique : quels enjeux pour les villes ? », Energy Cities [en ligne], janv. 2019, pp. 7 et s., https://energy-cities.eu/wp-content/uploads/2019/01/energy-cities-etude-blockchain_2018_fr.pdf. – V. également les projets du PNUD (Programme des Nations unies pour le développement) au Liban, pays victime de fréquentes pénuries d'électricité, SONNET (François), « Blockchain-Enabled Solutions for the Uptake of Renewables Energy in Lebanon », UNDP [online], 26 Nov. 2020, https://www.lb.undp.org/content/dam/lebanon/docs/2020/Publications/CEDRO%20_%20Blockchain%20Report%2025.11.2020_for%20publication.pdf. – En Inde, a été initié un projet pilote de plateforme compatible avec la *blockchain* et dédiée à la gestion de l'énergie produite par les panneaux solaires installées sur les toits des bâtiments de la ville de Lucknow (Inde). Ce projet est porté par les entreprises Uttar Pradesh Power Corporation (UPPCL), Madhyanchal Vidyut Vitran Nigam Limited (MVVNL), et Uttar Pradesh New and Renewable Energy Development Agency (UPNEDA). Pour plus de details, v. notamment, NAIR (Rahul), « Uttar Pradesh Starts India's First Blockchain-Enabled Rooftop Solar Trading Platform », *Mercom India* [online], 18 Dec. 2020, https://mercomindia.com/uttar-pradesh-blockchain-rooftop-solar-trading/.

[768] Items International, « Actualités. Blockchain dans le domaine de l'énergie : où en est-on ? », *Think Smartgrids* [en ligne], 7 mars 2019, https://www.thinksmartgrids.fr/actualites/blockchain-domaine-energie.

entreprises du secteur, elle ambitionne de créer un nouveau système énergétique fondé sur des réseaux autonomes et potentiellement gérés par des *smart contracts*[769]. Parmi ses membres, la société allemande Tennen a lancé un projet sur la *blockchain Hyperledger Fabric* de la Fondation Linux visant à automatiser la gestion et l'échange de l'électricité autoproduite au sein de la *sonnenCommunity*. En plus de mettre en œuvre un réseau d'autoconsommation, Tennen constitue le premier système de redistribution et de stabilisation des réseaux d'énergie électrique à l'échelle de l'Allemagne, et projette de l'étendre dans toute l'Europe[770].

B. Le projet d'une « blockchain de centaines de milliards d'objets »[771]

88. ADEPT, un projet décentralisé et interopérable. Partant du constat selon lequel une approche centralisée pour la construction d'un « *Internet of hundreds of billions of things* »[772] impose des frais élevés, manque de confidentialité et n'est finalement pas réalisable d'un point de vue technique[773], la société IBM s'est associée à la société sud-coréenne *Samsung* pour créer une preuve de concept pour leur plateforme « ADEPT »[774], qui utilise la *blockchain* du *Bitcoin* afin de construire un réseau distribué et transparent de périphériques – une forme d'IoT décentralisé[775]. Le projet ADEPT (*Autonomous Decentralized Peer-To-Peer Telemetry*) est basé sur un ensemble de trois protocoles lui assurant à la fois une certaine sécurité et des coûts de production abordables, à savoir, *BitTorrent* qui est un protocole de partage de fichiers, *Ethereum* qui héberge les *smart contracts* et permet donc l'autonomisation du réseau, et *TeleHash* qui est une messagerie

---

[769] *Id.* – Une étude a été menée par une équipe de chercheurs anglaise, dévoilant que la technologie *blockchain*, et notamment dans sa version automatisée (*smart contract*) dispose d'un fort potentiel en matière énergétique, bien qu'il soit encore trop tôt pour préjuger de ses capacités à mener, à si grande échelle, une révolution du système. V., ANDONIA (Merlinda), ROBUA (Valentin), FLYNNA (David) *et al.*, « Blockchain technology in the energy sector: A systematic review of challenges and opportunities », *in* FOLEY (Aoife M.) (dir.), *Renewable and Sustainable Energy Reviews*, éd. Elsevier, Vol. 100, Feb. 2019, pp. 143-174.

[770] Items International, art. cit.

[771] IBM, « ADEPT: An IoT Practitioner Perspective – Draft Copy For Advance Review », *IBM* [en ligne], 10.3 version, 2015, p. 2, http://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/55f73e5ee4b09b2ff5b2eca/55f73e72e4b09b2bff5b3267/1442266738638/IBM-ADEPT-Practictioner-Perspective-Pre-Publication-Draft-7-Jan-2015.pdf?format=original.

[772] IBM, « ADEPT: An IoT Practitioner Perspective – Draft Copy for Advance Review », préc., p. 2.

[773] IBM, Executive report, « Device democracy Saving the future of the Internet of Things », préc. – Sur la solution de la decentralization, *supra* n°s 73 et s.

[774] IBM, « ADEPT: An IoT Practitioner Perspective – Draft Copy For Advance Review », préc., pp. 2-3 : « *In building a proof of concept for a decentralized* IoT, *we wanted to establish a foundation on which to build and to prove several key capabilities. These include: 1. Distributed Transaction Processing & Applications:* […]. *2. Robust Security:* […]. *3. Privacy By Design & Default:* […]. »

[775] HALLORAN (Mickael), « Blockchain, Mobile and the Internet of Things », *Insights* [online], 17 Mar. 2016, https://insights.samsung.com/2016/03/17/block-chain-mobile-and-the-internet-of-things/.

cryptée[776]. Après avoir rempli la condition de la décentralisation, il leur a fallu créer un protocole interopérable. ADEPT a donc été programmé pour reconnaître les technologies des dispositifs électroniques de différents constructeurs, et ainsi d'en former un réseau capable de se maintenir de manière autonome et d' « inspirer une confiance évolutive »[777]. En principe, les appareils électroménagers seraient en mesure de signaler leurs dysfonctionnements et d'effectuer les mises à jour de logiciels dont ils ont besoin. L'objectif du projet est finalement de construire une « *Economy of Things* », autrement dit une architecture fondée sur le partage, constituée d'objets évoluant en autonomie et créant de la valeur économique au sein de marchés à la fois financiers et non-financiers[778].

89. L'objet comme initiateur de la relation contractuelle : l'interaction Homme-machine. En collaboration avec *Samsung*, les équipes d'IBM ont identifié plusieurs cas d'usage qu'ils expérimentent depuis 2016[779], notamment l'appareil autonome (« *standard* ») et l'appareil d'auto-verrouillage tel que la serrure de porte « intelligente » (« *light device* »)[780].

En ce qui concerne plus particulièrement la fonction « *standard* » de la plateforme, il s'agirait selon IBM France d'un lave-linge, en l'occurrence une machine *Samsung W9000* créée spécialement pour le projet, qui, « grâce au *Smart Contract*, […] va commander la lessive qui sera livrée automatiquement afin de ne pas être en rupture de stock […] et pourrait gérer sa maintenance en avertissant le réparateur de l'usure des pièces à changer », ajoutant que l' « on peut imaginer d'organiser ainsi une délégation de paiement contractualisée, […] le propriétaire [étant] bien sûr averti de chaque transaction »[781]. D'après les développeurs, connectée à ADEPT, la machine serait

[776] « IBM y Samsung: la cadena de bloques de Bitcoin para un Internet de las Cosas descentralizado (Adept) », *Oroy Finanzas* [en línea], 22 En. 2015, https://www.oroyfinanzas.com/2015/01/ibm-samsung-cadena-bloques-bitcoin-internet-de-las-cosas-descentralizado-adept/. – D'après certains auteurs, pourrait être un *fork* (un *fork* est une fourche, c'est-à-dire une nouvelle version d'un protocole dérivée du protocole existant d'*Ethereum* créé par IBM [« [R&D] ADEPT : Le projet IOT de IBM & Samsung utilisant Ethereum », *CryptoFR* (forum) [en ligne], https://cryptofr.com/topic/907/r-d-adept-le-projet-iot-de-ibm-samsung-utilisant-ethereum]. – Pour une définition plus détaillée du *fork*, *infra* n^{os} 321 et s.

[777] IBM, « ADEPT: An IoT Practitioner Perspective – Draft Copy for Advance Review », préc., p. 7.

[778] *Ibid.*, préc., pp. 2-3 : « *Finally, we believe the* IoT *will create an Economy of Things. Every device, every system can be a point of transaction and economic value creation for owners and users. Every device should be able to engage in multiple markets, both financial and non-financial and should be able to autonomously react to changes in markets. These capabilities will be crucial to everything from the sharing economy to energy efficiency and distributed storage. While not every one of these principles is fully developed in our proof of concept, we believe the architecture we have developed reflects those goals and is capable of implementation as we expand the capability of our solution*. »

[779] DAVIES (Alex), « IBM and Samsung unveil ADEPT blockchain proof of concept for IoT », *ReTHINK* [online], 22 Jan. 2015, https://rethinkresearch.biz/articles/ibm-samsung-unveil-adept-blockchain-proof-concept-iot-security/.

[780] IBM, « ADEPT: An IoT Practitioner Perspective – Draft Copy for Advance Review », préc., p. 12.

[781] GENESTIER (Philippe) *et al.*, art. cit., p. 70.

capable de détecter non seulement le niveau d'approvisionnement en lessive[782], mais également, par exemple, en interrogeant sa propre liste d'homologues, d'exécuter un certain nombre de tâches. Elle pourrait donc déterminer s'il existe un précédent contrat entre son propriétaire et un détaillant de lessive, demander un réapprovisionnement de certaines marchandises au fournisseur *via* la messagerie, invoquer le contrat et effectuer un paiement pour la commande, ou encore prévenir le propriétaire qu'une commande de réapprovisionnement est en cours[783]. Parallèlement, le détaillant aurait la possibilité, *via* la plateforme ADEPT, de vérifier la validité du *smart contract* initié par la machine, de recevoir le paiement, de communiquer à la machine *via* le service de messagerie la date de livraison estimée ainsi que divers détails concernant le *smart contract*. Une fois la commande confirmée, le propriétaire est censé recevoir un message de confirmation avec les détails de livraison sur son téléphone[784]. On constate l'existence d'une transformation du rôle de l'utilisateur qui, en plus d'être consommateur, devient également fournisseur en consommables de sa propre machine[785].

Par ailleurs, la machine serait également en mesure de gérer ses propres informations concernant son identifiant, sa garantie, ses propres analyses intégrées, notamment afin d'évaluer la performance d'une pièce ou d'un composant[786]. L'idée est qu'en cas de panne, celle-ci puisse formuler instantanément une demande de service de réparation[787]. Pour cela, la machine doit, seule, pouvoir identifier un fournisseur de service approprié et émettre une demande de devis auprès du professionnel sélectionné qui dispose de l'ensemble des informations nécessaires sur la *blockchain*. Plus encore, la machine pourrait mettre en relation le propriétaire et le dépanneur, et formuler l'accord sous la forme d'un *smart contract* que le propriétaire pourrait vérifier avant d'accepter. Le programme doit également pouvoir contrôler l'état de garantie de la machine pour exiger ou non que la réparation soit acquittée. Dès le contrat formé, le dépanneur tiendrait informé le propriétaire et s'entendrait avec lui pour fixer la date de livraison de la prestation *via* la machine elle-même[788]. Force est de constater que la machine s'apparente à un intermédiaire, sans toutefois reproduire le rôle des actuels intermédiaires de confiance.

---

[782] HIGGINS (Stan), « IBM Reveals Proof of Concept for Blockchain-Powered Internet of Things », *CoinDesk* [online], 17 Jan. 2015, https://www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things/.
[783] *Id.*
[784] IBM, « ADEPT: An IoT Practitioner Perspective – Draft Copy for Advance Review », préc., p. 13.
[785] *Ibid.*, pp. 70-71.
[786] *Ibid.*, p.14.
[787] DAVIES (Alex), préc.
[788] IBM, « ADEPT: An IoT Practitioner Perspective – Draft Copy for Advance Review », préc., p. 14.

90. L'objet comme initiateur de la relation contractuelle : l'interaction machine-machine. Les appareils pourraient également utiliser ADEPT pour interagir de manière autonome avec d'autres objets de la maison placés à proximité afin de faciliter l'échange et l'efficacité énergétique[789], et notamment pour qu'ils régulent ensemble leur consommation en électricité[790]. Techniquement, il s'agirait d'une négociation entre le lave-linge qui, par exemple, demanderait au téléviseur sa mise hors tension le temps d'un cycle de lavage. Si celui-ci refuse, il adresserait alors à la machine un *token* (jeton) pour qu'elle retarde son cycle de quelques heures. Les concepteurs vont même jusqu'à imaginer une machine capable de négocier seule avec un micro-réseau électrique de quartier à l'image des *SmartGrids*[791].

91. Limites de l'auto-exécution dans les relations contractuelles. À notre sens, la machine ne doit cependant pas être en mesure de s'auto-gérer au point de pouvoir conclure le contrat seule. Elle peut en effet initier la relation contractuelle entre son propriétaire et le ou les cocontractants qu'elle a sélectionnés, ou encore formuler une version possible du contrat et des obligations tenant à chaque partie. Mais, cette phase préparatoire ne doit pas permettre à la machine d'être en situation de consentir à l'acte juridique au nom et pour le compte du propriétaire, au risque de se substituer à lui et, *in fine*, de se substituer à l'Homme.

En ce sens, le dédoublement de la personnalité juridique qui serait ainsi opéré par la machine conduirait à étudier l'analogie avec le contrat de mandat (C. civ., art. 1984 et s.). Seulement la *summa divisio* ne connaît que les « personnes » (*personae*) ou les « choses » (*res*). Or, le mandataire ne peut être une chose, puisque l'art. 1984 du C. civ. spécifie expressément qu'il est « une personne », devant de surcroît manifester la volonté de s'engager dans un tel contrat[792], ce dont une machine est, en l'état actuel, incapable. La position de la machine en tant qu'intermédiaire entre le propriétaire et le professionnel ne peut, de la même manière, être rapprochée de celle du courtier, puisque celui-ci exerce

[789] « IBM y Samsung: la cadena de bloques de Bitcoin para un Internet de las Cosas descentralizado (Adept) », préc.
[790] *Ibid.*, p. 15.
[791] Sur les *smart grids*, *supra* n° 86. – V. également, *ibid.*, p. 16.
[792] L'art. 1984 du C. civ. dispose en effet que « le mandat ou procuration est un acte par lequel une personne donne à une autre le pouvoir de faire quelque chose pour le mandant et en son nom. Le contrat ne se forme que par l'acceptation du mandataire ». Un auteur constate d'ailleurs qu' « en confiant au mandataire le pouvoir de le lier, le mandant dédouble sa personnalité juridique, et confie sa volonté à la volonté d'un autre. Le mandataire, en effet, n'est pas un simple porte-parole : il exerce sa propre volonté, dans l'intérêt d'autrui » [AYNÈS (Laurent), « La révocabilité du mandat irrévocable », *D.* 2002, n° 37, p. 2858].

une activité commerciale indépendante[793]. De plus, le régime du contrat de courtage impose à la fois au courtier d'être en mesure d'engager sa responsabilité en cas de défaut d'information[794], mais exige également du donneur d'ordres une rémunération du courtier[795]. Or, ces deux caractéristiques sont invraisemblables dans le cas d'une machine. Plus encore, cette situation serait contraire à l'intention originelle de la *blockchain* qui a toujours été de s'autonomiser et *a fortiori* d'autonomiser l'Homme dans ses relations contractuelles vis-à-vis des tiers de confiance, et non de remplacer l'Homme.

Parce que la technologie doit faciliter la vie de l'Homme et non l'aliéner, il s'agira pour ces systèmes de veiller à recueillir le consentement du propriétaire au cas par cas, de sorte que l'acceptation de l'offre de contrat proposée par la machine soit conforme aux exigences de l'art. 1113, al. 1er, du C. civ. La machine pourra toutefois accomplir les formalités de paiement et autres exigences administratives prévues et validées par les cocontractants afin de finaliser le contrat, éventuellement munie d'une forme de délégation sur ces aspects.

92. Force est de constater que désormais, par le biais de l'interconnexion des technologies, une confiance triangulaire s'est instaurée entre les cocontractants et les algorithmes, de sorte que, finalement, la technologie devient à la fois un instrument et une garantie tantôt virtuelle tantôt physique de l'exécution du contrat. *A fortiori*, elle impose le respect des règles d'organisation de la vie en société établies par le contrat social, aboutissant à l'adoption des règles de droit[796] et contribuant à l'amélioration des relations entre les Hommes. En sous-traitant le processus, suivi ou instantané, d'exécution contractuelle à une suite de 0 et de 1[797] réputée neutre grâce à l'utilisation de la *blockchain*, l'impératif de confiance entre cocontractants – presque condition *sine qua non* de la relation –, est minimisé, au profit d'un renforcement des engagements.

---

[793] GUEZ (Philippe), « Contrat de courtage », *JCl. Contrats-Distribution*, fasc. 850, n° 6.
[794] Le courtier est tenu d'une « obligation générale d'information » concernant la personne du cocontractant proposé et concernant l'opération juridique envisagée. V., *ibid*, n°s 29 et s. – V. également, Cass. Civ. 1ère, 11 mars 2010, n° 09-11.383 ; CA Paris, 26 déc. 1929, *Gaz. Pal*. 1932, 2, p. 563 (sur l'identité du cocontractant ; responsabilité engagée du courtier qui a mis en contact le donneur d'ordre avec une société, sans vérifier si ladite société était inscrite au registre du commerce) ; CA Douai, 3e Ch., 15 sept. 2011, n° 10/02244 ; Cass. Civ. 1ère, 10 nov 1964 : *JCP* 1965, II, 13981 (sur l'obligation de conseil et de mise en garde du courtier relative à l'opération juridique projetée).
[795] GUEZ (Philippe), *op. cit.*, n°s 38 et s. – V. également, Cass. Com., 28 févr. 1984, JurisData n° 1984-700296.
[796] FABRE-MAGNAN (Muriel), « Chapitre V. La justice », *in* FABRE-MAGNAN (Muriel), *Le droit des* contrats, éd. Presses Universitaires de France, coll. « Que sais-je ? », 2018, pp. 121-122.
[797] Logique binaire propre aux systèmes de traitement de l'information.

93. Bien qu'initialement liée à la crypto-monnaie, il est désormais indéniable que la technologie soit parvenue depuis à se développer au-delà de *Bitcoin*[798]. Outre l'aspect « auto-exécuté » prometteur en matière contractuelle, une autre facette de la *blockchain* est elle aussi envisagée, proposant à la fois de stocker et de transmettre le contrat numérisé et signé en toute sécurité : il s'agit de sa qualité de registre distribué et décentralisé (*ledger*).

[798] GALEON (Dom), HOUSER (Kristen), « IBM Just Launched Blockchain Beyond Currency », *Futurism* [online], 22 Mar. 2017, https://futurism.com/ibm-just-launched-blockchain-beyond-currency/.

TITRE 2. La *blockchain* : promesse d'une sécurité juridique accrue

94. « *Verba volant, scripta manent* », « Les paroles s'envolent, les écrits restent ». Si ce proverbe latin, supposément prononcé par le sénateur Caius Titus lors d'un discours devant le Sénat romain[799], a subsisté à travers les siècles jusqu'à être encore d'actualité de nos jours, c'est dire la vérité qu'il renferme. Parfois exigé *ad validitatem*, parfois simplement essentiel *ad probationem*, l'écrit est le premier mode de preuve inscrit au Code civil. À l'ère de la digitalisation, le législateur français de 2001[800] a fait entrer dans le régime du droit de la preuve l'écrit électronique, et donc immatériel. Aujourd'hui, le support, papier ou électronique, de la preuve littérale est indifférent en ce que celle-ci, consiste, en vertu de l'art. 1365 du C. civ., « en une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible ». La force probante de l'écrit électronique est donc légalement admise. Une double condition s'ajoute cependant, à savoir, d'une part, « que puisse être dûment identifiée la personne dont il émane » et, d'autre part, « qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité »[801]. Reste donc à savoir si la technologie *blockchain* est capable de remplir les exigences d'imputabilité et d'intégrité visées par ce texte.

Bien que les procédés d'identification des informations inscrites sur les *blockchains* ne soient pas parfaitement identiques à ceux des signatures électroniques circulant actuellement sur le marché, ils constituent une variété de signature existante qu'il convient d'évaluer (Chapitre 1).

La qualité de « registre décentralisé » de la technologie rend par ailleurs possible la traçabilité, tant des actions que des dates auxquelles ces dernières ont été effectuées. Elle assure en cela un archivage pour une durée en principe illimitée, contribuant ainsi à créer une nouvelle variété de preuve algorithmique de faits mais également d'actes juridiques (Chapitre 2).

[799] GRIGORIEFF (Nathan), *Citations latines expliquées*, éd. Eyrolles, 2003.
[800] Décr. n° 2001-272, 30 mars 2001, pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, *JORF* n° 0077, 31 mars 2001, texte n° 19.
[801] C. civ., art. 1366.

Chapitre 1. Une variété de signature électronique existante

95. *A priori*, la *blockchain* semble parfaitement épouser les caractéristiques de la signature électronique actuelle[802] puisqu'elles ont toutes deux en commun d'être basées sur les mêmes mécanismes cryptographiques, qui sont d'ailleurs la clé de leur conception et de leur sécurisation (Section 1). Toutefois, c'est en s'imprégnant davantage des fonctions légalement attendues d'une signature électronique qu'un élément non des moindres de la *blockchain* semble, en l'état actuel, faire défaut. Il s'agit de l'identification du signataire. En effet, les systèmes d'authentification divergent selon la technologie utilisée et la *blockchain* devra en particulier supporter le poids d'une de ses exigences originelles à savoir, la « pseudonymisation » (Section 2). L'étude s'orientera alors vers la recherche de solutions afin de contrer ce potentiel obstacle.

Section 1. Des mécanismes cryptographiques identiques : l'avantage de la sécurisation

96. Préalablement la confrontation du procédé de signature fournie par la *blockchain* avec les caractéristiques requises, notamment, par l'art. 1367 du C. civ. visant à évaluer la fiabilité de son procédé (§ 2), il est nécessaire d'approfondir les notions techniques intervenant au sein de la technologie *blockchain* afin de mieux appréhender ses spécificités et son potentiel en matière de signature électronique (§ 1).

§ 1. La technicité du procédé de signature *via blockchain*

97. À l'image de l'utilisation d'un grand livre sûr et immuable, l'usage de la *blockchain* facilite le partage sécurisé des données inscrites sur ses pages. Cette caractéristique découle de l'alliance de deux procédés informatiques pouvant s'apparenter aux différentes étapes de la formation d'un contrat. Il s'agit, d'une part, de la cryptographie asymétrique, fondée sur une logique identique à celle de l'offre et de l'acceptation contractuelle (A) et, d'autre part, des mécanismes de hachage, permettant à la fois l'authentification des cocontractants et l'intégrité des informations inscrites (B).

[802] LEGEAIS (Dominique), « Blockchain », *JCl. Sociétés Traité*, fasc. 2160, n° 29.

98. Fondements de la cryptographie. Les fondements de ce procédé reposent sur un problème de mathématiques largement utilisé dans l'univers de l'informatique qui consiste en la métaphore du problème des généraux byzantins, évoquant la recherche de fiabilité dans n'importe quelle transmission à travers l'intégrité des interlocuteurs[803]. L'énoncé du problème est le suivant : plusieurs généraux de l'armée byzantine ont planté leurs campements autour d'une cité ennemie et entament un siège. Ils n'ont pas d'état-major et leur seul moyen de communication est de recourir aux services de messagers. Les différents généraux doivent malgré tout organiser une offensive commune, faute de quoi la défaite sera inéluctable. Seulement, certains de ces messagers sont soupçonnés d'être des traîtres dont la mission est de semer la confusion pour faire échouer le plan de bataille des généraux. Il s'agit alors de trouver un mode de communication qui soit infalsifiable, capable de prévenir toute interception voire corruption par l'ennemi des données communiquées.

Il a été démontré que le problème pouvait être entièrement résolu avec des messages écrits et non falsifiables, mais également avec des messages uniquement oraux si, et seulement si, plus des deux tiers des messagers sont loyaux[804]. Ces deux hypothèses correspondent au concept originel d'une technologie immuable et distribuée, initiée par le protocole *Bitcoin* de Satoshi Nakamoto[805] et applicable à tous types d'informations. Fondée sur des techniques de cryptographie, la *blockchain* propose en effet de garantir le secret et l'intégrité des termes d'une écriture inscrite sur un bloc et ce, sans autorité centrale de supervision[806]. Précisément, et pour ce qui concerne l'analyse subséquente[807], l'immuabilité des informations repose sur l'usage de la cryptographie asymétrique, qui constitue, conformément à l'art. 29, al. 1er de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, un procédé de chiffrement mathématique par clés, intimement liée à la fonction de hachage informatique[808].

---

[803] MEKKI (Mustapha), « Les mystères de la blockchain », *D*. 2017, n° 37, pp. 2160 et s., n° 8.

[804] LAMPORT (Leslie), SHOSTAK (Robert), PEASE (Marshall), « The Byzantine Generals Problem », *ACM Transactions on Programming Languages and Systems*, 1982, Vol. 4, No. 3.

[805] LEE (David), CHUEN (Kuo), DENG (Robert H.), *Handbook of Blockchain, Digital Finance, and Inclusion: vol. 2:ChinaTech, Mobile Security, and Distributed Ledger*, ed. Academic Press, 2017, p. 161.

[806] Cité dans : PRISCO (Giulio), « Bitcoin 2.0 Will Be a Very Big Deal », *CCN* [online], 27 Oct. 2014, https://www.ccn.com/bitcoin-2-0-will-big-deal/. – V. également, PRISCO (Giulio), « Fixing The Internet With The Blockchain », *CCN* [online], 25 Sept. 2014, https://www.ccn.com/fixing-the-internet-with-the-blockchain/.

[807] Sur le principe de distributivité de la *blockchain*, *infra* n°s 142 et s.

[808] La cryptographie correspond à un « moyen de cryptologie », c'est-à-dire « tout matériel ou logiciel conçu ou modifié pour transformer des données, […] à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur

99. Définition générale de la cryptographie asymétrique. La cryptographie asymétrique en dehors de la *blockchain* se distingue fondamentalement de la cryptographie symétrique, au travers de laquelle les deux parties à une quelconque transaction choisissent conjointement le code de chiffrage/déchiffrage du message échangé, en d'autres termes la clé[809]. En cryptographie asymétrique, l'hypothèse commune est qu'un message doit pouvoir être échangé, alors même que les deux parties à la transaction ne se connaissent absolument pas. Cette hypothèse est inimaginable en matière de cryptographie symétrique[810]. Schématiquement, il s'agit d'un échange tel que l'expéditeur doit pouvoir rendre secret son message *via* un calcul complexe, et le destinataire vérifier la méthode de ce calcul pour garantir que l'expéditeur est bien l'auteur du message, et ensuite ouvrir le message[811]. Cette technique permet d'authentifier tant le contenu que l'origine du message. Pour cela, elle met à disposition de chaque utilisateur deux clés cryptographiques associées[812], à savoir une clé nommée « clé publique » qui a vocation à générer une « adresse » publique connue de tous – ce qui implique qu'aucun échange de clé préalable à l'échange d'informations n'est nécessaire[813] –, et une autre clé nommée « clé privée », autrement nommée « convention secrète » par le législateur[814], et qui doit impérativement rester confidentielle[815]. Pour imager, l'adresse « publique » dérivée de la clé publique est à quelques chiffres près la boîte-aux-lettres[816], la clé privée correspond au mot de passe pour ouvrir/fermer la boîte

confidentialité, leur authentification ou le contrôle de leur intégrité. » [L. n° 2004-575, 21 juin 2004, pour la confiance dans l'économie numérique, *JORF* n° 0143, 22 juin 2004, texte n° 2, art. 29, al. 1er].

809 FOUQUE (Pierre-Alain), *Cryptographie appliquée*, éd. Techniques Ingénieur, 2002, pp. 16-17.

810 LEGEAIS (Dominique), *op. cit.*, n° 2.

811 MOUTON (Dimitri), *Sécurité de la dématérialisation : De la signature électronique au coffre-fort numérique, une démarche de mise en œuvre*, éd. Eyrolles, coll. Solutions d'entreprise, 2012, p. 27.

812 En pratique, le portefeuille de *bitcoins* ou d'une autre crypto-monnaie (*wallet*) contient une « clé maître » générée à partir d'une « graine » (*seed*). Les propriétés des courbes elliptiques permettent de dériver de nouvelles clés à partir de la clé maître et donc de la graine. C'est ainsi que, de cette clé maître, sont généralement dérivées *n* « sous-clés », correspondent aux bi clés composés d'une clé publique et d'une clé privée. Pour connaître la valeur d'un *wallet*, il faut donc additionner l'ensemble des crypto-monnaies inscrites dans chacune des sous-clés publiques.

813 FOUQUE (Pierre-Alain), *op. cit.*, p. 14.

814 L. n° 2004-575, préc., art. 29, al. 1er.

815 MOUTON (Dimitri), *op. cit.*, p. 27.

816 La boîte aux lettres constitue l'adresse publique générée à partir de la clé publique, elle-même générée à partir de la clé privée, le tout généré grâce à une fonction mathématique nommée « fonction de hachage ». Une confusion existe mais, tel que Vitalik Buterin le souligne, celle-ci est globalement acceptée et utilisée au sein de la communauté [v., BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », *github* [liens de publication originaux supprimés] [online], Nov. 2013, https://github.com/ethereum/wiki/wiki/White-Paper. Trad. : Asseth (Stéphane Roche, Jean Zundel, Frédéric Jacquot, Alexandre Kurth et Etienne Jouin), v., http://www.asseth.fr/2016/11/09/traduction-whitepaper-ethereum/] : « Un lecteur averti notera qu'en pratique, une adresse *Bitcoin* est l'empreinte de la clé publique de courbe elliptique, et non la clé publique elle-même. Cependant, il est parfaitement admis en terminologie cryptographique d'assimiler l'empreinte de la clé publique à la clé publique elle-même. En effet, la cryptographie *Bitcoin* peut être considérée comme un algorithme de signature numérique particulier, où la clé publique est constituée de l'empreinte de la clé publique ECC, où la signature représente la clé publique ECC concaténée avec la signature ECC,

aux lettres et y déposer l'objet de l'opération, et l'une comme l'autre sont indispensables pour effectuer cette opération[817]. Ainsi, pour chiffrer un message et l'envoyer à un autre utilisateur, l'expéditeur chiffre à l'aide de l'adresse « publique » du destinataire, et pour déchiffrer ledit message, le destinataire utilise à l'inverse sa clé privée associée. De cette manière, la confidentialité du message est assurée car il ne peut être lu que par le destinataire propriétaire du jeu de clés publique/privée[818].

100. La cryptographie asymétrique appliquée à la *blockchain* : notions de clés, d'adresses et de transactions. Puisque Satoshi Nakamoto a généré ces dispositifs avant d'alimenter – de près ou de loin – les protocoles des différentes générations de *blockchains* actuelles, il apparaît admissible de fonder cette présentation sur les mécanismes développés pour la *blockchain* du *bitcoin*. Ainsi, si auparavant les utilisateurs du protocole *Bitcoin* ne disposaient que d'une seule clé privée associée à une clé publique et à une adresse, la pratique et le besoin de sécurité ont nécessité quelques changements. Après plusieurs mises à jour, nommées « BIP » au sein de la communauté (« *Bitcoin improvement protocols* », qui correspondent à des « protocoles d'amélioration de Bitcoin »[819]), le fonctionnement des *wallets* a été entièrement remanié. Désormais, l'inscription à un portefeuille *Bitcoin*[820] entraine la création automatique d'une « *root seed* », c'est-à-dire une graine primaire/de récupération, renfermant l'intégralité des *bitcoins* sauvegardés sur la chaîne par son détenteur[821]. Cette *root seed* est transmise à l'utilisateur au moment de son inscription, et seulement à ce moment. Il doit alors la mémoriser, sinon en prendre note, avec prudence étant donné son extrême importance et vulnérabilité. Ensuite, le *wallet* dérive de cette *root seed* un jeu de clés (bi-clés), c'est-à-dire une clé publique et une clé privée associée[822]. De ce couple de clés, nommé « parent » ou « principal », sont ensuite à nouveau dérivés un nombre de bi-clés appelés

et où l'algorithme de vérification consiste à valider la clé publique ECC dans la signature avec l'empreinte de la clé publique ECC fournie en tant que clé publique pour ensuite valider la signature ECC avec la clé publique ECC. ». Cette fonction de hachage est à sens unique, ce qui signifie que personne ne peut calculer la clé publique à partir de l'adresse publique, ou même la clé privée à partir de la clé publique. – Pour une étude détaillée de la fonction de hachage, *infra* n°s 104-106.

[817] BARRAUD (Boris), « Les blockchains et le droit », *RLDI* 2018/4, nº 147, p. 2.

[818] À titre d'exemple, Louis doit valider une demande de crédit auprès de sa banque. Pour ce faire, cette dernière va lui transmettre un document sécurisé, le principe étant qu'un message codé avec une clé privée ne peut être décodé que par la clé publique qui lui est associée, et inversement. Ainsi, la banque va crypter son propre message avec la clé publique de Louis. Par conséquent, seul Louis pourra décrypter le message de la banque puisque seul lui possède la clé privée associée à la clé publique utilisée.

[819] L'intégralité de ces mises à jour sont disponibles sur GitHub à l'adresse : https://github.com/bitcoin/bips.

[820] L'utilisation d'un *wallet* n'est pas obligatoire, mais elle est fortement conseillée pour des raisons de sécurité et de protection des clés privées.

[821] MAGUAYO, « Update bip-0032.mediawiki », *GitHub* [online], 25 Oct. 2018, https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki#Specification_Key_.

[822] V., Annexe n° 6. Schéma exposant la provenance des bi-clés, p. 438.

« enfants »[823]. Par habitude, les utilisateurs du protocole *Bitcoin* font souvent référence au fait de « transmettre la clé publique » afin de percevoir le fruit d'une « transaction de *bitcoins* ». En réalité, il s'agit de transmettre aux potentiels émetteurs le dérivé de la clé publique, appelée « *Public Key Hash* », qui correspond alors à une adresse *Bitcoin*[824]. Ainsi, *a priori* la clé publique n'est effectivement pas connue de tous, et l'adresse est quant à elle le plus souvent « jetable » en ce que l'utilisateur est vivement incité à fournir une nouvelle adresse à chaque nouvelle utilisation, afin d'éviter tant que faire se peut tout risque de traçage[825]. Cette règle de fonctionnement a souvent été reprise par les *blockchains* qui ont été créées par la suite. En parallèle, prouver la détention d'une adresse pour envoyer des *bitcoins* ou pour récupérer les *bitcoins* transférés par transaction ne requiert plus du destinataire la saisie de sa clé privée associée à l'adresse d'envoi ou de réception puisqu'en règle générale, le *wallet* se charge de la gestion des clés privées associées à chaque adresse du compte utilisateur[826]. De cette manière les clés privées ne sont, en principe, jamais diffusées.

101. Quelle qualification juridique pour la « transaction de *bitcoins* » ? Il faut remarquer que du point de vue juridique, le terme « transaction » n'a effectivement pas la même portée. D'une part, il ressort du vocabulaire purement commercial que la « transaction » équivaut davantage à une acception stricte de l'idée de « négociation »[827],

---

[823] Pour plus de précisions techniques, v., MAGUAYO, « Update bip-0032.mediawiki », art. cit., notamment : « *In what follows, we will define a function that derives a number of child keys from a parent key. In order to prevent these from depending solely on the key itself, we extend both private and public keys first with an extra 256 bits of entropy. This extension, called the chain code, is identical for corresponding private and public keys, and consists of 32 bytes.* » ; « *Serialization format - Extended public and private keys are serialized as follows:*

- *4 byte: version bytes (mainnet: 0x0488B21E public, 0x0488ADE4 private; testnet: 0x043587CF public, 0x04358394 private)*
- *1 byte: depth: 0x00 for master nodes, 0x01 for level-1 derived keys, ...*
- *4 bytes: the fingerprint of the parent's key (0x00000000 if master key)*
- *4 bytes: child number. This is ser32(i) for i in xi = xpar/i, with xi the key being serialized. (0x00000000 if master key)*
- *32 bytes: the chain code*
- *33 bytes: the public key or private key data (serP(K) for public keys, 0x00 || ser256(k) for private keys)* ».

[824] DE QUENETAIN (Stanislas), « L'arbre de Merkle : la Colonne Vertébrale de la Blockchain », *Blockchains Experts* [en ligne], 2015, https://www.blockchains-expert.com/larbre-de-merkle-colonne-vertebrale-de-blockchain/.

[825] *Infra* n° 109.

[826] MAGUAYO, « Update bip-0032.mediawiki », art. cit. : « *Because of this construction, knowing an extended private key allows reconstruction of all descendant private keys and public keys, and knowing an extended public keys allows reconstruction of all descendant non-hardened public keys*. »

[827] Le décr. n° 72-678, 20 juill. 1972, fixant les conditions d'application de la L. n° 70-9 du 2 janvier 1970 réglementant les conditions d'exercice des activités relatives à certaines opérations portant sur les immeubles et fonds de commerce, *JORF*, 22 juill. 1972, évoque les « transactions sur immeubles et fonds de commerce ». – V. également, Cass. Civ. 1ère, 14 nov. 2018, n° 16-23.730 (« relève de l'activité de transaction immobilière le fait de prêter son concours, de manière habituelle, même à titre accessoire, à des

qui cesse donc au stade des pourparlers. D'autre part, en droit civil, comme dans d'autres dispositions particulières du droit où il en est question[828], la « transaction » s'apparente au « *settlement* » anglo-saxon, soit le « contrat par lequel les parties terminent une contestation née, ou préviennent une contestation à naître » (C. civ., art. 2044). Simples discussions ou climat de litige, ces acceptions juridiques ne reflètent cependant pas ce que les *bitcoiners* entendent par « transaction de *bitcoins* ».

Afin de s'approcher du sens que *Bitcoin* donne à l'opération effectuée sur son protocole, il semble adéquat de parler d'exécution de prestations, souvent synallagmatiques, que les parties se promettent réciproquement, via échanges de *bitcoins*. Ainsi est-il possible de retrouver dans le mécanisme de *Bitcoin* des principes connus du droit des obligations. Dans les faits, et puisque le protocole *Bitcoin* a été initié pour des paiements, il s'agit la plupart du temps d'une personne qui émet une « requête de paiement » équivalente à une offre ferme et précise à la lecture des articles 1113 et 1114 du C. civ.[829], offre qu'une tierce personne décide d'accepter. Pour cela, l'offrant met à disposition son « adresse publique » soit par e-mail, soit sous la forme d'un *QR code*[830] contenant ladite adresse, mais également d'autres éléments essentiels du contrat envisagé (C. civ., art. 1114) : le montant à accepter, le label du destinataire ainsi que celui du paiement. Par ce biais l'offrant exprime expressément sa volonté d'être lié[831]. Tout utilisateur de la plateforme peut, *via* son portefeuille de *bitcoins*, accepter l'offre émise en sélectionnant l'option « envoyer » vers « l'adresse publique » préalablement reçue, ce qui a pour conséquence d'autoriser la procédure de paiement – sous la forme d'un « *script* » – d'un *wallet* à l'autre. En d'autres termes, à travers cette manipulation l'utilisateur manifeste à son tour sa volonté de s'engager (C. civ., art. 1113, al. 1er). Apparaissent ainsi les notions d'offre et d'acceptation propres au droit des obligations, et *a fortiori* s'impose la notion de contrat (C. civ., art. 1118, al. 1er, et 1121), qui implique la production d'effets de droit entre les parties (C. civ., art. 1103). Par ailleurs et contrairement au déroulé traditionnel, à ce stade de l'opération le *script* de la *blockchain* verrouille automatiquement le montant envoyé à l'aide de l'adresse publique du destinataire. Pour pouvoir le déverrouiller et en bénéficier, l'offrant devra fournir une

opérations portant sur la vente de biens immobiliers ; […] dans la délivrance de conseils à l'occasion d'une vente immobilière, notamment au titre de conseils en investissement ou en défiscalisation »).

828 Par exemple, en matière d'indemnisation des victimes d'accident de la route, est « qualifi[ée] de transaction la convention qui se forme entre la victime et l'assureur » [Cass. Civ. 1ère, 20 janv. 2010, n° 08-19.627], et en droit du travail, « une transaction ne peut avoir pour objet de mettre fin à un contrat de travail » [Cass. Soc., 5 déc. 2012, n° 11-15.471].

829 V. également, concernant les conditions de fermeté et de précision de l'offre, Cass. Com., 29 juin 1993, n° 91-20.380.

830 DE QUENETAIN (Stanislas), « L'arbre de Merkle : la Colonne Vertébrale de la Blockchain », art. cit.

831 *Id.*

solution au *script*. Cette solution n'est autre que la clé privée associée, autrement dit *sa* clé privée.

102. Cependant, rien n'assure que celui qui se dit expéditeur est bel et bien le propriétaire du montant ou en règle générale du message transmis, ni que ce dernier n'a pas été modifié voire corrompu par la suite. De plus, étant donné que la *blockchain* agit sur un réseau public et distribué, et pour les raisons qui s'imposeront à chacun, il est impossible et même proscrit de communiquer sa clé privée sur le réseau pour prouver son authenticité. C'est précisément dans ce contexte que l'utilisation d'un dispositif de signature numérique présente un intérêt manifeste.

B. Authentification et intégrité : l'utilisation des mécanismes de hachage

103. Le principe de la signature *via blockchain*. Andreas M. Antonopoulos indique que l'authentification du contractant sur *Bitcoin* prend la forme d'une « preuve de propriété pour chaque montant […] de *bitcoin input*, dont la valeur est transférée sous la forme d'une signature numérique du propriétaire »[832]. Il ajoute que, « dans le langage *bitcoin*, dépenser c'est signer une transaction qui transfère la valeur d'une transaction précédente à un nouveau propriétaire identifié par une adresse *bitcoin* »[833]. Cette authentification s'effectue donc à travers le dispositif de signature numérique mis en place[834].

L'idée est celle d'un utilisateur qui, de façon à ne pas divulguer sa clé privée secrète sur la *blockchain*, va fournir une signature découlant de ladite clé. En pratique, est joint au message envoyé une signature générée à partir du codage de deux éléments à savoir, le message – lui-même constitué du message initial, de l'adresse « publique » de l'expéditeur et de l'adresse « publique » de son destinataire –, et la clé privée de l'expéditeur[835]. De cette façon, l'utilisateur peut prouver son lien avec le message sans

---

[832] [Trad. : ROBYR (Fabien), [en ligne], 2016, p. 25, https://bitcoin.fr/wp-content/uploads/2016/01/Mastering-Bitcoin.pdf], ANTONOPOULOS (Andreas M.), *Mastering Bitcoin*, ed. O'Reilly, 1st edition, 2014.

[833] *Id.*

[834] V., Annexe n° 7. Schéma de la signature numérique *via blockchain* : l'exemple de *Bitcoin*, p. 439.

[835] En langage algorithmique, cette requête se traduit en deux instructions successives. La première crée la « transaction », autrement dit le message envoyé en clair sur la *blockchain*, *via* « *createrawtransaction* ». Elle requiert, d'une part, une entrée (« *input* »), correspondant au montant total du *wallet*, et, d'autre part, une sortie (« *output* ») correspondant aux montants, à la fois dépensé et envoyé à l'adresse de l'offrant, et non dépensé et réexpédié vers l'adresse initiale. La seconde commande, « *signrawtransaction* », consiste à signer le message en calculant le *hash* de deux éléments réunis, à savoir le *hash* du message envoyé et la clé privée du signataire. – Pour plus de précisions sur le sujet, v., ANTONOPOULOS (Andreas M.), *Mastering Bitcoin*, ed. O'Reilly, 2nd edition, 2017, pp. 50 et s.

mettre en danger sa clé privée. Cette signature va certifier que l'émetteur possédait effectivement la clé privée associée à l'adresse qui a envoyé l'information au moment de l'expédition à l'adresse de réception, sans jamais la laisser apparaître en clair puisqu'elle aura été mélangée à d'autres éléments. De plus, cette signature est unique, il est donc impossible de la falsifier ou d'en reproduire les données de création. Il reste qu'il faille assurer avec certitude l'intégrité de cette signature.

104. Authentifier l'origine du message : calculer l'empreinte du message signé (*hash*). Le codage donnant naissance à la signature numérique est permis grâce à une fonction utilisée en mathématiques appelée fonction de hachage (ou *hashing*). Cette fonction permet, quelle que soit l'information numérique (qu'il s'agisse d'un message, d'un document[836], d'une image, d'un son, d'une vidéo, etc.)[837] d'obtenir une empreinte de cette information – un « *hash* »[838]. Schématiquement, le *hash* est comme un condensé du message signé, sous la forme de chiffres et de lettres dont la longueur est fixe. Mais cette séquence de chiffres et de lettres est loin d'être née du hasard. *Bitcoin* utilise deux fonctions pour générer un *hash*. Il applique d'une part, la cryptographie sur les courbes elliptiques (*Elliptic Curve Cryptography*, ECC)[839] et, d'autre part, l'algorithme de hachage *SHA256*[840] (*Ethereum* utilise pour sa part *SHA2 et SHA3,* appelé aussi *Keecack*[841]) qui exécute l'ECC et produit le *hash*.

La courbe elliptique est une courbe algébrique qui a de nombreuses applications, et en particulier celles de factoriser des entiers et de créer des codes en cryptographie[842]. Contrairement à d'autres procédés de chiffrement, notamment les algorithmes RSA largement utilisés de nos jours[843], l'ECC est capable de fournir la même puissance de chiffrement avec des clés beaucoup plus courtes, de sorte que la sécurité est optimisée

[836] D'ailleurs, il est préférable d'opter pour un format de document tel que PDF (.pdf) plutôt que *Microsoft Word* (.docx), étant donné que le contenu de ce dernier est voué à être modifié constamment (du fait des enregistrements automatiques, par exemple).
[837] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 14.
[838] FOUQUE (Pierre-Alain), *op. cit.*, p. 15.
[839] D'après le dictionnaire en ligne Larousse, un « bit » est une : « - Unité binaire de quantité d'information. - Information représentée par un symbole à deux valeurs généralement notées 0 et 1, associées aux deux états d'un dispositif. - Unité de mesure de la longueur des mots utilisés par un ordinateur. » [Dictionnaire Larousse [en ligne], v° Bit, https://www.larousse.fr/dictionnaires/francais/bit/9639].
[840] ANTONOPOULOS (Andreas M.), *op. cit.*, p. 191.
[841] Pour plus de détails sur le sujet, v., notamment, MUKHI (Vijay), *The Undocumented Internals of the Bitcoin Ethereum and Blockchains*, ed. BPB Publications, 2018, pp. 771 et s.
[842] HERSANT (Olivier), *L'Internet des objets : Les protocoles (KNX, ZigBee, 6LowPan...) et les principales applications M2M*, éd. Dunod, coll. Automatiques et réseaux, 2014, p. 258.
[843] Sur le système RSA, v., TOUBOUL (Jonathan), « Nombres premiers et cryptologie : l'algorithme RSA », *Interstices* [en ligne], 21 déc. 2007, https://interstices.info/nombres-premiers-et-cryptologie-lalgorithme-rsa/.

alors même que l'algorithme requiert moins de calculs, et donc moins de temps, pour s'exécuter[844].

Associée au générateur *SHA256*, ils produisent ensemble une empreinte numérique sur 256 bits[845], c'est-à-dire d'une longueur de 256 caractères[846]. Mais en réalité, le *hash* utilisé ne fait pas cette taille car il est ensuite « compressé » en forme hexadécimale par une fonction de compression[847]. Grâce à une convention[848], cette fonction permet de réduire quatre bits en un seul. Le *hash* utilisé sur *Bitcoin* est donc présenté sous la forme d'une suite de soixante-quatre caractères de longueur[849], telle que, par exemple, la suite « e27266783eee2696a1a7b8401d9e9474c71aea91d173c2086a8b771afd19885f ».

105. Assurer l'intégrité du message signé : propriétés du *hash*. L'intérêt de la fonction de hachage réside dans l'équivalent du caractère immuable de la technologie *blockchain*, à savoir que le hachage inverse est impossible. En principe[850], aucun ordinateur existant ne peut déchiffrer le fichier inscrit sur la chaîne à partir de son empreinte cryptographique, ce qui par conséquent assure la confidentialité de son contenu[851]. C'est pourquoi l'anonymat, ou le pseudonymat, est souvent permis sur les *blockchains* car c'est le seul endroit où il peut être effectivement garanti. Autrement dit, l'empreinte est à sens unique[852]. Cette caractéristique induit trois conséquences idéalement comprises dans toute *blockchain* et permettant d'assurer l'intégrité des

---

844 « Qu'est-ce que l'ECC et pourquoi l'utiliser ? », *GlobalSign* [en ligne], 11 juin 2015, https://www.globalsign.com/fr/blog/infos-sur-ecc-et-pourquoi-l-utiliser.

845 BARTHELEMY (Pierre), ROLLAND (Robert), VERON (Pascal), *Cryptographie : principes et mises en œuvre. 2ème édition revue et augmentée*, éd. Lavoisier, 2e édition (revue et augmentée), 2012, p. 53.

846 Ces caractères étant essentiellement, et à ce stade, des « 0 » et des « 1 ».

847 Il s'agit de la fonction de compression de la construction de Merkle-Damgård [v., FOUQUE (Pierre-Alain), *op. cit.*, p. 14].

848 Par exemple, l'équivalence entre les systèmes binaire (en l'espèce, il s'agirait d'un *hash* de 256 *bits*) et hexadécimal (64 bits) correspondait à : 0000 = 0 ; 0001 = 1 ; 0010 = 2 ; 0011 = 3 ; 0100 = 4 ; 0101 = 5 ; 0110 = 6 ; 0111 = 7 ; 1000 = 8 ; 1001 = 9 ; 1010 = a ; 1011 = b ; 1100 = c ; 1101 = d ; 1110 = e ; 1111 = f ; etc. Ainsi, à partir d'un générateur binaire [http://md5decrypt.net/Outils-conversion/], la phrase « Bonjour ! » correspondrait, dans le système hexadécimal, à « 426f6e6a6f75722021 ». – Pour plus de précisions sur le sujet, v., CHANG (Weng-Long), VASILAKOS (Athanasios V.), *Molecular Computing: Towards a Novel Computing Architecture for Complex Problem Solving*, ed. Springer, Vol. 4, coll. Studies in Big Data, 2014, pp. 11-12.

849 MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., n° 12.

850 Une exception semble toutefois apparaître avec la création d'un ordinateur quantique. V., par exemple, à ce sujet, « L'informatique quantique, une menace pour Bitcoin ? », *Bictoin.fr* [en ligne], 9 déc. 2016, https://bitcoin.fr/linformatique-quantique-une-menace-pour-bitcoin/ ; « Des ordinateurs quantiques pourraient permettre de pirater le Bitcoin d'ici à 2027 », *Crypto-France* [en ligne], nov. 2017, https://www.crypto-france.com/piratage-bitcoin-ordinateurs-quantiques/.

851 BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 3.

852 GUILHAUDIS (Élise), « Comprendre la blockchain à travers l'étude d'un cas pratique : le covoiturage "Blockcar" », *RLDI* 2017/12, nº 143, p. 3.

informations inscrites[853] ; il est techniquement impossible de créer une « collision », c'est-à-dire un fichier possédant le même *hash*[854], de même qu'il est inconcevable de trouver deux fichiers différents ayant un *hash* identique ou de modifier le contenu dudit fichier sans en modifier son *hash*[855]. Sur *Bitcoin*, cette suite de chiffres et de lettres a pour fonction de débloquer la transaction de *bitcoins* de l'adresse « publique » émettrice (« *input* ») vers l'adresse « publique » destinataire (« *output* ») indiquée par l'utilisateur-destinataire[856]. Ainsi, en plus de garantir l'intégrité des inscriptions, la signature *via blockchain* semble établir avec une certaine certitude l'intégrité du consentement du signataire d'accepter la requête en signant.

106. Au-delà des *bitcoins* : les contenus admissibles pour les messages inscrits sur *blockchain*. Il s'avère important de préciser que la *blockchain* ne « stocke » pas forcément *que* des informations de transactions d'actifs cryptographiques entre deux cocontractants. En effet, dans le cas d'*Everledger* la *blockchain* sert de registre, appelé « *global ledger* », et stocke des informations relatives à des documents. Cependant, lorsque l'utilisateur dépose un document, il ne stocke pas le fichier en lui-même sur la chaîne, mais son empreinte[857]. La fonction de hachage va donc, en même temps qu'assurer son intégrité, servir à assurer la confidentialité du contenu du document objet de l'opération. C'est pourquoi, en règle générale, le message/fichier haché avec la clé privée émettrice pour obtenir la signature digitale de l'émetteur sont tous les deux le condensé en chiffres et en lettres du condensé en chiffres et en lettres du message/fichier initial. Autrement dit, dans cette configuration l'utilisateur chiffre non le fichier mais le *hash* de ce fichier avec sa propre clé privée, telle une signature finalement[858]. Dans le cas d'un contrat entre deux individus inscrit sur une *blockchain*, il s'agira toutefois de vérifier que le *hash* du fichier inscrit par l'un des contractants corresponde à l'exemplaire du fichier accepté et détenu par l'autre contractant avant que celui-ci ne signe.

---

[853] NAKAMOTO (Satoshi), « Bitcoin: A Peer-to-Peer Electronic Cash System », [online], Oct. 2008, https://bitcoin.org/bitcoin.pdf.

[854] C'est ce qui est arrivé en 2004 pour *MD5*. En effet, une équipe de recherches chinoise a trouvé un moyen de créer des « collisions » et n'est, depuis, plus utilisé.

[855] Par exemple, si l'on supprime le « ! » de l'exemple précédant (« Bonjour ! » = « bc7444869484dd1ed34bfc4465724b887fecf604fcad0d0eaf40d3746d0bfeb7 »), l'empreinte devient : « 9172e8eec99f144f72eca9a568759580edadb2cfd154857f07e657569493bc44 ».

[856] ANTONOPOULOS (Andreas M.), *op. cit.*, pp. 22-24, 114 et s. – V. également, Annexe n° 2. Schéma simplifié du mécanisme de transaction sur *blockchain*, p. 434 ; Annexe n° 7. Schéma de la signature numérique *via blockchain* : l'exemple de *Bitcoin*, p. 439.

[857] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 14.

[858] *Supra* n° 104.

107. L'étape de « validation » de l'opération sur la *blockchain* par les mineurs[859] procède ensuite à une dernière vérification de la correspondance clé privée/clé (adresse) publique et donc de l'authenticité de l'émetteur et de l'intégrité du contenu du message selon les règles prédéfinies avant leur inscription définitive. Les éventuelles usurpations ou falsifications d'identité ou corruptions de message sont en principe rendues inopérantes.

Le protocole propose donc de signer, d'authentifier, et de prouver, à l'instar des signatures électroniques actuelles. Ce procédé est-il toutefois suffisamment fiable pour répondre aux exigences probatoires de l'art. 1367 du C. civ. ?

§ 2. La fiabilité du procédé de signature *via blockchain*

108. Afin d'évaluer la fiabilité de son procédé, il s'agira de confronter les qualités, en apparence similaires, des dispositifs de signatures électroniques classiques avec celles des signatures *via blockchain* (B). Mais pour cela, il conviendra, dans un premier temps, de revenir sur la théorie et les pratiques actuelles, à savoir l'application des exigences légales par les signatures électroniques classiques (A).

A. Entre théorie et pratiques actuelles : des exigences légales à la création de la signature électronique classique

109. Définition et conditions de validité de la signature en droit des obligations. Le Code civil ne donne pas de définition de la signature appréhendée dans un sens large. L'al. 1er de l'art. 1367 indique simplement qu'elle est « nécessaire à la perfection d'un acte juridique » et qu'elle « identifie son auteur » tout en « [manifestant] son consentement aux obligations qui découlent de cet acte ». De ces indications davantage fonctionnelles émane toutefois un ensemble de règles.

Placée sur l'*instrumentum* de l'acte juridique, la signature donne à l'écrit la force probante que la loi attache aux actes sous signature privée. Cela signifie également qu'*a contrario*, son absence a pour conséquence de lui retirer toute force probante[860]. En parallèle, bien que la signature se réfère à « l'inscription du nom de la personne qui manifeste ainsi son adhésion aux mentions de l'acte »[861], il n'est pas exigé que cette inscription reproduise fidèlement ce que les registres d'état civil indiquent de cette

[859] *Infra* n° 143.
[860] Cass. Civ. 2e, 2 juill. 1996, *RTD civ*. 1996. 663.
[861] MOURALIS (Jean-Louis), « Preuve : Modes de preuve », *Rép. civ. Dalloz*, v° Preuve, 2011, n° 193.

personne, en ce sens que « l'inscription du prénom ou du surnom suffit si c'est la forme habituelle utilisée par la personne pour signer »[862]. Il est en réalité nécessaire de prendre en compte le contexte de signature et de veiller à ce que l'inscription choisie corresponde au type d'acte juridique effectué. Selon Jean-Louis Mouralis, la mention utilisée sera effectivement différente selon qu'il s'agisse d'un contrat passé avec un membre de la famille ou qu'il s'agisse d'un contrat d'affaires[863]. Enfin, bien qu'une relation synallagmatique oblige en principe les deux parties à signer chaque exemplaire de l'acte (C. civ., art. 1375), il apparaît que seule la signature de la personne qui s'oblige est nécessaire à celui qui s'en prévaut. En effet, ce dernier manifeste *ipso facto* sa propre adhésion au contrat en produisant l'écrit à titre de preuve[864]. Cette règle met par ailleurs en lumière l'importance de la mise à disposition de l'acte auprès de chacune des deux parties.

110. La reconnaissance de la signature dématérialisée. L'omniprésence progressive d'Internet au sein des foyers et des entreprises a conduit de nombreux processus traditionnels à se moderniser pour investir les pratiques de la digitalisation. En 1999, la directive communautaire 1999/93/CE consacre la validité de la signature électronique dans tous les États de l'actuelle Union Européenne[865]. À l'échelle de l'hexagone, le Code civil accueille ce nouveau procédé en mars 2000 avec l'adoption de la loi n° 2000-230 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique[866]. Dernièrement, c'est l'entrée en vigueur du règlement 910/2014 dit « eIDAS » (*electronic IDentification, Authentication and trust Services*) en septembre 2014[867] qui vient parachever le corpus législatif, d'une part, en précisant les règles tenant à l'identification électronique et aux services de confiance dans toute l'Union et, d'autre part, en « instaur[ant] un climat de confiance […] en ligne »[868]. Depuis l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations[869], le Code civil s'est muni de l'art. 1367 précité, aux

[862] Req., 20 octobre 1908, *DP* 1910. 1. 291.
[863] MOURALIS (Jean-Louis), *op. cit.*, *loc. cit.*
[864] Cass. Soc., 19 avr. 1963, *Gaz. Pal.* 1963. 2. 62. – Cass. Civ. 1ère, 18 nov. 1965, *Gaz. Pal.* 1966. 1. 83.
[865] Dir. n° 1999/93/CE du Parlement européen et du Conseil, 13 déc. 1999, sur un cadre communautaire pour les signatures électroniques, *JOUE* L 13, 19 janv. 2000, pp. 12-20.
[866] L. n° 2000-230, 13 mars 2000, portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, *JORF* n° 62, 14 mars 2000, p. 3968, texte n° 1. – Décr. n° 2017-1416 du 28 sept. 2017 relatif à la signature électronique, *JORF* n° 0229, 30 sept. 2017, texte n° 8.
[867] Règl. (UE) n° 910/2014 du Parlement européen et du Conseil, 23 juill. 2014, sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, *JOUE* L 257, 28 août 2014, pp. 73-114.
[868] Règl. (UE) n° 910/2014, préc., considérant n° 1.
[869] Ord. n° 2016-131, préc.

termes duquel « [la signature électronique] consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache », et qui fait d'ailleurs écho à l'art. 1366 qui le précède[870]. Cette définition laisse apparaître que, même s'il semble plus facile de subtiliser une signature « manuscrite », le législateur a malgré tout jugé essentiel de garantir *via* la signature électronique la fonction originelle d'identification de la signature traditionnellement « manuscrite »[871]. Il existe aujourd'hui trois niveaux de fiabilité reconnue à une signature électronique[872]. Bien que son caractère « non visuel » soit parfois déconcertant dans la pratique, il est impossible, en vertu du considérant n° 49 et de l'art. 25, §1, du règlement (UE) 910/2014, ainsi que de l'art. 1366 du C. civ., d'écarter une signature au seul motif qu'elle se présente sous la forme « électronique » et non « manuscrite ».

Réservée aux personnes physiques, la signature électronique se veut sécurisante, que ce soit auprès des citoyens, des entreprises ou des autorités publiques[873]. Concernant les personnes morales, un procédé identique est admissible sous la forme d'un cachet électronique pouvant se coupler à la signature électronique du dirigeant, à condition qu'il permette de « garantir l'origine et l'intégrité [du] document » émis par la personne morale[874]. Étant donné la similitude des exigences applicables à ces deux procédés, il semble acceptable de poursuivre cette étude sous l'angle de la signature électronique.

111. Élaboration et caractéristiques des signatures électroniques actuellement admises. D'une manière générale, la signature électronique intervient lorsque deux personnes, physiques et/ou morales, désirent échanger en toute sécurité un message sous forme électronique et que ce message doit être authentifié, autant vis-à-vis de son contenu que vis-à-vis de son expéditeur. Ce message peut consister en une facture, un contrat commercial/fournisseur, un processus RH, un bulletin de paie, une télédéclaration fiscale, etc. La plupart des signatures électroniques mettent en œuvre des procédés de signature cryptographique de type asymétrique[875]. Leur admissibilité et leur valeur probante est fonction de la reconnaissance de la « fiabilité » du procédé utilisé (C. civ., art. 1367, al.

[870] C. civ., art. 1366 : « L'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. »
[871] Concernant les divergences doctrinales actuelles sur la pertinence du vocable « manuscrite », v., SUXE (Florent), *La preuve du contrat électronique*, Paris : Université Jean Monnet Paris XI, 2012, pp. 14-15.
[872] *Infra* n° 119.
[873] Règl. (UE) n° 910/2014, préc., considérant n° 2.
[874] *Ibid.*, considérants n°s 58-60.
[875] MOUGENOT (Dominique), *Droit des obligations, la preuve*, éd. Larcier, 2e édition, 2002, p 172. V. désormais, MOUGENOT (Dominique), *Droit des obligations, la preuve*, éd. Larcier, 4e édition, 2017.

2). En règle générale, l'utilisation d'un algorithme RSA[876] avec fonction de hachage *SHA256* est préférée en matière de commerce électronique et d'échange de données sur Internet car il est conforme aux recommandations des organismes nationaux et internationaux[877]. Le processus d'élaboration de la signature cryptographique actuellement admise requiert donc de l'expéditeur, dont la signature est exigée, qu'il signe le message électronique, le crypte avec la clé publique du destinataire, puis le renvoie au destinataire. De cette façon, seul le destinataire peut décoder le message électronique et le lire puisqu'il est le seul à détenir la clé privée associée à la clé publique de cryptage[878].

En pratique, ces couples de clés, appelés « bi-clés », sont générés par une Infrastructure de gestion de clé (IGC) – généralement indiquée sous sa forme anglaise « PKI » pour « *Public Key Infrastructure* ». Chaque cocontractant a ainsi la possibilité d'obtenir ce bi-clés par lui-même, ou par l'intermédiaire d'une autorité d'enregistrement tierce et spécialisée[879]. Dans les deux cas, il demeure ensuite sous le contrôle et la responsabilité de l'utilisateur-signataire qui, en toute autonomie, les stocke, par exemple, sur une clé USB, sur une puce, sur n'importe quel support matériel informatique et/ou magnétique, ou sous une forme dématérialisée tel que sur un *cloud*[880]. Bien que la confidentialité du message électronique semble ainsi être protégée, il est essentiel d'assurer tant son intégrité que l'identification de son expéditeur.

Pour signer, l'expéditeur utilise un dispositif de création de signature électronique[881]. Celui-ci consiste en un matériel informatique, prenant la forme d'un logiciel ou d'une application, spécialement configuré pour permettre la signature et l'échange de documents. Il peut être à utilisation libre et indépendante, tel que le logiciel PDF[882], ou être relié à une plateforme remplissant le rôle d'intermédiaire prestataire de

---

[876] Héritant des initiales des noms de ses trois inventeurs, Ronald Rivest, Adi Shamir et Leonard Adleman, l'algorithme RSA est un algorithme de cryptographie asymétrique.

[877] Il s'agit notamment des normes ETSI relatives à la signature électronique [v., https://portail-qualite.public.lu/fr/actualites/confiance-numerique/2016/actualite-etsi.html] et des normes ISO 35.030 « Sécurité des technologies de l'information » [v., https://www.iso.org/fr/ics/35.030/x/], telle la norme ISO/IEC 9798-4:1999 « Partie 4: Mécanismes utilisant une fonction cryptographique de vérification » [https://www.iso.org/fr/standard/31488.html].

[878] *Supra* n° 99.

[879] L. n° 2004-575, préc., art. 29, al. 1er : « On entend par prestation de cryptologie toute opération visant à la mise en œuvre, pour le compte d'autrui, de moyens de cryptologie. » – V. également, « Certificate Policy and Public Certificate Practice Statement », DocuSign [en ligne], pp., 18, 50 et s., https://www.docusign.fr/sites/default/files/Politiques%20de%20Certifications/EV_SSL_CA_Certification_Practice%20Statement_v_1_2.pdf.

[880] Pour plus de précisions, v., TOUTCHKOV (Hélène), « Tout savoir sur la signature électronique », *Certeurope* [en ligne], 2018, https://www.certeurope.fr/blog/tout-savoir-sur-la-signature-electronique/.

[881] Règl. (UE) n° 910/2014, préc., art. 3, §22.

[882] V. le site officiel d'Adore Reader, https://helpx.adobe.com/fr/reader/using/sign-pdfs.html. – Pour plus de précisions, v. également, https://helpx.adobe.com/fr/acrobat/11/using/digitahttps://helpx.adobe.com/fr/acrobat/11/using/digital-ids.htmll-ids.html.

confiance[883] telle que *DocuSign* ou encore *ChamberSign*[884]. Afin de garantir l'intégrité du message, il est nécessaire qu'aucun caractère – qu'il s'agisse d'une phrase entière, d'un mot ou d'un simple espace – n'ait été supprimé ou ajouté sans que le destinataire n'en ait été informé et y ait préalablement consenti. En matière de contrat d'affaires notamment, l'expérience révèle que la position d'une virgule est en effet capable de bouleverser la teneur des obligations de chaque partie[885]. Seulement, le destinataire ne peut vérifier caractère par caractère un fichier pouvant contenir plus d'une centaine de pages. La solution a été de créer un dispositif mettant en œuvre deux étapes dans le processus. L'émetteur, en plus de crypter le message avec la clé publique du destinataire, utilise la fonction de hachage[886] pour obtenir le *hash* du message électronique initial, qui a pour fonction de prouver son intégrité. Il le crypte ensuite avec sa propre clé privée. De cette façon, la moindre différence de contenu dans le message modifiera automatiquement son *hash*. De surcroît, en signant de sa clé privée le message initial, l'expéditeur s'authentifie en tant que tel, étant seul propriétaire de la clé privée et de la clé publique associée. En parallèle, en cryptant le message électronique avec sa clé privée secrète, l'expéditeur, d'une part, constitue sous forme dématérialisée l'élément matériel nécessaire à la validité de l'acte et, d'autre part, extériorise sa volonté de signer, élément intentionnel correspondant au consentement.

La similarité entre le dispositif de signature des *blockchains* et celui des signatures électroniques classiques est importante et suggère dès lors que le premier a autant de chances que le second d'être reconnu fiable.

B. Face à face entre signatures électroniques classiques et signatures via blockchain : des similarités de procédés à la question de la fiabilité

112. L'équivalence des mécanismes permettant l'authentification et garantissant l'intégrité. Les procédés de signature digitale *via blockchain* et de signature électronique classique sont en de multiples points ressemblants.

[883] Règl. (UE) n° 910/2014, préc., art. 3, §16, a).
[884] V. les sites officiels, respectivement, https://www.docusign.fr/ ; https://www.chambersign.fr/.
[885] V., par exemple, l'affaire de l' « Oxford comma », VICTOR (Daniel), « Lack of Oxford Comma Could Cost Maine Company Millions in Overtime Dispute », *The New York Times* [online], 16 Mar. 2017, https://www.nytimes.com/2017/03/16/us/oxford-comma-lawsuit.html?action=click&pgtype=Homepage&clickSource=story-heading&module=c-column-middle-span-region&region=c-column-middle-span-region&WT.nav=c-column-middle-span-region&_r=0.
[886] Ce qui explique l'utilisation du générateur *SHA256*.

En effet, dans le cadre de *Bitcoin*[887], lorsque l'utilisateur veut réaliser un paiement, le système hache à deux reprises sa clé privée et lui fournit une « adresse de réception » – en d'autres termes, « l'adresse publique » mentionnée dans le *script* de l'inscription sur une *blockchain*. Or, la signature numérique, elle aussi inscrite sur la *blockchain* et hachée avec la clé privée, semble capable de confirmer ou d'infirmer la propriété de « l'adresse publique » puisque, l'une comme l'autre, appartient à l'utilisateur qui possède la clé privée associée.

Par ailleurs, l'utilisation commune de techniques de hachage suggère que les deux types de dispositifs présentent des garanties analogues en termes d'intégrité et de confidentialité des contenus.

Concernant ensuite la sécurisation des dispositifs et processus de signature, le « risque zéro » n'existe pas, mais diverses mesures de protection sont mises en œuvre. Les dispositifs de signatures électroniques traditionnellement admis déploient des mécanismes de protection tant au niveau du réseau qu'en interne contre toute attaque malveillante, telles que des « virus informatiques et autres formes de logiciels compromettants et non-autorisés »[888]. La signature générée par une *blockchain* bénéficie pour sa part de la neutralité et de la distributivité du réseau qui la protègent, en principe, naturellement contre toute attaque et/ou détournement malveillant[889]. Somme toute, l'un comme l'autre des procédés font l'objet de mises à jour constantes de logiciel, de plateforme, ou de protocole. Ces multiples mesures sont autant de gages d'une sécurisation en temps réel efficace et pérenne aptes à susciter la confiance.

113. Les bénéfices de la signature *via blockchain*. En tout état de cause, l'observation de la pratique de la signature électronique communément admise ne permet pas de lui reprocher une quelconque défaillance que la *blockchain* pourrait potentiellement solutionner, et qui, à terme, l'aurait peut-être menée à la remplacer. Simplement, à différents points de vue, les techniques de hachage semblent présenter certains avantages, la signature *via blockchain* apparaissant comme une solution aussi efficace sinon plus que les dispositifs traditionnels.

D'abord, force est de constater que le *hash* inscrit sur une *blockchain* est peu volumineux, alors qu'en pratique la signature électronique ordinaire d'un document

[887] D'ailleurs, avant de travailler sur les *smart contracts*, Nick Szabo a lui-même longtemps étudié les systèmes de signatures électroniques, notamment à travers l'algorithme ECDSA (*Elliptic Curve Digital Signature Algorithm*). V. en ce sens, RODRIGUEZ (Philippe), *La révolution blockchain : Algorithmes ou institutions, à qui donnerez-vous votre confiance ?*, éd. Dunod, 2017, p. 44.
[888] « Certificate Policy and Public Certificate Practice Statement », préc., p. 55.
[889] Sur le principe de distributivité de la *blockchain*, *infra* n°S 142 et s.

équivaut en termes de taille au document originel. Donc si celui-ci fait 7 Go, la signature fera elle aussi 7 Go, contrairement à une signature *blockchain* de 256 bits[890] qui, de plus, demeure accessible en clair sur la chaîne pour tout individu. Il s'agit donc d'un avantage comparatif évident, notamment lorsqu'il s'agit de transmettre la signature par e-mail ou sur Internet dans le cadre d'un site d'*e-commerce*, et d'autant plus lorsque la signature électronique est conservée par l'utilisateur lui-même. Par conséquent, l'aspect stockage est plus contraignant en ce qui concerne la signature électronique classique, ce qui conduit d'ailleurs souvent le secteur à limiter ses offres en fonction du poids des documents à signer[891].

Le même constat peut être réalisé concernant le système de bi-clés en lui-même puisque la pratique révèle que les procédés de création de signatures électroniques ne font qu'augmenter la taille des clés RSA utilisées, et ce afin de maintenir une force de chiffrement, et donc une sécurité, toutes deux suffisantes. Mais aujourd'hui ces clés ont dépassé les 2048 bits. En parallèle, l'homologue ECC propre aux *blockchains* est capable d'offrir un niveau de sécurité équivalent pour des bi-clés plus courtes, donc moins volumineuses, et un temps d'exécution réduit[892]. Pour un bi-clés RSA de 3072 bits, par exemple, un bi-clés ECC de 256 bits, soit douze fois plus court que le premier, est suffisant en termes de sécurité, et plus rapide en termes de calculs. L'ECC de la *blockchain* présente en cela une alternative dont les qualités de simplification de l'utilisation du procédé de signature peuvent être appréciables à plusieurs points de vue.

Exprimée en termes de budget, une inscription sur *blockchain* est par ailleurs d'ordinaire moins coûteuse que la souscription d'un abonnement généralement annuel à un dispositif de signature électronique traditionnel. Il s'agit sur ce point pour chaque utilisateur, et plus particulièrement pour les entreprises, de procéder à une analyse coûts-avantages – ou coûts-bénéfices – afin de déterminer en fonction de leurs besoins si un tel investissement serait rentable sur long-terme. Qui plus est, cette évaluation des coûts pourrait également prendre en compte la gestion des aspects logistiques tels que l'archivage évoqué ci-dessus, qui exigera plus ou moins d'investissement en matière de supports numériques de stockage, de puissance réseau, mais aussi d'alimentation énergétique et de climatisation, etc., selon le processus adopté.

[890] À titre informatif, 1 Go = 8 589 934 592 bits.
[891] BAUFUMÉ (Vivien), CARMINATI (Christophe), « La blockchain, un outil technologique… et juridique », *JCP N* 2020, entretien n° 30, p. 1162.
[892] En algorithmique, le temps d'exécution d'un algorithme, appelé « complexité en temps », est fonction du nombre d'étapes de calculs qu'il doit achever avant d'aboutir à un résultat, lui-même fonction de la taille de la donnée d'entrée.

Enfin, il ressort de l'analyse jusqu'ici exposée de la signature électronique classique, qu'elle vise continuellement à davantage de sécurité puisque sa « fiabilité » trouve son fondement dans la sécurisation des échanges qu'elle permet. Or, la technologie des chaînes de blocs est intrinsèquement protégée grâce à ses qualités de distributivité et de neutralité. Bien que les risques de détournement et *a fortiori* de falsification ne sont pas impossibles et feront d'ailleurs l'objet de développements ultérieurs, une *blockchain* est en effet de nature plus sécurisée qu'une plateforme reliée à un serveur centralisé. En cela, elle mène le procédé à un échelon supérieur sur l'échelle de la sécurisation des échanges informatiques au sens où plus il y a de sécurité, plus le procédé est fiable, et plus la confiance se développe. C'est pour cet ensemble de raisons que certains auteurs considèrent non pas que la *blockchain* est vouée à terme à remplacer les procédés actuels de signature, mais qu'elle pourrait constituer une variété de signature électronique existante, et peut-être même une nouvelle forme de tiers de confiance[893]. Il reste à savoir si ces similitudes et atouts seront suffisants pour pleinement considérer la signature digitale de la *blockchain* comme étant un procédé de signature électronique effectivement « fiable » lui aussi.

114. La limite de la *blockchain* : l'aléa de l'identification. Toutefois, un dernier détail et non le moindre semble faire immédiatement défaut. En effet, une personne voulant non pas confirmer ou infirmer la propriété d'une adresse mais identifier l'émetteur d'un document ou message quelconque, ne parviendrait pas à trouver une *identité* proprement dite mais obtiendrait un *pseudonyme*, ou même l'adresse d'un compte s'il s'agit de la *blockchain Bitcoin*. En effet, l'une des particularités de la *blockchain* souvent mentionnée, tantôt comme un avantage tantôt comme un inconvénient, est l'anonymisation[894] sous le couvert d'une « pseudonymisation » des comptes utilisateurs[895]. Alors que les institutions bancaires, par exemple, authentifient les détenteurs de compte par leur identité civile[896], certains types de protocoles tels *Bitcoin* n'enregistrent que les transactions de type « $A \rightarrow B$ », « A » étant l'adresse « publique »

[893] LEGEAIS (Dominique), *op. cit.*, n° 29.
[894] BAYLE (Aurélie) *et al.*, « Smart contracts : études de cas et réflexions juridiques », *ECAN* [en ligne], 19 sept. 2017, p. 16, https://ecan.fr/Smart-Contracts-Etudes.pdf.
[895] HELLEU (Guillaume), MASURE (Anthony), « Total Record. Les protocoles blockchain face au post-capitalisme », *Multitudes* 2018/2, n° 71, p. 76.
[896] Requérant des informations d'état civil, telles que les nom, prénom, adresse, date de naissance, etc.

de l'émetteur, « *B* » l'adresse « publique » du destinataire[897], et la plupart des autres fonctionnent avec des pseudonymes[898].

Pourtant, il s'avère parfois que l'anonymat pratiqué ne soit pas aussi protégé que souhaité. C'est effectivement le constat qui a été réalisé par les plus de 300 utilisateurs arrêtés et jugés pour avoir fait l'acquisition de stupéfiants contre paiement en *bitcoins* par le biais du site *Silkroad*[899]. Ces informations de « transactions » figurent en clair sur la *blockchain*, ce qui induit qu'il est en théorie possible de mettre un nom sur une ombre en analysant les transactions, soit émises, soit reçues, ou les deux, ou même en utilisant la topologie du réseau pour croiser une adresse avec une localisation et/ou une adresse IP[900]. Il est également possible en théorie de parvenir à identifier un utilisateur *via* les données collectées par des objets connectés et/ou intelligents, ou par des *cookies*, à condition pour ce dernier cas que l'utilisateur en question ait utilisé ses identifiants sur un site Internet ayant recueilli ses données[901]. Il est aussi probable que l'identité d'un utilisateur soit découverte dans le cas où son *wallet* serait hébergé *via* un site opérant à partir d'un établissement centralisé, une banque par exemple[902]. Comme le souligne Jean-Yves Pronier, « c'est bien d'avoir des données, mais c'est mieux de les faire parler »[903]. Pourtant, le succès de ces procédés n'est pas établi avec certitude et ils restent en cela des démarches expérimentales. Par conséquent, leur utilisation ne peut suffire à arguer de la fiabilité, tant technique que juridique, de l'identification devant un juge.

Plus encore, il est nécessaire de remarquer que dans le contexte des *blockchains* financières, les propriétaires de crypto-monnaies sont relativement prudents en termes de confidentialité et de sécurité. Certains avocats réussissent parfois – et s'ils tentent – à

---

[897] HELLEU (Guillaume), MASURE (Anthony), art. cit., p. 7.

[898] BEAUDEMOULIN (Nathalie) *et al*., « Les enjeux de la Blockchain pour la Banque de France et l'Autorité de Contrôle prudentiel et de Résolution (ACPR) », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 31.

[899] COX (Joseph), « This Researcher Is Tallying All the Arrests From Dark Web Markets », *Mother Board* [online], 7 May 2015, https://motherboard.vice.com/en_us/article/z4m77a/this-researcher-is-tallying-arrests-from-dark-web-markets.

[900] En fait, il apparaît que les adresses IP des nœuds sont stockées sur la chaîne de blocs *via* des DNS. Un auteur s'appuie, pour l'expliquer, sur le mécanisme de prise de contact initial entre les pairs du réseau [v., ANTONOPOULOS (Andreas M.), *op. cit.*, p. 152, (trad., préc.)] : « comment un nouveau nœud trouve des pairs ? La [...] méthode consiste à interroger un DNS en utilisant un certain nombre de graines DNS (*DNS seeds*), des serveurs DNS qui fournissent une liste 8 d'adresses IP de nœuds *bitcoin*. Certaines de ces graines DNS fournissent une liste statique des adresses IP des nœuds *bitcoin* stable en écoute. D'autres sont des implémentations personnalisées de BIND (*Berkeley Internet Name Daemon*) qui renvoient un sous-ensemble aléatoire d'adresses à partir d'une liste d'adresses de nœuds *bitcoin* recueillies par un robot ou d'un nœud *bitcoin* en activité depuis longtemps. Le client *Bitcoin Core* contient les noms de cinq graines DNS différentes ». – Pour plus de précisions, v. également, Bitcoin Project, « Protéger votre confidentialité », *Bitcoin.org* [en ligne], https://bitcoin.org/fr/proteger-votre-vie-privee.

[901] DEVILLIER (Nathalie), « Jouer dans le "bac à sable réglementaire" pour réguler l'innovation disruptive : le cas de la technologie de la chaîne de bloc », *RTD com.* 2017, p. 1037.

[902] *Id.*

[903] PRONIER (Jean-Yves), cité dans : SIMEON (Gabriel), « Données le vertige », *Libération* [en ligne], 3 déc. 2012, http://www.liberation.fr/futurs/2012/12/03/donnees-le-vertige_864585.

obtenir du juge une ordonnance d'identification d'une adresse IP auprès des opérateurs[904]. Cependant, beaucoup d'utilisateurs de *Bitcoin*, par exemple, s'astreignent à un changement systématique d'adresse « publique » à chaque opération inscrite[905], sinon utilisent un mécanisme de dissimulation de l'adresse IP utilisée tel que *Tor*[906]. Ce dernier consiste en un protocole de réseau Internet traversant les serveurs informatiques de milliers de volontaires répartis sur toute la surface du globe, et permettant de rendre anonymes les données transmises au cours de la navigation. Pour cela, il regroupe l'ensemble des données des utilisateurs puis supprime une partie de celles-ci afin de les rendre inidentifiable, pour enfin les crypter et les acheminer vers d'autres serveurs, appelés « relais »[907]. De cette manière les informations sont rendues quasi-intraçables[908].

115. Finalement, bien que la signature *via blockchain* semble présenter de multiples qualités, en particulier, selon Laure De La Raudière et Jean-Michel Mis, en matière de « traçabilité […] et [d]'immuabilité des transactions », qui lui permettraient en partie de répondre aux spécifications du règlement eIDAS et d'être ainsi reconnue comme étant un procédé fiable de signature[909], cet anonymat partiel couramment pratiqué au sein des *blockchains* ne permet pas l'identification immédiate et efficace des acteurs. Or, l'al. 2 de l'art. 1367 du C. civ. érige comme condition essentielle la fonction d'identification de la signature[910], ce qui mène à s'interroger sur le caractère insurmontable de cet obstacle technique au regard des recherches en cours.

Section 2. Des systèmes d'authentification divergents : le poids de la pseudonymisation

116. Au-delà des similitudes de fonctionnement, les systèmes d'authentification respectivement utilisés, d'une part, par les mécanismes classiques de signature et, d'autre

[904] COIFFARD (Didier), « Entretien du mois : La Blockchain a un sens pour répartir une partie de la confiance en rendant une information infalsifiable mais cette confiance est très en deçà de celle conférée par le notaire », *RLDC* 2017/4, n° 147.
[905] Bitcoin Project, « Bitcoin pour les entreprises », *Bitcoin.org* [en ligne], https://bitcoin.org/fr/bitcoin-pour-entreprises.
[906] V. le site officiel du protocole, https://www.torproject.org/.
[907] *Id.*
[908] Sur les difficultés d'identification de réseaux s'appuyant sur des systèmes de type Tor, v., par exemple, l'étude sur le dossier Black Hand, LAURENT (Xavier), « Retour d'expérience sur le premier démantèlement d'une plateforme francophone du darkweb : le dossier Black Hand », *D. IP/IT* 2021, n° 2, p. 79.
[909] Rapp. AN n° 1501, 12 déc. 2018, de Laure DE LA RAUDIÈRE et Jean-Michel MIS sur les chaînes de blocs (*blockchains*).
[910] C. civ., art. 1367, al. 2 : « la signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte ».

part, par la plupart des *blockchains*, divergent en raison du pseudonymat pratiqué au sein du protocole de ces dernières. Par ailleurs et contre toute attente, la loi nº 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises, dite « loi PACTE »[911], n'a pas pris en compte l'amendement n° 1317 qui proposait de compléter l'art. 40 du projet par la reconnaissance, au sein de l'art. 1358 du C. civ., de la présomption de fiabilité de l'empreinte de « tout fichier numérique enregistré dans un dispositif électronique d'enregistrement partagé (DEEP) »[912], tel qu'une *blockchain*[913].

Cependant, comme l'a souligné l'Assemblée Nationale interrogée au sujet de la valeur probante des informations inscrites par le biais de la technologie *blockchain*, « si aucun texte juridique ne mentionne spécifiquement la *blockchain*, il n'en résulte pour autant aucun vide juridique »[914]. En effet, les règles communes en matière de preuve restent applicables en cas de conflit devant les tribunaux. Les commerçants peuvent prouver par tous moyens les actes de commerce (C. com., art. 110-3) et, d'une manière générale, les parties restent libres de déterminer par tous moyens la preuve des faits juridiques (C. civ., art. 1358) ainsi que des actes sous signatures privées portant sur une somme ou une valeur n'excédant pas le montant de 1 500 euros (C. civ., art. 1359, al. 1er ; Décret n° 2016-1278 du 29 septembre 2016[915], art. 1). Toutefois, au-delà de ce montant, pour que la signature d'un acte obtenue grâce à une *blockchain* puisse bénéficier de la même valeur que la signature électronique classique, la condition essentielle, homologue à celle de l'intégrité, impose de pouvoir livrer de manière fiable l'identité du contractant signataire de l'écrit. Bien que cette faculté s'avère relativement limitée en matière de registre décentralisé (*ledger*), il s'agit d'analyser la résistance *au* principe – plus que la résistance *du* principe[916] – du pseudonymat. L'objectif étant d'en déduire s'il est véritablement impossible de considérer que la signature numérique de la chaîne de blocs

[911] L. nº 2019-486, 22 mai 2019, relative à la croissance et la transformation des entreprises, *JORF* n° 0119, 23 mai 2019, texte n° 2.

[912] Amendement n° 1317, 3 sept. 2018, au Projet de loi relatif à la croissance et la transformation des entreprises (PACTE), présenté par M. Mis, Mme Hérin, M. Rudigoz, Mme Le Peih, M. Buchou, M. Son-Forget, Mme Gipson, Mme Couillard, M. Martin, M. Cesarini, Mme Cazarian, M. Trompille, M. Tan, M. Bois, M. Borowczyk, Mme Frédérique Dumas et Mme Fontenel-Personne, Assemblée Nationale : « ARTICLE ADDITIONNEL - APRÈS L'ARTICLE 40, insérer l'article suivant : Après l'unique alinéa de l'article 1358 du code civil, insérer un alinéa ainsi rédigé : "À cet effet, tout fichier numérique enregistré dans un dispositif électronique d'enregistrement partagé (DEEP), de nature publique ou privée vaut preuve de son existence et de sa date, jusqu'à preuve contraire, dès lors que ledit DEEP répond à des conditions définies par décret" ».

[913] DEEP est l'équivalent de « *Distributed Ledger Technology* » (DLT). Dans sa fonction de *ledger*, la technologie *blockchain* est qualifiée de DLT.

[914] Question AN n° 22103, 30 juill. 2019, *JO*, 10 déc. 2019, p. 10774, Fasquelle D.

[915] Décr. n° 2016-1278, 29 sept. 2016, portant coordination des textes réglementaires avec l'ordonnance n° 2016-131 portant réforme du droit des contrats, du régime général et de la preuve des obligations, *JORF* n° 0228, 30 sept. 2016, texte n° 34.

[916] À l'instar des moyens évoqués *supra* n° 114 permettant d'identifier, avec plus ou moins de chance de réussite, les détenteurs d'adresses *bitcoin*.

est capable de répondre aux exigences des textes en vigueur concernant la signature électronique.

C'est pourquoi il importera, dans un premier temps, d'apprécier l'effectivité des moyens mis à disposition des parties pour emporter la conviction du juge de la fiabilité du procédé de signature utilisé, et notamment en ce qui concerne son propre mécanisme d'identification (§ 1). Face à des moyens, somme toute, relativement limités, il conviendra de rechercher, dans un second temps, des solutions permettant de conformer la *blockchain* aux exigences probatoires, sans toutefois contrevenir à ses principes (§ 2).

§ 1. L'effectivité des moyens de preuve de la fiabilité du procédé

117. Quand bien même sa crédibilité ne s'impose pas au juge, la fonction de *ledger* de la *blockchain* a été reconnue à plusieurs occasions pour son intégrité en tant que dispositif d'enregistrement électronique partagé (DEEP). En effet, l'art. 2 de l'ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse[917] a introduit un nouvel art. L. 223-12 du C. mon. et fin. qui reconnaît la fiabilité du mécanisme en matière d'émission et de cession de minibons. Cette ordonnance précède la reconnaissance formelle d'un effet de droit à l'utilisation d'un DEEP pour la représentation et la transmission de titres financiers. Celle-ci a été obtenue par l'adoption de l'ordonnance nº 2017-1674 du 8 décembre 2017[918] et de son décret d'application[919], qui ont donc conduit également à modifier le Code monétaire et financier (C. mon. et fin., art. L. 211-3 et L. 211-7). Enfin, les art. 85 et 88 de la « loi PACTE » ont mis en place un cadre juridique rénové et adapté aux offres au public et émissions de jetons. En parallèle de ces reconnaissances législatives ponctuelles, il résulte de la rédaction des textes fixant les conditions d'admissibilité des dispositifs de signatures électroniques deux éléments essentiels. D'une part, leurs dispositions ont vocation à s'appliquer de manière extensive et, d'autre part, leur interprétation et application doivent être conformes à un ensemble de principes fondés sur la non-discrimination de l'écrit électronique par rapport à l'écrit sur support papier. Cette liberté dans l'administration de la preuve laisse, en principe, envisager la possibilité pour les parties de produire les éléments dont elles disposent, et notamment de démontrer la fiabilité du procédé de signature électronique utilisé, que les juges du fond apprécieront

[917] Ord. n° 2016-520, 28 avr. 2016, relative aux bons de caisse, *JORF* n° 0101, 29 avr. 2016, texte n° 16.
[918] Ord. nº 2017-1674, 8 déc. 2017, relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers, *JORF* n° 0287, 9 déc. 2017, texte n° 24.
[919] Décr. nº 2018-1226, 24 déc. 2018, relatif à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers et pour l'émission et la cession de minibons, *JORF* n° 0298, 26 déc. 2018, texte n° 33.

souverainement afin d'accorder ou non force probante à l'écrit inscrit sur un dispositif *blockchain* (A). Toutefois, il s'avère qu'en la matière cette liberté dans l'administration de la preuve doit être maniée avec prudence. En effet, maladroitement exploitée, elle peut entraîner un défaut de confidentialité susceptible de représenter un danger pour les utilisateurs d'une *blockchain*. Il s'agira donc de cibler les éléments de preuve de la fiabilité de l'identification des contractants dont il résulterait que la production caractériserait un risque (B).

A. Le principe de la liberté de la preuve

118. La possibilité de conclure un accord sur la preuve : une signature *blockchain* aménagée. Avant d'analyser la possibilité de démontrer la fiabilité du procédé de signature utilisé, il convient d'évoquer la liberté laissée aux parties qui, face aux « règles "normales" de la preuve judiciaire »[920] et au pouvoir d'appréciation du juge qui détermine souverainement la vraisemblance des titres portés à l'audience[921], ont été tentées de s'accorder pour anticiper ce qu'elles pourraient percevoir comme un aléa. En droit commun, la liberté contractuelle est de principe. Par conséquent, les parties peuvent aménager, d'un commun accord, un régime probatoire spécial – et *a priori* simplifié – qui s'exécutera immédiatement en cas de procédure judiciaire. Cet aménagement peut ainsi porter directement sur la charge de la preuve de la fiabilité, sur l'admissibilité des « moyens et modalités des procédés de preuve », ou sur la détermination des faits à prouver[922], dans la limite des prescriptions d'ordre public[923]. Partant de là, les parties qui désirent modifier expressément les règles de preuve leur étant en principe applicables pourraient donc choisir entre deux options. D'une part, elles peuvent admettre *a priori* la fiabilité de la *blockchain* comme procédé utilisé pour signer le document qui les lie l'une à l'autre, et ainsi renverser la charge de la preuve sur celle des deux qui en nierait l'attribution et/ou en contesterait la fiabilité[924]. D'autre part, elles ont la possibilité de dresser une liste des éléments de preuve nécessaires à la démonstration de la fiabilité du procédé employé, tels que, par exemple, le numéro de bloc ou encore le numéro de transaction afin de certifier l'exactitude de son origine, et le document original et son *hash* sur la *blockchain* utilisée afin de certifier l'intégrité du contenu.

---

[920] Cass. Com., 8 nov. 1989, *Bull. civ.* IV, n° 342, « Crédicas ».
[921] C. civ., art. 1368.
[922] Cass. Com., 8 nov. 1989, *Bull. civ.* IV, n° 342, « Crédicas ».
[923] C. civ., art. 1356, al. 2 (présomptions légales irréfragables) ; C. consom., art. R. 212-1, 12° (charge de la preuve imposée au consommateur ou au non-professionnel).
[924] En rappelant que l'établissement d'une présomption irréfragable au profit de l'une des parties invalide l'accord contractuel sur la preuve établi, v., Cass. Com., 6 déc. 2017, n° 16-19.615.

Cependant, force est de constater que cette faculté apparaît, malgré tout, assez restreinte, puisqu'effectivement la preuve contraire peut être rapportée par tous moyens (CPC, art. 288-1) et, surtout, il est nécessaire dans ce cas que les parties aient pensé à anticiper la question de la preuve dès la formation du contrat.

119. La possibilité de démontrer la fiabilité du procédé utilisé : l'application du principe d'équivalence fonctionnelle. Le règlement « eIDAS »[925] fixe trois catégories graduelles de signature électronique, à savoir les signatures électroniques simples, avancée et qualifiée[926]. La force probante de l'écrit électronique dépend de la fiabilité du procédé de signature utilisé. Un certain nombre de règles de forme posées par le règlement, notamment par l'annexe 2, et par le décret n° 2017-1416 du 28 septembre 2017[927] en ce qui concerne la signature qualifiée, permettent d'évaluer la fiabilité d'un dispositif. À la lecture des textes, l'appellation « qualifiée » est à l'évidence le but ultime qu'une signature doit atteindre afin de bénéficier de la présomption de fiabilité qui lui est *ipso facto* attachée[928]. L'exigence d'un haut niveau de sécurité technique s'explique par la volonté du législateur de circonscrire les cas pour lesquels une signature bénéficie du statut de preuve parfaite[929] et donc de la présomption d'imputabilité[930] car en effet, dès lors que la signature est reconnue comme étant « qualifiée », nul besoin de prouver tant la crédibilité de son procédé que son origine puisque celles-ci sont intrinsèques. Plus encore, c'est donc à celui qui en nierait l'attribution et/ou en contesterait la fiabilité de prouver ses dires.

Mais en réalité, et tel que le relèvent Eric A. Caprioli et Pascal Agosti, « ces dispositions […] n'ont d'implication que sur la charge de la preuve »[931]. En aucun cas la signature qui ne répondrait pas aux exigences de la signature qualifiée entraverait sa propre valeur juridique ou la force probante de l'écrit sur lequel elle est apposée. En effet, sa fiabilité ne serait simplement pas présumée[932]. Cette règle découle du principe de non-

[925] Règl. (UE) n° 910/2014, préc.
[926] *Ibid.*, respectivement : art. 3, §10 ; art. 26 ; art. 28-33.
[927] Décr. n° 2017-1416, 28 sept. 2017, relatif à la signature électronique, *JORF* n° 0229, 30 sept. 2017, texte n° 8.
[928] Règl. (UE) n° 910/2014, préc., considérant n° 49, art. 25, §2. – C. civ., art. 1367, al. 2.
[929] GAVANON (Isabelle), « *Blockchain*, PI et mode : enjeux de la *blockchain* au regard des règles relatives à la preuve électronique », *D. IP/IT* 2019, n°2, pp. 91-95.
[930] LARDEUX (Gwendoline), « Preuve : modes de preuve », *Rép. civ. Dalloz*, v° Les preuves parfaites, 2019, n° 207.
[931] CAPRIOLI (Éric A.), AGOSTI (Pascal), « Principales évolutions du régime de la signature, du cachet et de la copie numériques », *AJCA* 2016, n° 2, p. 2.
[932] CA Aix-en-Provence, 8e Ch., 26 juin 2014, n° 13/19600 : JurisData n° 2014-024259 : « le principe n'est pas qu'à défaut de respecter les exigences du décret, la signature est sans valeur mais seulement que la fiabilité du procédé n'est pas présumée ». – Confirmé par, Cass. Civ. 1ère, 6 avr. 2016, n° 15-10.732 : JurisData n°2016-011416 (« La validité d'une signature électronique peut être reconnue dès lors qu'elle

discrimination technologique expressément prescrit par la Commission, et repris en majeure partie par l'art. 1366 du C. civ., qui refuse d'aboutir, par le biais de la présomption, à un quelconque jugement de valeur juridique entre les signatures électroniques[933]. L'expression de ces exigences a donné naissance au « principe d'équivalence fonctionnelle » siégeant au sein du règlement « eIDAS », au considérant n° 49, couplé à l'art. 25, §1 et §2, et instituant que ni la forme électronique de la signature, ni sa non-conformité à l'intégralité des impératifs requis pour la signature qualifiée, ne peuvent être retenus comme motif pour refuser de constater sa fiabilité. Par conséquent, ce n'est pas parce que la *blockchain* ne permet ni l'établissement ni la certification des écrits inscrits par un tiers de confiance qu'elle ne peut être admise par le juge. Simplement dépourvu de présomption, à l'instar des commencements de preuve par écrit il appartiendra, d'une part, au juge de fonder sa propre conviction en appréciant souverainement la valeur probante de l'écrit électronique[934] et, d'autre part, à la partie qui l'invoque de produire à l'instance les éléments de preuve suffisants à prouver la fiabilité du dispositif utilisé[935].

120. La possibilité de démontrer la fiabilité du procédé utilisé : l'application du principe de neutralité technologique. En parallèle, si le règlement « eIDAS » se veut non-discriminant vis-à-vis du type de signature utilisé, il préconise tout autant la neutralité en ce qui concerne le procédé technologique exploité[936]. Il s'agit de la seconde facette du principe d'équivalence fonctionnelle de l'art. 25, §1, du règlement. Jusqu'à présent, seules les signatures découlant de mécanismes de cryptographie asymétrique, et en particulier d'algorithmes RSA, sont juridiquement admises. Mais il ne s'agit pas de l'archétype de la signature électronique selon la Commission puisque cette dernière n'exclut pas l'émergence de nouvelles techniques. En effet, elle se déclare au contraire « ouverte aux innovations »[937], « pour autant que les exigences posées […] soient satisfaites »[938]. Le corps du règlement ne fait d'ailleurs pas lui-même spécialement échos

remplit les exigences prévues aux articles 1316-1 et 1316-4 du Code civil, exigences que le juge est tenu de vérifier, sans pour autant devoir correspondre aux exigences cumulées de l'article 2 du décret du 30 mars 2001 applicables uniquement au bénéfice de la présomption de fiabilité. »).

933 CAPRIOLI (Eric A.), AGOSTI (Pascal), « Principales évolutions du régime de la signature, du cachet et de la copie numériques », art. cit., p. 2.

934 GAVANON (Isabelle), art. cit., *loc. cit.*

935 LARDEUX (Gwendoline), *op. cit.*, n°s 205-206.

936 V. par exemple, CJUE, 15 sept. 2001, n° C-540/09, *République Fédérale d'Allemagne* (« en cas d'intervention publique, celle-ci doit viser la neutralité technologique, et que s'il peut être admis que les pouvoirs publics décident de soutenir une option technique déterminée, c'est seulement si ce soutien est justifié par des objectifs d'intérêt général définis et proportionnés »).

937 Règl. (UE) n° 910/2014, préc., considérant n° 26 : « vu la rapidité de l'évolution technologique, le présent règlement devrait consacrer une approche qui soit ouverte aux innovations ».

938 *Ibid.*, considérant n° 27.

à une technologie ou même à un modèle de technologies[939]. Il apparaît ainsi que la performance prévaut, en lien avec la recherche continuelle d'infaillibilité. Or, sur ces points, la *blockchain* a le potentiel pour apporter sa pierre à l'édifice. Dans ses choix, tant de promulguer la non-discrimination et la neutralité technologique, que d'impulser l'ouverture à l'innovation, le règlement « eIDAS » semble lui laisser l'opportunité de faire ses preuves. Reste alors pour la partie qui voudrait se prévaloir d'une signature lors d'une instance – qu'il s'agisse donc du signataire comme de son cocontractant[940] – de démontrer la fiabilité du procédé utilisé lors de leur accord, et au juge d'évaluer son admissibilité à l'instance.

Comme le souligne une auteure, cela suggère donc de déterminer la façon dont les juges du fond vont apprécier la valeur probante d'informations inscrites sur une *blockchain*, en particulier en cas de contestation de la partie à qui l'acte est opposé[941].

B. La dangerosité d'une divulgation d'informations identifiantes pour les utilisateurs d'une blockchain

121. La preuve de fiabilité et l'impératif de l'identification. Le juge peut être invité à examiner deux types de demandes. D'une part, il pourrait s'agir d'un créancier sollicitant son appréciation concernant la fiabilité de sa propre signature. La jurisprudence révèle que nombre d'organismes ont recours aux procédés de signature électronique, notamment pour des affaires de recouvrement. Face à des contestations de diverses natures fondées sur l'invalidité de ces signatures – qui se répercutaient sur la validité de l'acte juridique sur lequel elles sont apposées –, les représentants de ces organismes ont dû démontrer la fiabilité du procédé utilisé afin de faire reconnaître la régularité des actes qu'ils avaient émis et enfin de pouvoir contraindre leurs débiteurs à s'exécuter[942]. D'autre part, il pourrait s'agir d'un créancier lui demandant d'apprécier la fiabilité du procédé de signature proposé à son client pour signer électroniquement un contrat que ce dernier conteste. Il en irait ainsi d'une société auprès de laquelle un individu aurait signé un contrat d'adhésion à des services divers, telle qu'une police d'assurance ou un crédit à la

[939] Les articles 3 §10 et 25 §1 du règlement sont exempts de toute indication allant en ce sens.
[940] CPC, art. 287, al. 2.
[941] GAVANON (Isabelle), art. cit., *loc. cit.*
[942] V. par exemple, Cass. Civ. 2e, 17 mars 2011, n° 10-30.501 (était contestée par la société débitrice « la validité des mises en demeure que l'Union de Recouvrement des Cotisations de Sécurité Sociale et d'Allocations Familiales de Haute Savoie lui a adressées […], pour obtenir le paiement des rappels constatés à la suite [d'un] contrôle de ses Établissements […], en faisant valoir que la signature, manifestement pré-imprimée, ne permet pas de savoir si les documents qui lui font grief ont été authentifiés par un agent de l'Organisme ayant qualité et pouvoir pour le faire ». La Cour a ainsi rappelé que les tribunaux devaient impérativement procéder à la vérification du procédé mis en œuvre).

consommation, et qui exigerait de son client le règlement des échéances dues en vertu du contrat. Face à un client qui nierait la validité de sa signature et *a fortiori* de son consentement à l'acte, la jurisprudence indique qu'il incombe à la société de prouver que le client a valablement signé le contrat et a donc consenti aux obligations afférentes[943].

En définitive, pour que le juge puisse, de son côté, évaluer la valeur probante du procédé de signature utilisé, la partie qui souhaite s'en prévaloir doit démontrer sa fiabilité. Autrement dit, elle doit prouver que son système de signature électronique est conforme aux règles du référentiel général de sécurité visé par les textes, et notamment qu'il remplit les conditions requises pour que la signature soit considérée comme identifiant celui qui l'appose. En ce qui concerne la *blockchain*, il semble essentiel de réussir à renverser l'incertitude existante concernant ses capacités d'identification.

122. La méthode du faisceau d'indices. L'identification du signataire avec un procédé de signature électronique classique découle, en général, d'un ensemble d'informations qui, reliées les unes aux autres, permettent de certifier à la fois l'identité de l'expéditeur et l'identité du destinataire. En plus de ne pas être doté d'une représentation visuelle, la signature électronique prend une forme particulière par rapport à la signature manuscrite. Sans que l'expéditeur, ni le destinataire, ne s'en aperçoivent, l'application de création de signature électronique joint à la signature quatre éléments, à savoir le message codé par la clé publique du destinataire, la fonction de hachage utilisée, la signature électronique de l'expéditeur, ainsi que sa clé publique. En théorie, il suffirait au destinataire d'ouvrir le message transmis avec sa clé privée et calculer son *hash*, puis d'ouvrir la signature électronique avec la clé publique de l'émetteur pour obtenir le *hash* initial, et enfin de comparer le premier *hash* au second tant pour s'assurer de l'intégrité du message que pour confirmer ou non l'identité de l'expéditeur[944].

---

[943] V. par exemple, Cass. Civ. 1ère, 6 avr. 2016, n° 15-10.732 (la signature « d'une demande d'adhésion sur internet à une assurance complémentaire » était contestée par le débiteur. Il refusait, par conséquent, de payer les sommes dues).

[944] Pour reprendre l'exemple précédent avec la *blockchain*, afin d'authentifier l'origine du message et vérifier l'intégrité du contenu, la banque doit effectuer d'autres contrôles. Elle utilise une fonction de hachage pour factoriser le message en une suite de chiffres. Ensuite, ce condensé est à nouveau crypté, mais cette fois avec la clé privée de la banque qui constitue la signature électronique de la banque. La banque va alors transmettre à Louis quatre éléments, à savoir (1) le message objet du transfert codé par la clé publique de Louis, (2) la signature électronique de la banque, (3) la fonction de hachage utilisée, et enfin (4) la clé publique de la banque. Louis va alors décoder le message avec sa clé privée, et ensuite décrypter la signature électronique de la banque pour obtenir le condensé crypté du message. De son côté Louis va crypter le message qu'il vient de recevoir avec la même fonction de hachage que la banque et va comparer les deux *hash.* S'ils sont identiques, cela signifie que le message n'est pas altéré. Comme les couples de clés sont uniques, c'est la preuve que la banque est véritablement à l'origine du message et que Louis en était effectivement le destinataire. La banque ne pourra jamais arguer ne pas avoir envoyé le message ou de ne pas en être à l'origine. De son côté, Louis ne pourra pas dire qu'il n'a pas reçu ce message. La signature

La même méthode pourrait être utilisée à l'égard d'une signature obtenue par le biais d'une *blockchain*, d'autant plus qu'elle présente des similitudes avec le procédé utilisé par le protocole lui-même[945]. À partir du document original, impérativement conservé de manière intacte par les parties, et de la clé privée de l'expéditeur, il s'agirait de calculer le *hash* du document fourni et dont l'origine autant que le contenu seraient à vérifier. Ensuite, il faudrait reproduire la fonction de hachage pour obtenir la signature électronique en utilisant le *hash* précédemment calculé, et la clé privée. Il conviendrait enfin de comparer la signature obtenue de ces calculs et celle inscrite en clair sur la *blockchain*, qu'il est d'ailleurs possible de repérer grâce à un explorateur de *blockchain*[946]. Le résultat de cette comparaison permettrait immédiatement de confirmer ou d'infirmer la paternité dudit document, mais également de vérifier si le contenu a été modifié unilatéralement, voire falsifié. En effet, une adresse erronée ou la modification d'un seul caractère au sein du document est propre à altérer la valeur de son *hash*[947]. Dans l'idéal, il s'agirait pour la partie qui souhaite se prévaloir de la signature obtenue grâce au procédé d'une *blockchain* de prouver la fiabilité du mécanisme à travers un faisceau d'indices similaire à ceux exposés, capable de confirmer l'identité tant de l'expéditeur que du destinataire à partir d'informations en partie disponibles en clair sur la chaîne, à savoir, l'adresse publique de l'expéditeur, le *hash* de la « transaction » c'est-à-dire de l'inscription du message, et/ou du numéro de bloc contenant l'inscription.

Quid toutefois du contractant n'ayant pas accès à la clé privée qui a été utilisée par son cocontractant pour signer l'acte ? En d'autres termes, comment la société d'assurance ou la banque pourrait-elle prouver, à la fois la fiabilité de l'identification effectuée par le procédé de signature qu'elle a mis à disposition de son client, et l'identité de ce dernier ? Dans le cadre d'une instruction ou d'une enquête judiciaire, l'art. 230-1 du CPP astreint en principe le juge à « effectuer les opérations techniques permettant d'obtenir l'accès à ces informations », autrement dit à obtenir « leur version en clair », y compris si cela le conduit à devoir exiger, « si cela apparaît nécessaire [et] dans le cas où un moyen de cryptologie a été utilisé », la convention secrète de déchiffrement, c'est-à-dire la clé privée. Dans ce cas, le tribunal peut recourir aux services d'un prestataire agréé,

électronique est donc un processus informatique qui s'appuie sur un protocole d'authentification et d'identification autrement sécurisé.

[945] Sur les mécanismes de hachage utilisés par le protocole de *Bitcoin*, notamment, *supra* n°s 103 et s.

[946] DELAHAYE (Jean-Paul), *Mathématiques et mystères*, éd. Belin, coll. Pour la science, 2016, pp. 45-46. – HELLEU (Guillaume), MASURE (Anthony), art. cit., p. 75.

[947] Comme évoqué précédemment, le hash de « Bonjour ! », calculé avec la fonction de hachage *SHA256* correspond à « bc7444869484dd1ed34bfc4465724b887fecf604fcad0d0eaf40d3746d0bfeb7 ». Toutefois, si le simple « ! » est retiré de l'expression hachée, l'empreinte devient « 9172e8eec99f144f72eca9a568759580edadb2cfd154857f07e657569493bc44 ».

séquestre des conventions secrètes, qui tient la place de Tierce Partie de Confiance[948]. De plus, le juge peut condamner à une peine d'emprisonnement allant jusqu'à trois ans, et à une amende de 270 000 €, l'individu qui, dans cette situation, refuserait de remettre la clé privée en cause aux autorités judiciaires ou de la mettre en œuvre[949].

Le juge civil quant à lui n'a pas à disposition de textes juridiques envisageant de manière spécifique la question de la clé privée ou de la « convention secrète de déchiffrement ». Mais, cela ne signifie pas qu'il ne peut prendre aucune mesure à l'encontre de l'utilisateur d'un moyen de cryptologie[950]. Force est de constater que les règles procédurales lui permettent, dans certaines conditions et notamment de certitude sinon de vraisemblance de son existence, de contraindre une partie à produire un élément de preuve qu'elle seule détient (CPC, art. 11, 143 et s.)[951]. Guidé par l'importance croissante du « droit à la preuve », le juge a effectivement le pouvoir d'apprécier, à la requête de l'autre partie, à la fois la nécessité et la proportionnalité d'une telle mesure[952]. Si le juge civil n'a pas le pouvoir de contraindre par le biais de peines privatives de liberté, il a toutefois à disposition un panel de peines qu'il peut prononcer, prenant la forme d'une astreinte (CPC, art. 11, al. 2) et de dommages et intérêts (C. civ., art. 10, al. 2). Il peut également tirer d'office les conséquences d'une abstention ou d'un refus (CPC, art. 11, al. 1er).

Mais il reste que, dans une telle approche, il est essentiel que le juge s'engage à protéger, tout au long de l'instance, le secret de toute clé privée ayant été révélée par leurs propriétaires[953].

---

[948] Régi par la L. n° 90-1170, 29 déc. 1990, sur la réglementation des télécommunications, *JORF* n° 303, 30 déc. 1990, et le D. n° 2007-663, 2 mai 2007, pris pour l'application des articles 30, 31 et 36 de la L. n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie, *JORF* n° 104, 4 mai 2007, texte n° 1.

[949] C. pén., art. 434-15-2 : « Est puni de trois ans d'emprisonnement et de 270 000 € d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du code de procédure pénale. Si le refus est opposé alors que la remise ou la mise en œuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 450 000 € d'amende. » – V. également, DECORSE (Johanne), « Une plate-forme bitcoin démantelée, une première en France », *L'Usine Nouvelle* [en ligne], 7 juill. 2014, https://www.usinenouvelle.com/article/une-plate-forme-bitcoin-demantelee-une-premiere-en-France.

[950] D'après la définition officielle, « on entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité. » [L. n° 2004-575, 21 juin 2004, pour la confiance dans l'économie numérique, *JORF* n° 0143, 22 juin 2004, texte n° 2].

[951] V. sur le sujet, BLONDEAU (Alison), « Le juge civil face au secret entourant le système de clé privée sur blockchain », *in* NEVEJANS (Nathalie) (dir.), *Données et technologies numériques. Approches juridique, scientifique et éthique*, éd. mare & martin, coll. Droit & Science politique, 2021, pp. 159-160.

[952] Cass. Civ. 1ère, 5 avr. 2012, n° 11-14.177, *D.* 2012. 1597, note G. Lardeux.

[953] BLONDEAU (Alison), art. cit., pp. 161-162, 164.

123. La vulnérabilité des informations requises à titre d'identification : une apparence de facilité. Seulement, si, en théorie, s'identifier en fournissant les informations nécessaires paraît être la solution qui s'impose par sa simplicité, en pratique, délivrer une clé privée peut se révéler dangereux dans le cadre des *blockchains,* et en particulier des *blockchains* financières[954]. En effet, selon la clé révélée, l'accès et la disposition d'un compte dans son intégralité peuvent être ainsi permis. Une clé privée est source d'importantes convoitises, notamment lorsqu'elle est capable de débloquer à elle seule l'intégralité des fonds d'un compte vers un autre compte, sans que son propriétaire puisse évoquer ni prouver efficacement la fraude ou en demander l'annulation. Dans le cadre d'une simple signature, elle permettrait à n'importe quel individu l'interceptant d'usurper la signature de son propriétaire, et finalement une partie de son identité numérique. Bien que toutes les dispositions nécessaires à en garantir la confidentialité pourraient être prises[955], eu égard à la vulnérabilité de cet élément, rien ne préserve le juge d'un refus émanant d'un propriétaire réticent. D'ailleurs, la jurisprudence en matière de dispositifs de signatures électroniques classiques ne semble pas avoir procédé par obtention des identifiants ou, à tout le moins, de données aussi vulnérables lorsqu'il était question d'identifier le destinataire ou l'expéditeur d'un acte signé électroniquement. En effet, la signature électronique classique est, en règle générale, créée et gérée par un programme informatique spécifique. Bien qu'il prenne autant de formes que de noms différents dans la pratique, ce dispositif de création de signature électronique intègre un logiciel de vérification de signature électronique qui exécute automatiquement l'ensemble des opérations tenant aux calculs et comparaison de *hash*[956]. Le protocole des *blockchains* est également programmé pour effectuer ces vérifications lors de l'étape de l'inscription sur la chaîne, cependant, contrairement à elles, les dispositifs classiques retournent aux utilisateurs le résultat de leurs calculs et sont capables de certifier l'identité réelle de l'utilisateur. Plus encore, pour renforcer l'identification, bien souvent ces dispositifs munissent la signature d'un « certificat de signature électronique » (CSE)[957]. Ce CSE contient diverses données d'identification personnelles[958], telles que des données d'identité avec le nom ou le pseudonyme de son utilisateur, les dates de début et de fin de validité du certificat, l'autorité ou l'organisme émettrice, et la clé publique de l'utilisateur. Ils peuvent être émis « à la volée »[959], c'est-à-dire à usage unique, ou par des Autorité de

[954] *Ibid.*, p. 157.
[955] *Ibid.*, pp. 161-162.
[956] *Supra* n° 122.
[957] Règl. (UE) n° 910/2014, préc., art. 3, §14.
[958] *Ibid.*, Annexe I.
[959] V., PAPIN (Etienne), « Le certificat électronique à la « volée » comme succédané à la signature électronique présumée fiable : pour qui ? Pour quoi ? », *Feral Avocats* [en ligne], 16 juin 2015,

certification (AC) qui procèdent à des vérifications d'identité lors de l'émission du CSE[960], mais également lors de la phase de vérification de la signature électronique[961] en comparant notamment le certificat avec une liste officielle des certificats révoqués[962].

Une auteure propose de simplifier le procédé et, d'éviter de révéler, même au juge, la clé privée, en apposant le *hash* obtenu *via* la chaîne de blocs en tant que nom du document original conservé électroniquement par celui qui voudrait s'en garder la preuve[963]. De cette façon il serait possible de prouver le lien logique entre le *hash* inscrit sur la *blockchain* et le *hash* qui nomme le document original, dont la date d'enregistrement se trouverait dans les propriétés dudit document[964]. Cependant, ne serait-il pas possible de lancer un système d'exploitation à une date et à une heure fixées, et d'enregistrer, sous le nom du *hash* du document original inscrit sur la chaîne, un nouveau document au sein de cet espace temporellement modifié[965] voire, simplement, d'intervertir deux documents différents dès l'inscription de l'original ?

Finalement, en l'état actuel, la *blockchain* ne semble pas être capable de fournir une preuve de la fiabilité de son système de signature numérique en ce sens que, principalement, elle n'est pas en mesure de fournir un schéma solide d'identification sans risquer de mettre en danger les informations qu'elle renferme. En effet, bien que la solution de transmettre la clé privée utilisée pour signer pourrait permettre, sur le plan probatoire, d'apporter la preuve incontestable tant de la fiabilité de la signature que de sa capacité à identifier son auteur, certaines réserves persistent du point de vue de la confidentialité. D'autant plus qu'au-delà de l'identification et de la confidentialité, le risque est, à terme, de fragiliser la sécurité de l'intégralité de la chaîne utilisée.

124. Force est de reconnaître qu'en l'état actuel, ce pan de la *blockchain* ne se distingue que trop de celui de la signature électronique classique. Pourtant, malgré ces nombreuses difficultés rencontrées, il n'en demeure pas moins que la technologie *blockchain* dispose de fonctionnalités dont le domaine de l'écrit probatoire et du document électronique

http://www.feral-avocats.com/fr/publication/le-certificat-electronique-a-la-volee-comme-succedane-a-la-signature-electronique-presumee-fiable-pour-qui-pour-quoi/.

[960] Règl. (UE) n° 910/2014, préc., art. 24, §1.

[961] *Ibid.*, art. 32, §1, et 33.

[962] *Ibid*., art. 22. – La liste française est consultable en ligne, sur le site officiel de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-reglement-eidas/liste-nationale-de-confiance/. Empreinte de la liste (à la date du 2 mars 2021) : 75e3d48d27515135f15617bf4fd109c76077a5de084c0f09c65875aaeaa551a5.

[963] GUILHAUDIS (Élise), art. cit., p. 12.

[964] *Id.*

[965] La date ainsi redéfinie correspondrait à la date apparaissant sur le registre de la *blockchain*, de sorte que, si le juge ne vérifie pas le *hash* à partir des différents éléments l'ayant produit – et en particulier à partir de la clé privée – la preuve de propriété serait valablement falsifiée.

pourrait tirer avantage. Il apparaît alors qu'elle pourrait s'inspirer du procédé auquel elle est si proche techniquement, de manière à rendre sa reconnaissance envisageable.

§ 2. La recherche de solutions conformes aux exigences probatoires

125. Il était question précédemment d'élaborer ce qui aurait été un faisceau d'indices permettant la reconnaissance de la fiabilité de l'identification effectuée par le mécanisme de signature *via blockchain*. Or, les indices mis actuellement à disposition par les *blockchains* utilisées ne sont pas suffisants, et pourraient parfois même exposer ces dernières à des risques conséquents dans le cas où certains éléments seraient découverts. Face à ces multiples difficultés, il apparaît intéressant d'établir un processus probatoire visant l'irréfutabilité et la reconnaissance du procédé comme étant une variété de signature électronique existante. Pour déterminer la façon dont les juges du fond vont apprécier la valeur probante d'informations inscrites sur une *blockchain*, il faut préalablement déterminer la façon dont ils apprécient actuellement la fiabilité du système d'authentification d'une signature électronique classique, tout en préservant son intégrité. Ces questions avaient fait l'objet d'une étude par le Comité Européen de Coopération Juridique (CECJ) qui visait à mettre en évidence l'existence d'une « procédure légale spécifique » à la production en justice d'éléments de preuve électroniques, sinon de « lignes directrices techniques ou […] bonnes pratiques publiées » y faisant référence au sein des États membres[966]. Le législateur français avait alors répondu par la négative à ces deux interrogations. À défaut de fournir de plus amples précisions sur les exigences probatoires communément admises, cette étude confirme que la valeur probante d'un élément dépend de sa capacité à emporter la conviction du juge.

Des auteurs ont cherché une solution applicable à la *blockchain* et nombre d'entre eux, malgré les réticences de la communauté, soutiennent le recours à des tiers de confiance, à l'instar de ce qui est mis en place pour les signatures électroniques qualifiées[967]. Il semble pourtant que, au risque de ne pas bénéficier de la présomption de fiabilité, la technologie et son écosystème disposent d'autres moyens, sans risque pour la

[966] MASON (Stephen), *L'utilisation des preuves électroniques dans les procédures civiles et administratives et son impact sur les règles et modes de preuves. Étude comparative et analyse, rapport préparé par Stephen Mason, avec le concours de Uwe Rasmussen*, Strasbourg, 27 juill. 2016, CDCJ(2015)14-final [en ligne], n°s 56 et s., notamment Questions n°s 10 et 12, https://rm.coe.int/16807007ca.

[967] À ce titre, v., notamment, DOUVILLE (Thibault), VERBIEST (Thibault), « Blockchain et tiers de confiance : incompatibilité ou complémentarité ? », *D.* 2018, pp. 1144 et s. – BARREAU (Catherine), « La régulation des smart contracts et les smart contracts des régulateurs », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 75.

confidentialité, qui leur permettraient, en s'inspirant des solutions d'identification déjà admises, de s'adapter au régime probatoire imposé par les textes et la jurisprudence.

Il s'agit donc, dans un premier temps, d'effectuer une analyse de l'interprétation par les juges du fond des exigences légales en matière de fiabilité d'un dispositif de signature électronique afin d'élaborer un prototype de schéma probatoire applicable à la technologie *blockchain* et susceptible d'emporter la conviction des juges du fond (A). Il conviendra, dans un second temps, d'étudier la possibilité d'adapter la technologie en créant, à partir de solutions existantes, son propre système autonome d'identification (B).

A. Analyse des exigences probatoires

126. L'évolution des exigences des tribunaux. Au début des années 2010, les juges saisis d'affaires dans lesquelles intervenait une signature électronique prêtaient une attention particulière au fait que le signataire contestait ou non la validité de sa signature. En effet, en présence d'une contestation ou d'une dénégation d'écriture, les juges du fond sont obligés, en vertu de l'art. 287, al. 2, du CPC, de procéder à une vérification d'écriture[968]. En matière de signatures électroniques, cette mesure se traduit en principe par une vérification de la fiabilité du procédé, et notamment du dispositif d'identification[969], à la lumière des conditions de validité prévues par les art. 1366 et 1367 du C. civ.[970]. Ainsi, dans un arrêt en date du 2 mai 2013, le juge a constaté que l'emprunteur ne déniait pas avoir signé et a donc reconnu *ipso facto* la fiabilité de la signature[971]. Peu importait finalement que le procédé de signature soit effectivement fiable et suffisamment identifiant, ou non. Toutefois, il apparaît que, dès lors qu'il y a eu dénégation de signature, le juge a refusé de reconnaître la fiabilité du dispositif de signature utilisé, et a écarté l'écrit électronique sur lequel la signature était apposée, au motif qu'il ne présentait « aucune garantie d'authenticité » alors même que le demandeur avait produit un CSE émis par le logiciel de signature[972].

---

[968] CHOLET (Didier), « Vérification d'écriture », *Rép. pr. civ. Dalloz*, v° Rôle du juge et des parties, 2016 (actualisation : 2019), n°s 9-11.
[969] *Id.*
[970] V., Cass. Civ. 1ère, 15 juin 1999, n° 97-18.446, *Bull. civ*. I, n° 203 ; Cass. Civ. 1ère, 16 janv. 2007, n° 06-12.207.
[971] V. par exemple, CA Douai, 8e Ch., Sect. 1ère, 2 mai 2013, n°12-05299, comm. CAPRIOLI (Éric), « Signature électronique d'un avenant électronique d'un contrat de crédit à la consommation », *Comm. com. électr*. 2014, comm. 2. En l'espèce il apparaît que le défendeur n'avait pas été représenté au cours de l'audience, et n'avait pas non plus contesté la fiabilité de la signature ou sa propriété, le juge a donc admis l'écrit à titre de preuve à son encontre pour la condamner à payer les sommes dues en vertu du contrat signé.
[972] TI Épinal, 12 déc. 2011, n° 11-11-000080.

Cette décision du tribunal d'instance d'Épinal a été tantôt critiquée tantôt approuvée[973]. Un auteur soulignait qu'elle reflétait une lecture quelque peu faussée des textes[974], un autre concédait que la preuve « avait été mal présentée au juge »[975]. Il n'en demeure pas moins qu'en termes de confiance, cette décision « a été perçue comme un mauvais signal judiciaire pour [un] marché émergeant »[976]. De plus, elle mettait en évidence l'existence d'une incertitude généralisée en ce qui concerne l'administration et la gestion des preuves électroniques dans les systèmes judiciaires. Force est de constater qu'à ses débuts, la mise en œuvre de la signature électronique classique, elle aussi, n'a pas été sans soulever de nombreuses difficultés. Comme le souligne une auteure, « confronter les apports de la *blockchain* aux principes généraux du droit de la preuve relève du même type d'enjeu »[977].

Il convient de rappeler que ce n'est pas parce que l'écrit et la signature qui l'accompagne se présentent sous une forme électronique qu'ils ne sont pas valables. Ce point a d'ailleurs motivé un revirement opéré dans la même affaire par la Cour d'appel de Nancy le 14 février 2013[978]. La Cour s'est attachée à une application plus stricte des textes afin de mettre en exergue les modalités relatives à l'administration de la preuve électronique devant un juge[979] et ainsi pourvoir, progressivement par interventions successives, le marché de bases jurisprudentielles stables en la matière. Leur efficacité témoigne de la possibilité d'élaborer une méthode probatoire applicable à toute signature émise *via* un support électronique, y compris la signature du protocole *blockchain*. Les signatures électroniques reconnues fiables par les tribunaux sont donc celles capables de garantir tant l'intégrité que l'imputabilité du contenu de l'information transmise, la sécurisation du procédé et, de manière subsidiaire, le consentement du signataire – étant donné que les affaires concernent le plus souvent la souscription d'avenants renouvelant des crédits *revolving*. Dans la pratique, l'étendue des services automatisés proposés aux utilisateurs varie selon la plateforme ou le logiciel utilisé(e). Par conséquent la signature reconnue correspondra à une signature simple ou à une signature avancée dans le sens du règlement eIDAS en fonction des éléments qui auront pu être produits par la partie qui

[973] RENARD (Isabelle), « E-commerce : Une bonne et une mauvaise nouvelle pour la signature électronique des contrats B to C », *Expertises*, mars 2013, n° 378, pp. 103-104.
[974] PAPIN (Etienne), « Le certificat électronique à la « volée » comme succédané à la signature électronique présumée fiable : pour qui ? Pour quoi ? », art. cit., p. 2.
[975] CAPRIOLI (Éric A.), AGOSTI (Pascal), art. cit., p. 418.
[976] CA Nancy, 14 févr. 2013, préc., comm. CAPRIOLI (Éric), « Première décision sur la preuve et la signature électroniques d'un contrat de crédit à la consommation », *JCP G* 2013, II, n° 18, pp. 866-869.
[977] MAGNIER (Véronique), « Enjeux de la blockchain en matière de propriété intellectuelle et articulation avec les principes généraux de la preuve », *D. IP/IT* 2019, n° 2, p. 76.
[978] CA Nancy, 14 févr. 2013, n° 12/01383 : *JurisData* n° 2013-004062.
[979] CAPRIOLI (Éric A.), AGOSTI (Pascal), « Principales évolutions du régime de la signature, du cachet et de la copie numériques », art. cit., *loc. cit.*

s'en prévaut. Toutefois, mise à part l'importance pour les parties d'opter pour l'une ou pour l'autre en fonction des risques afférents à la relation contractuelle en formation[980], le niveau de signature importe peu d'un point de vue probatoire. En effet, la mise en œuvre d'une signature ne se cantonne pas à sa qualité mais à sa validité en ce sens qu'une signature électronique, même simple, fournit force probante à l'écrit électronique sur lequel elle est apposée si elle emporte la conviction du juge.

Ainsi est-il possible d'élaborer un schéma probatoire en la matière. Rapporter la preuve des fonctionnalités attendues d'une signature électronique consiste en la réunion de trois éléments, éventuellement quatre en fonction du dispositif utilisé, dont le niveau de sécurité technique varie en fonction du degré de sécurité juridique correspondant.

127. L'élaboration d'un prototype de schéma probatoire applicable à la technologie *blockchain* : l'exigence de production de l'écrit original. Il s'agit d'abord de produire à l'instance le document original sans signature[981] correspondant à une « représentation lisible » de l'acte électronique[982].

Pour pouvoir administrer la preuve de l'intégrité des termes de l'acte signé *via* une *blockchain*, il reste donc essentiel, pour la partie qui s'en prévaut, d'avoir conservé dans un format fixe[983] le document original soumis à signature. D'autant plus que la *blockchain* ne « stocke » que le *hash* de ce document lorsqu'elle l'inscrit et non le document lui-même[984].

128. L'exigence de fiabilité du procédé d'identification. Il appartient ensuite au demandeur d'alléguer et de prouver l'identité du signataire. Selon des auteurs, cette identité doit avoir été préalablement vérifiée, sinon déclarée « de manière suffisamment fiable »[985]. Pour accéder au niveau de sécurité de l'art. 26 du règlement eIDAS s'agissant de la signature électronique avancée, il sera nécessaire de procéder à une vérification d'identité en présentiel, sinon à distance (art. 26, b)) à partir de pièces d'identité ou de pièces justificatives valides transmises par voie électronique[986]. Les auteurs précisent

[980] *Id.*
[981] La signature scannée n'étant pas assimilée à une signature électronique, v. en ce sens, Cass. Civ. 2e, 30 avr. 2003, n° 00-46.467, *Bull. civ*. II, n° 118.
[982] CA Nancy, 14 févr. 2013, préc.
[983] *Supra* note 834 sous n° 104, concernant l'intégrité d'un document et la différence entre un enregistrement PDF et *Word*, par exemple.
[984] *Supra* n° 106.
[985] CAPRIOLI (Éric A.), AGOSTI (Pascal), « Principales évolutions du régime de la signature, du cachet et de la copie numériques », art. cit., *loc. cit.*
[986] CAPRIOLI (Éric A.), AGOSTI (Pascal), « Principales évolutions du régime de la signature, du cachet et de la copie numériques », art. cit., *loc. cit.*

qu'un contrôle minutieux n'est pas obligatoire[987], ce que confirme la jurisprudence en se contentant d'exiger la preuve de « traces de vérifications »[988] ou de la réalisation d'une « recherche »[989]. Le CECJ souligne que « la distinction entre l'identité numérique et l'identité physique peut être source de problèmes pour la fiabilité de la preuve », de sorte qu'il préconise, dans le cas où la législation applicable ne précise pas comment établir l'identité de l'auteur de données électroniques, que la preuve en soit apportée « par tout moyen objectif »[990], tel que par l'utilisation de « mécanismes technologiques qui garantissent la fiabilité des preuves. Par exemple, les certificats de signature électronique »[991]. Il apparaît en effet que la production à l'instance d'un certificat émis « à la volée » et pour une durée déterminée lorsque le signataire est un client déjà connu de l'établissement cocontractant – en l'espèce il s'agissait d'une banque –[992], ou d'un certificat établi par une autorité de certification[993] a permis de prouver la fiabilité du procédé d'identification. Ce certificat, qu'il soit à usage unique ou réutilisable, est entendu comme une « attestation électronique qui associe les données de validation d'une signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne » (art. 3§ 14), et a donc, en principe, l'avantage de remplir l'exigence d'un « lien univoque avec le signataire » fixée à l'art. 26, a). L'analyse des décisions jurisprudentielles révèle également que ce certificat peut être inséré dans un « fichier de preuve », créé spécialement pour prouver la fiabilité du procédé utilisé et délivré au moment de la signature[994]. Éric Caprioli constate d'ailleurs que la preuve de la fiabilité d'une signature électronique se présente sous la forme d'un « ensemble de documents techniques autour de cette signature », et peut ainsi être accompagnée, par exemple, de Politiques de Certification, de Signature, de Gestion de Preuve, ou encore « de l'attestation du fournisseur de service et du fichier (ou dossier) de preuve »[995].

En respectant le schéma probatoire présenté, il s'agirait, pour l'utilisateur qui aurait eu recours à une plateforme de signature électronique reposant sur l'utilisation d'une *blockchain*, de se munir d'une forme de certificat de signature spécifique à la

[987] *Id.*
[988] CA Nancy, 14 févr. 2013, préc.
[989] Cass. Civ. 1ère, 6 avr. 2016, préc.
[990] MASON (Stephen), RASMUSSEN (Uwe), préc., n° 37.
[991] *Ibid.*, n° 38.
[992] CA Nancy, 14 févr. 2013, préc., comm. CAPRIOLI (Éric), « Première décision sur la preuve et la signature électroniques d'un contrat de crédit à la consommation », art. cit., *loc. cit.*
[993] Cass. Civ. 1ère, 6 avr. 2016, n° 15-10.732. En l'espèce il s'agissait de la solution *Contraleo NPAI*.
[994] CA Nancy, 14 févr. 2013, préc. En l'espèce le fichier de preuve avait été délivré par *Keynetics*, un logiciel de signature électronique.
[995] CA Rouen, 31 mai 2018, n° 17/03404 : JurisData n° 2018-009965, comm. CAPRIOLI (Éric), « Charge de la preuve et signature électronique d'un contrat de crédit à la consommation : errances jurisprudentielles », *Comm. com. électr*. 2018, n° 10, comm. 78.

technologie et délivré par la plateforme. Ce certificat lui permettrait de s'identifier et de relier sa signature à son identité. L'opération pourrait d'ailleurs nécessiter une validation de l'identité en amont, lors de l'inscription. Celle-ci pourrait être effectuée en toute autonomie par le destinataire-signataire avant la signature, éventuellement en fournissant une preuve officielle de son identité, telle que la copie ou le numéro de sa carte d'identité nationale. Elle pourrait également faire l'objet d'une demande de validation, plus ou moins exhaustive, auprès des opérateurs de la plateforme dédiée selon le niveau de garantie escompté, suivie éventuellement d'un enregistrement de l'identité sur *blockchain* le cas échéant. Une telle conjoncture impliquerait donc l'inscription de chaque contractant sur la plateforme préalablement à la signature d'un acte. En parallèle il serait éventuellement intéressant d'envisager l'émission d'un document de synthèse par la plateforme s'inspirant du « fichier de preuve » communément admis et énumérant l'intégralité des informations mentionnées nécessaires à la démarche probatoire.

L'exigence de fiabilité du mécanisme d'identification proposé par le dispositif de signature induit également, en ce qui concerne les signatures avancées, l'utilisation sous le contrôle exclusif du signataire des données de création de signature (art. 26, c)). Les auteurs constatent que cette règle a souvent représenté un obstacle au déploiement de la signature électronique sécurisée eu égard à l'obligation implicite de disposer d'un support et de moyens cryptographiques[996]. Il apparaît néanmoins que le protocole des *blockchains* met naturellement à disposition et sous le contrôle exclusif de ses utilisateurs de telles données cryptographiques servant à la création des signatures.

129. L'exigence d'un lien logique entre la signature électronique et la garantie d'intégrité de l'acte. Quel que soit son degré de sécurité, le dispositif de signature utilisé doit être capable d'assurer l'immuabilité de l'écrit électronique signé ainsi que de garantir le lien entre la signature et l'écrit auquel elle est attachée afin de démontrer l'existence du consentement à l'acte. Dans la pratique, il s'est agi le plus souvent d'utiliser, voire de faire figurer sur l'acte, un code sécurisé à usage unique[997] qui associe le document à l'identité de son signataire et qui a pu être communiqué à celui-ci par le biais d'un e-mail, d'un SMS, etc. Plus encore, en établissant un lien logique, par le biais de mécanismes cryptographiques, le dispositif de signature permet de prévenir « toute modification ultérieure des données » conformément à l'art. 26, d), du règlement eIDAS.

[996] CAPRIOLI (Éric A.), AGOSTI (Pascal), « Principales évolutions du régime de la signature, du cachet et de la copie numériques », art. cit., *loc. cit.*
[997] CA Caen, 5 mars 2015, n° 13/03009 : *JurisData* n° 2015-007764.

La dernière étape est donc de réussir à lier de manière infaillible et immuable le document initial conservé, et celui reçu, puis signé et déposé sur la *blockchain*. La solution en matière de *blockchains* pourrait être de faire figurer sur chacun d'eux un numéro unique ou une suite de nombres codés, tels que le numéro d'identification national inscrit sur la carte d'identité nationale, ou d'un autre numéro créé spécialement pour l'opération, par exemple un numéro de contrat, d'avenant[998], de « proposition Internet 5887042 »[999], ou simplement du *hash* du document qui fait l'objet de l'inscription sur la chaîne. En règle générale, et notamment sur *Bitcoin*, il est possible de joindre un message de 80 octets de caractères à une transaction[1000]. Néanmoins, le *hash* du document figure forcément en clair sur la chaîne de blocs. Par ailleurs, le mécanisme du *hash* présente l'avantage d'être beaucoup plus sécurisé puisqu'il constitue véritablement *la* preuve inaltérable de l'intégrité du document conservé.

En parallèle, il est possible également de penser à adapter les exigences légales relatives au consentement, dès l'instant où il est donné, afin d'en tirer parti au moment où il doit être prouvé. Le principe du « double-clic » du droit anglo-saxon, repris par le législateur sous la notion de « confirmation » opérée par le destinataire après avoir vérifié les clauses contractuelles et avant de signer[1001], pourrait ainsi prendre la forme d'une « double-saisie » de la clé privée pour signer. La première saisie interviendrait au moment du *login* sur la plateforme de signature électronique *via* une *blockchain*, la seconde en dernière étape avant d'inscrire définitivement la « transaction » contractuelle. Cette éventuelle solution ne serait toutefois pas applicable au cachet électronique puisque celui-ci ne permet pas d'exprimer un quelconque consentement en ce sens que la personne morale ne peut être que représentée[1002].

130. Le constat d'huissier sur la fiabilité du dispositif. Il apparaît, au travers de plusieurs arrêts datant de 2015 concernant des délégations de pouvoir signées électroniquement, que les juges, en cours d'instance, avaient recouru à l'expertise d'un huissier de justice afin de « constater la fiabilité du processus » utilisé pour signer un pouvoir en ligne[1003].

---

[998] CA Nancy, 14 févr. 2013, n° 12/01383, préc.
[999] Cass. Civ. 1ère, 6 avr. 2016, n° 15-10.732.
[1000] Cette application de la *blockchain Bitcoin* est permise par l'utilisation de la commande « *OP_RETURN* ». Elle crée une « requête de paiement » sans sortie puisqu'il est techniquement impossible de la dépenser. Par ailleurs, *Bitcoin Cash* limite la taille du message à 220 octets depuis mai 2018.
[1001] C. civ., art. 1127-2, al. 1er.
[1002] QUEMENER (Myriam), *Le droit face à la disruption numérique : Adaptation des droits classiques - Émergence de nouveaux droits*, éd. Gualino, Hors collection, 2018, p. 207.
[1003] CA Caen, 5 mars 2015, préc. – CA Nîmes, 1er oct. 2015, n° 14/01618.

Conformément à l'art. 143 du CPC[1004] le juge peut en effet, dès lors qu'il l'estime nécessaire, solliciter l'expertise d'un professionnel, huissier de justice ou spécialiste de la *blockchain*, dont il considère que l'examen et/ou les connaissances peuvent l'éclairer dans sa prise de décision. Cette expertise peut jouer un rôle décisif dans la constatation de la fiabilité du procédé de la *blockchain*.

131. Finalement, l'association de ces divers éléments est parvenue à faire reconnaître la fiabilité des procédés classiques de signature électronique. Ce constat suggère qu'en adoptant un schéma probatoire similaire, la signature du protocole *blockchain* pourrait également figurer comme étant une variété de signature électronique valable devant les tribunaux. Cependant, il semble pour cela que la technologie *blockchain* devra veiller au plus vite à s'adapter en retour aux exigences légales, et elle devra en particulier permettre malgré tout un commencement d'identification[1005].

B. Préludes d'un système autonome d'identification

132. L'existence de mécanismes d'identification découlant des exigences en matière de KYC. La question de l'adaptation aux exigences légales d'identification s'est en réalité déjà posée pour des raisons d'intérêt public. Bien qu'il s'avère fondamental pour la confidentialité des informations d'instaurer un niveau de sécurité élevé sur les plateformes en ligne[1006], les autorités judiciaires, et plus particulièrement en matière pénale, peuvent en effet solliciter une collaboration dans le cadre d'une enquête l'exigeant (C. pén., art. 230-1, al. 1er) [1007]. Cette collaboration suppose que la plateforme visée soit en mesure de transmettre aux autorités certaines données identifiantes, y compris, en cas de besoin, des séquences de clés privées utilisées pour signer des transactions sur une

[1004] Dans le respect des prescriptions de l'art. 146 du CPC, à savoir les exigences d'éléments préalables suffisants fournis par la partie qui allègue le fait faisant l'objet d'une expertise et l'absence de carence dans l'administration de la preuve.
[1005] *Supra* n°115, notamment en ce qui concerne les exigences pénales.
[1006] Il en va ainsi des divers protections mises en place par le législateur concernant la vie privée (C. civ., art. 9 ; CRPA, art. L. 311-6 (dans le cadre des relations avec l'administration) ; CE, 17 avr. 2013, Min. du travail, de l'emploi et de la santé c/ Cabinet de La Taille, req. n° 344924, mentionné tables *Recueil Lebon*. 38 (principe incluant les personnes morales également)), le secret professionnel (C. pén., art. 226-13 et 226-14 ; v., par exemple, Cass. Crim., 7 mars 1989, n° 87-90.500 (concernant les avocats) ; Cass. Com., 8 févr. 2005, n° 03-10.749 (concernant les experts comptables)), le secret des affaires (L. n° 2018-670, 30 juillet 2018, relative à la protection du secret des affaires, *JORF* n° 0174, 31 juillet 2018, texte n° 1, transposition en droit internet de la Dir. (UE) n° 2016/943 du Parlement européen et du Conseil, 8 juin 2016, sur la protection des savoir-faire et des informations commerciales non divulgués (secret d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, *JOUE* L 157, 15 juin 2016, pp. 1-18), le secret de fabrication (notamment, CPI, art. L. 621-1), le secret médical (CSP, art. L. 1110-4 et L. 1111-7), le secret de la défense nationale (C. pén., art. 413-9).
[1007] *Supra* n° 115.

blockchain. C'est ainsi qu'est apparu le processus « *Know Your Customer* » (KYC). Issue d'obligations de mise en conformité[1008], la politique KYC est désormais appliquée dans la quasi-totalité du monde des affaires au niveau international, et aide les professionnels à se prémunir contre des activités illégales en mettant en place un système de vérification de l'identité de leurs clients[1009]. Face, d'une part, à ces impératifs juridiques et, d'autre part, à la méfiance sociétale vis-à-vis du protocole, alimentée de divers cas de corruption, de financement du terrorisme et de blanchiment de capitaux permis par l'utilisation dérivée de *Bitcoin*, l'écosystème *blockchain* a évolué.

Plusieurs plateformes de *trading* de crypto-monnaies telles que *Coinbase*[1010], *Bit Bay*[1011] ou encore *Binance*[1012], se sont intéressées aux systèmes d'identification des utilisateurs et des souscripteurs. Elles ont ainsi procédé à une vérification des identités de leurs utilisateurs et requièrent désormais, pour toute nouvelle inscription, de fournir une photo d'identité, ainsi qu'une pièce d'identité en prenant en photo la carte d'identité nationale mentionnant le numéro de carte, le permis de conduire, ou éventuellement le passeport. *Bit Bay* demande, en plus, de vérifier le numéro de téléphone du souscripteur par l'envoi d'un code à usage unique par SMS, mais également de fournir un relevé bancaire et un document datant de moins de six mois confirmant l'adresse postale, tel qu'un document officiel, une facture (électricité, eau, téléphone, gaz, etc.), ou encore un

[1008] World Economic Forum, Deloitte (collab.), « Blueprint for Digital Identity », Industry Project of the Financial Services Community [online], Future of Financial Services Series, Aug. 2016, http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf.

[1009] Pour une définition du processus KYC, *supra* n° 8. – De nombreuses institutions financières s'engagent dans des procédures KYC en collectant des données et des informations basiques sur leurs clients et en utilisant idéalement la vérification d'identité électronique, à l'image d'un « programme d'identification du client ». Des informations telles que les noms, les numéros de sécurité sociale, les anniversaires et les adresses peuvent être très utiles pour déterminer si une personne est impliquée ou non dans un crime financier. Une fois ces données de base collectées, les banques le comparent généralement à des listes de personnes connues pour leur corruption, sur une liste de sanctions, soupçonnées d'être impliquées dans un crime ou à haut risque de corruption ou de blanchiment d'argent. Les institutions financières consultent également des listes de personnes politiquement exposées (listes PPE). Dès lors, l'établissement bancaire quantifie le degré de risque que son client présente et la probabilité qu'elle soit impliquée dans une activité corrompue ou illégale. Une fois ce calcul effectué, la banque peut donner un aperçu théorique de ce à quoi le compte de ce client devrait ressembler dans un avenir proche. Une fois que la trajectoire attendue du compte est en place, la banque peut alors surveiller en permanence l'activité du compte du client et s'assurer que rien ne semble être déplacé ou suspect. – V. également, ACPR, « Identification et connaissance de la clientèle (KYC) », *ACPR-Banque de France* [en ligne], 12 juin 2018, https://acpr.banque-france.fr/autoriser/fintech-et-innovation/nos-dossiers-thematiques/identification-et-connaissance-de-la-clientele-kyc.

[1010] V.., https://help.coinbase.com/, Products > Coinbase Help Center > Getting started > ID document verification.

[1011] V., https://bitbay.net/, Registre > Bitcoin & digital currencies > Beginner > Do I need to verify my account?

[1012] V., https://www.binance.com/, Home > Binance Terms of Use (II – General Provisions > 3. Binance Account Registration and Requirements > c. User Identity Verification).

contrat (banque, assurance) sur lequel figure le cachet de l'établissement et la signature d'un représentant[1013].

Directement issue d'une réflexion sur l'identification des utilisateurs au sein de l'écosystème *Bitcoin*[1014], la *blockchain Namecoin* peut quant à elle stocker des données dans sa propre base de données de transactions, ce qui lui permet d'associer des informations d'identité aux données de compte utilisées sur la chaîne[1015].

133. La création de services de crypto-identités *via blockchain*. Le procédé employé doit, selon l'art. 1366 du C. civ., être capable de « dûment identifi[er] la personne dont [un écrit électronique] émane », or cette fonctionnalité n'est évidemment pas intrinsèque au protocole de toute *blockchain* et les participants n'ont, malgré tout, pas toujours la volonté de quitter un environnement qu'ils considèrent comme protecteur eu égard au pseudonymat pratiqué. C'est pourquoi certaines *start-ups* ont conçu des mécanismes annexes de vérification et de gestion d'identités et de réputation numériques[1016], pour proposer, sur la base du volontariat, un système générant des crypto-identités directement sur le réseau d'une *blockchain*. À l'image d'un certificat de signature permettant de fournir instantanément les informations nécessaires à son identification, l'utilisateur disposerait d'une sorte de « carte d'identité *blockchain* » inaltérable – si ce n'est en cas de modifications des informations identifiantes – et éventuellement renouvelable, qu'il pourrait utiliser sur d'autres sites web. C'est sur ce support que s'est appuyé le projet *uPort*.

134. La création de services de crypto-identités *via blockchain* : l'exemple d'*uPort*, ou la solution d'une *self-sovereign identity*. Une identité numérique crée un lien entre un objet numérique et l'identité physique de son propriétaire, qui peut d'ailleurs être une personne, une entreprise, une association, ou n'importe quel objet[1017]. Contrairement au modèle actuel de gestion des différents fournisseurs d'identité sur le web[1018], le concept

[1013] V., https://bitbay.net/fr/helpdesk/beginner/do-i-need-to-verify-my-account, Registre > Bitcoin & digital currencies > Beginner > Do I need to verify my account?

[1014] Il s'agit en réalité d'un *fork* volontaire de la chaîne *Bitcoin* afin de permettre aux utilisateurs de choisir selon leurs préférences et besoins entre le pseudonymat de *Bitcoin* et l'identification de *Namecoin*. – Pour une définition détaillée du *fork*, *infra* n°s 321 et s.

[1015] V., https://namecoin.org/.

[1016] LORRE (Pierre-Marie), « Blockchain : évolution ou révolution pour les contrats en France ? », Courbevoie : Institut Léonard de Vinci [en ligne], 2016, p. 50, https://www.forumatena.org/files/livres blancs/LORE_BLOCKCHAIN_CONTRATS-FA.pdf.

[1017] DE VAUPLANE (Hubert), « Les applications de la blockchain en bref », *Les cahiers de l'innovation* [en ligne], 24 oct. 2016, https://www.lescahiersdelinnovation.com/2016/10/les-applications-de-la-blockchain-en-bref/.

[1018] IBM, « Rôles du fournisseur d'identité et du fournisseur de services », *ibm.com* [en ligne], https://www.ibm.com/support/knowledgecenter/fr/SSZSXU_6.2.1/com.ibm.tivoli.fim.doc_6.2.1/concept/

était de développer un processus capable de créer ce lien, de le sécuriser pour protéger la confidentialité des informations délivrées, et d'en donner accès aux autorités compétentes en cas de besoin, notamment dans le cas où il faudrait certifier l'identité d'un utilisateur *x* utilisant une adresse *y*[1019]. *uPort* crée un *smart contract* (« *proxy contract* ») sur *Ethereum* pour y déposer l'identité numérique de chaque utilisateur. En cas de perte ou de vol de la clé et des informations liées, le propriétaire peut librement remplacer et révoquer le *smart contract*. Cependant, l'avantage d'un réseau décentralisé est d'être en pratique beaucoup moins facile à pirater qu'un serveur centralisé contenant des millions d'identifiants, donc en principe beaucoup moins visé[1020].

En pratique, dès qu'un nouvel utilisateur se présente sur la plateforme, de manière automatisée *uPort* lui demande de remplir un formulaire renseignant sur son identité. Les informations fournies sont directement inscrites sur *Ethereum* au sein du *proxy contract*, qui transmet instantanément à l'utilisateur la séquence de la clé privée protégeant le *smart contract* qui permet désormais de l'authentifier. C'est le *hash* dudit *smart contract* qui permettra de certifier son identité lors de ses futures opérations. Les développements en cours prévoient de programmer un système de mise à jour automatique des informations d'identité stockées sur la *blockchain* dès que les attributs du propriétaire d'une identité sont modifiés. Ce processus permettrait, dans le cadre de *blockchains* contractuelles, par exemple, de créer des effets de droit continus *via* un processus personne-identité-preuve[1021]. *uPort* permet également de signer en privé des attestations à l'aide de la spécification « *JSON Web Token* » (JWT). Le principe est qu'en utilisant des JWT au lieu de sauvegarder des informations sur une *blockchain* publique, les informations privées de

---

federationproviderrolesSAML.html : « Le fournisseur d'identité est un partenaire de fédération qui garantit l'identité des utilisateurs. Le fournisseur d'identité authentifie un utilisateur et transmet un jeton d'authentification (c'est-à-dire les informations permettant de vérifier l'authenticité de l'utilisateur) au fournisseur de services. Le fournisseur d'identité authentifie directement l'utilisateur, par exemple en validant un nom d'utilisateur et un mot de passe, ou authentifie indirectement l'utilisateur, par exemple, en validant une assertion concernant l'identité de l'utilisateur, telle qu'elle est présentée par un fournisseur d'identité distinct. » – Par ailleurs, Jde Tychey (v., TYCHEY (Jde), « uPort ou la gestion de l'identité par la blockchain », *Ethereum France* [en ligne], 27 sept. 2016 (mis à jour : 30 mai 2017), https://www.ethereum-france.com/uport-ou-la-gestion-de-lidentite-par-la-blockchain/) fait remarquer que « cette situation empêche toute approche holiste et détériore l'expérience utilisateur par la répétition des demandes de login et mot de passe. La sécurité pâtit doublement de ces répétitions. D'une part, lorsque les utilisateurs refusent l'authentification centralisée, ils sont tentés de se servir du même mot de passe pour de nombreux comptes différents. D'autre part, les fournisseurs d'identité centralisés comme *Facebook* ou *Google* permettent certes de diminuer la charge de *login* et mot de passe, mais ils deviennent des cibles d'autant plus intéressantes ("*honeypots of data*") pour les *hackers*. Les attaques sont fréquentes, on peut citer pêle-mêle *Dropbox*, *LinkedIn*, *Yahoo*, … » et recommande d'ailleurs de « faire un tour sur le site *haveibeenpwned* pour vérifier si votre email n'a pas été compromis ».

[1019] LEGEAIS (Dominique), *op. cit.*, n° 17.

[1020] TYCHEY (Jde), « uPort ou la gestion de l'identité par la blockchain », art. cit.

[1021] Le protocole *uPort* n'a cessé de s'améliorer et d'évoluer. C'est pourquoi l'équipe d'*uPort* a retiré le livre blanc original du site web pour le remplacer par un document qu'ils nomment « *living and breathing* », une sorte de cahier des charges en ligne mis à jour en temps réel. – Pour plus de précisions, v., « uPort Protocol – Specs », uPort [en ligne], https://github.com/uport-project/specs.

l'utilisateur peuvent rester entièrement confidentielles. En parallèle, l'identification est rendue possible[1022] puisqu'*uPort* dispose, grâce à ce mécanisme, d'un système de vérification des identifiants intégré. Ainsi, lorsqu'un utilisateur reçoit un message signé, *uPort* vérifie automatiquement l'authenticité du JWT en le comparant à la clé publique de l'émetteur contenue dans le registre d'*uPort*[1023]. Cette dernière spécificité implique toutefois pour chaque utilisateur – potentiel cocontractant – de s'inscrire préalablement à toute « transaction » afin que le registre d'*uPort* puisse exécuter ses fonctions de base de données d'identification décentralisée.

Initialement, cette solution visait à stocker des informations d'identité sur une *blockchain* afin, d'une part, d'en contrôler l'utilisation par les tiers et, d'autre part, de les rendre utilisables lors de connexions à d'autres services ou applications, autrement dit pour permettre aux clients de remplir les divers formulaires des sites web en indiquant simplement le *hash* du *proxy contract* ou le JWT correspondant[1024]. Force est de constater qu'elle pourrait également servir sur toute *blockchain*, à l'instar de « *Onename* » applicable aux *blockchains Namecoin* et *Bitcoin*[1025] ou de « *BlockOne ID* » interagissant avec les *smart contracts* d'*Ethereum*[1026], comme un système d'identité déclarée – mais néanmoins pas forcément vérifiée.

D'autres *start-ups* se sont également intéressées aux systèmes d'identification par *blockchain,* diversifiant ainsi le panel d'offres de services dans le domaine.

135. La création de services de crypto-identités *via blockchain* : autres exemples de solutions existantes. Développant un système de « jetons » d'identités non-fongible (UNIK), la plateforme *Unik-Name* transforme des séquences d'informations multiples et complexes telles que des clés privées ou identifiants d'un *wallet* ou des données d'identité, en identifiants décentralisés (DID) ancrés sur la *blockchain uns.network*[1027].

[1022] Pour plus de précisions sur le sujet, v., uPort, « A Complete List of uPort's Protocols, Libraries and Solutions », *Medium* [online], 20 Jun. 2018, https://medium.com/uport/a-complete-list-of-uports-protocols-libraries-and-solutions-63e9b99b9fd6. – Portail développeur de *uPort*, disponible en ligne : https://developer.uport.me/attestcredentials/.

[1023] D'après le site *uPort*, « *To request information from your user you create a Selective Disclosure Request JWT and present it to your user in the web browser.* [...] *If you need to know the users address on a specific ethereum network, specify it's network_id (currently defaults to ropsten 0x3). In this case be aware that the address returned will be the address on the public network (currently ropsten) for the users profile. The requested network address will be in the networkAddress field and will be MNID encoded*. »

[1024] SOLANA (Albert), « Self-Sovereign Identity: 3, 2, 1, partez… », *Validated ID* [en ligne], https://www.validatedid.com/fr/self-sovereign-identity-3-2-1-partez/.

[1025] V., https://onename.com/ ; BOHIC (Clément), « On a testé Onename : une identité sur la blockchain », *ITespresso* [en ligne], 6 févr. 2016, https://www.itespresso.fr/test-onename-identite-blockchain-120763.html.

[1026] V., https://blockoneid.thomsonreuters.com/.

[1027] V., https://docs.uns.network/, Home > Introduction > Understanding uns.network.

Chaque DID est cryptographiquement sécurisé par des clés privées sous le contrôle exclusif du propriétaire[1028]. Il permet de s'authentifier sur n'importe quelle plateforme ou application tierce.

Issue des exigences légales en matière de KYC, la plateforme *Civic* associe les fonctionnalités d'*uPort* et des mécanismes d'identification des utilisateurs et souscripteurs de plateformes de *trading* de crypto-monnaies. Elle propose à ses clients de s'identifier à l'aide de documents officiels (carte d'identité nationale, permis, etc.) et de déposer, après vérification par les services de la plateforme, le *hash* de ces documents sur une *blockchain*[1029]. Une fois déposés, tous les documents transmis à la plateforme sont automatiquement supprimés des serveurs et seul leur *hash* est conservé[1030]. Ainsi, lorsqu'un utilisateur désire signer un document ou, à tout le moins, prouver son identité, il fournit à l'autre partie le document attestant de son identité que lui seul a conservé. L'autre partie peut alors immédiatement consulter la plateforme et s'assurer que le document est fiable et l'identité vérifiée[1031]. Il pourrait s'agir de procéder de la même manière en cas de litige. Il apparaît toutefois que le système de vérification d'identités de *Civic* met à contribution des participants volontaires, des tiers autrement dit, qui ont donc accès à des données personnelles et qui « peuvent changer de temps à autre à la seule et entière discrétion de Civic »[1032]. Or cette hypothèse n'est pas facilement concevable en France et dans l'UE[1033].

En Chine, le projet *THEKEY* tend à développer un outil d'identification autonome et décentralisé afin de créer, pour chaque identité réelle, une identité virtuelle. Le but est de permettre aux propriétaires de s'authentifier et de reprendre le contrôle sur leurs données tout au long de leur vie quotidienne sur Internet[1034]. Le projet repose sur l'utilisation d'un système d'identification dynamique multidimensionnelle basée sur la *blockchain* (*Blockchain based Dynamic Multi-Dimension Identification*), créé spécialement pour le projet[1035]. Le système a accès aux informations nominatives (*Personally Identifiable Information*, PII) provenant du *Big Data* national, de sorte qu'il peut vérifier en temps réel l'identité de chaque utilisateur par le biais d'une

[1028] V., https://docs.uns.network/, Home > Key concepts > Decentralized ID token.
[1029] V., https://www.civic.com/wallet/,
[1030] BOUZIDI (Djellil), FROSSART (Thibaud), MAINELLI (Michael), MATET (Simon), « L'identité numérique : un usage de la blockchain au profit du citoyen », *Terra Nova* [en ligne], 24 sept. 2018, p. 24, http://tnova.fr/system/contents/files/000/001/625/original/Terra-Nova_Note-Blockchain_240918.pdf?1537777511.
[1031] *Id.*
[1032] V., https://www.civic.com/wallet/, Home > Terms and Conditions of Use (How Civic Serves You).
[1033] BOUZIDI (Djellil), FROSSART (Thibaud), MAINELLI (Michael), MATET (Simon), préc., pp. 24-25.
[1034] V., https://www.thekey.vip/#/homePage.
[1035] *Id.*

reconnaissance faciale et/ou d'une comparaison d'empreintes digitales[1036]. Bien qu'éminemment intéressant, d'un point de vue juridique et éthique certaines finalités de ce système de vérification des identités, ainsi que d'autres pans du projet, ne seraient toutefois pas sans soulever nombre de difficultés s'il était question de le déployer en France ou en UE.

S'appuyant elle aussi sur des données externes, mais étant malgré tout plus respectueuse de la vie privée, la plateforme *AGEify* propose aux entreprises qui souhaitent, souvent pour des raisons légales, restreindre l'accès à leurs sites, de mettre en place un contrôle plus strict de l'âge des internautes[1037]. Pour procéder à des vérifications d'identité, la plateforme utilise des données provenant d'institutions affiliées telles que des banques, des compagnies d'assurances, des sociétés de télécommunications, qui ont déjà accès à des enregistrements d'âge vérifiés, et qu'elle stocke sur une *blockchain* dédiée[1038].

En 2018, un projet de *blockchain* se proposait de mettre en œuvre un système de vérification d'identités en lien avec les services de l'administration publique, qui permettrait aux utilisateurs d'inscrire un certain nombre d'informations les concernant au sein d'un *smart contract*[1039]. L'idée était de laisser aux seuls propriétaires, après vérification, les clés de chiffrement des *smart contracts* contenant leurs données pour qu'ils puissent ensuite réguler l'accès accordé à des tiers en fonction de leurs besoins[1040].

Alors que des services de crypto-identités fondés sur des *blockchains* continuent de se déployer[1041], les géants du web[1042] et les administrations publiques tendent, eux aussi, à développer leurs propres mécanismes. En 2018, le canton de Genève a notamment fait une demande d'étude auprès de la Direction Générale de la Sécurité Intérieure (DGSI) afin de développer au sein de ses services publics une identité numérique nationale (*swissID*) liée à un système de signature électronique (*eSignature*) fondés sur un protocole

---

[1036] THEKEY, « L'Identification dynamique multidimensionnelle reposant sur la chaîne de blocs (BDMI) amènera la troisième révolution de l'Internet », *CISSION PR Newswire* [en ligne], 26 oct. 2017, https://www.prnewswire.com/news-releases/lidentification-dynamique-multidimensionnelle-reposant-sur-la-chaine-de-blocs-bdmi-amenera-la-troisieme-revolution-de-linternet-653323593.html.

[1037] V., https://age-ify.com/, Home > Presentation.

[1038] *Id.*

[1039] BOUZIDI (Djellil), FROSSART (Thibaud), MAINELLI (Michael), MATET (Simon), préc., *loc. cit.*

[1040] *Id.*

[1041] V., par exemple, l'application *Peer Mountain*, similaire à *uPort* [https://www.peermountain.com/token-sale/], et bien encore. – V., MIRE (Sam), « Blockchain For Identity Management: 33 Startups To Watch In 2019 », *Disruptor Daily* [online], 8 Feb. 2019, https://www.disruptordaily.com/blockchain-startups-identity-management/.

[1042] V., par exemple, l'offre d' « identité décentralisée » de Microsoft [https://www.microsoft.com/fr/security/business/identity/own-your-identity?market=dz, Home > Identity > Own your identity ; DEBELLOIR (Marine), « Microsoft lance son service d'identité numérique décentralisée (DID) sur Bitcoin », *Cryptoast.fr* [en ligne], 11 juin 2020, https://cryptoast.fr/microsoft-did-identite-numerique-bitcoin/].

blockchain[1043]. Le Genève Lab envisage de réaliser une preuve de concept (*proof of concept*, POC) relative à un « Registre des plateformes de transactions avec signature électronique », qui proposerait d'authentifier n'importe quel utilisateur avant toute opération par le biais d'un *smart contract* déployé sur une *blockchain*[1044]. D'après les lignes directrices du projet, l'application d'*eSignature* devrait être en mesure de mettre à disposition de l'utilisateur un bi-clés d'identification *swissID* lui permettant de s'identifier. Pour interagir avec les applications des services de l'État, l'utilisateur devrait fournir son *swissID* ainsi qu'un *hash* de celui-ci, signé avec sa clé privée, pour recevoir en retour un « *token* d'identification temporaire » qui, en pratique, ferait le lien entre le *smart contract* déployé et l'identité de l'utilisateur. Pour vérifier l'identité d'un utilisateur, il s'agirait alors de comparer le *token* aux données du *swissID* signé.

136. L'adaptation de la technologie par la mise en place d'une collaboration entre chaînes. Ces solutions, à la fois plurielles et isolées, érigent finalement la *blockchain* en fournisseur d'identité[1045], voire pour certaines en autorité de certification des identités[1046]. Cette utilisation de la *blockchain* suggère qu'en alliant les systèmes entre eux, le protocole serait capable d'identifier ses utilisateurs – tout en laissant éventuellement une place au volontariat – et ainsi apparaître comme étant un dispositif de création de signature électronique valable devant les tribunaux. Une plateforme de signatures électroniques pourrait en ce sens déposer les informations nécessaires à la signature sur la *blockchain* principale et, en parallèle, consulter une autre *blockchain* sur laquelle les informations d'identification nécessaires auraient été inscrites. Cette dernière serait sollicitée en principe à deux reprises pour des vérifications, d'une part, en amont de la signature pour authentifier l'origine du message ou du document inscrit sur la chaîne et, d'autre part, en aval lors de la vérification de l'identité du signataire. Dans une telle hypothèse, et à condition que l'utilisation de tels mécanismes soit généralisée, la *blockchain* semble prête à créer son propre réseau de confiance fondé autour de mécanismes d'identification et de vérification d'identité, à l'instar des tiers de confiance du règlement « eIDAS »[1047].

[1043] Il s'agit de la demande n° 56104 concernant les multiples aspects de la problématique de la signature électronique (y compris *blockchain*). V., PIGNON (Vincent) (dir.), *Compte-rendu de projet : Preuve de concept blockchain appliquée au registre du commerce République et canton de Genève*, Direction générale des systèmes d'information [en ligne], Département de la sécurité et de l'économie, n° 2559, 1er janv. 2018, p. 16, https://www.ge.ch/document/rapport-experimentation-blockchain/telecharger.
[1044] *Ibid.*, p. 33.
[1045] TYCHEY (Jde), art. cit.
[1046] Règl. (UE) n° 910/2014, préc., art. 7.
[1047] Règl. (UE) n° 910/2014, préc., art. 21.

De plus, le contrôle certifiant l'identité d'un signataire et pouvant d'ailleurs mener à la délivrance d'un moyen d'identification électronique[1048], tel qu'un CSE, peut désormais être opéré à distance et non plus obligatoirement en « face-à-face » si tant est qu'il soit capable de fournir « une garantie équivalente en termes de fiabilité à la présence en personne »[1049]. Le règlement laisse les États membres libres, en coopération avec les organismes d'évaluation de la conformité[1050], de juger de la fiabilité des méthodes d'identification à distance et « équivalentes au face-à-face ». Myriam Quéméner propose ainsi l'utilisation, notamment lors de l'inscription de l'utilisateur ou lors de sa demande de certificat, de procédés basés sur la comparaison entre une image prise par le support informatique de l'utilisateur et celle apposée sur un titre officiel tel que la carte nationale d'identité. Elle précise que ce contrôle doit être « associé à la vérification de l'intégrité [du] titre »[1051]. Par ailleurs, il apparaît que le règlement ne bannit pas l'utilisation des pseudonymes – chère à l'écosystème – puisqu'au contraire il la déclare explicitement valide sous réserve que son utilisation soit clairement indiquée à la partie utilisatrice au moment de la signature[1052] et que le signataire puisse être postérieurement identifié si nécessaire. À condition donc de respecter l'impératif de l'information du cocontractant et, en parallèle en ce qui concerne les plateformes, de prendre certaines précautions en recueillant des informations identifiantes sur ses utilisateurs, l'écosystème pourrait éventuellement poursuivre la pratique des pseudonymes.

Il existe donc, de manière plus ou moins isolée et plus ou moins autonome, des solutions d'identification qui peuvent faire évoluer le domaine de la signature électronique à deux niveaux. D'une part, elles pourraient aujourd'hui permettre la reconnaissance de la validité de la signature effectuée *via blockchain* au cours d'une instance. D'autre part, elles sont susceptibles, par le biais d'une collaboration entre chaînes, d'optimiser le dispositif et de permettre sa reconnaissance, à l'instar de ce que l'amendement n° 1317 au projet de loi relatif à la croissance et la transformation des entreprises, désormais loi nº 2019-486 du 22 mai 2019, dite « loi PACTE », proposait[1053]. La mission d'information commune sur les chaînes de blocs (*blockchains*) soulignait d'ailleurs que « conférer une valeur probante certaine aux informations inscrites au sein

[1048] *Ibid.*, art. 8, §3, b). Menant à l'inscription sur la « Trusted List » européenne établie par la Commission Européenne et réunissant l'intégralité des listes nationales des États membres. Le site officiel de la Commission met à disposition un moteur de recherche spécialisé, v., https://webgate.ec.europhttps://webgate.ec.europa.eu/tl-browser/#/a.eu/tl-browser/#/.
[1049] *Ibid.*, art. 24, §1, d).
[1050] *Id*.
[1051] QUEMENER (Myriam), *op. cit.*, p. 208.
[1052] Règl. (UE) n° 910/2014, préc., art. 32, §1, 2).
[1053] L. nº 2019-486, préc.

des *blockchains* constitue une nécessité pour l'essor de la technologie » et, comme d'autres auteurs[1054], qu'il conviendra pour cela de modifier le règlement eIDAS[1055].

Mais, la mise en place d'un dispositif permettant la mise en œuvre de processus de vérification contraignants signifie-t-elle que la technologie pourrait, à terme, remplacer les tiers de confiance ?

137. La *blockchain*, prochain PSCo décentralisé ? Depuis 2014, les dispositifs qualifiés de création de signature électronique peuvent également assurer à distance, *via* un *cloud*, par exemple, ou éventuellement une *blockchain*, le pan gestion du bi-clés pour le compte de l'utilisateur. Cette faculté est soumise à certaines conditions.

Le dispositif en question doit, pour cela, être certifié et fourni par le prestataire de confiance. Dans l'hypothèse de l'utilisation d'un protocole décentralisé par une plateforme de signatures électroniques, le prestataire correspondrait donc à la *blockchain*[1056]. Il est également impératif que l'utilisateur puisse « utiliser [le dispositif] sous son contrôle exclusif », et que ce dispositif évoque un « niveau de confiance élevé »[1057], ce qui suppose *a fortiori* un niveau d'authentification tout aussi important lors du *login*, tant auprès de la plateforme de signature qu'auprès de l'autorité de certification des identités. En pratique, l'utilisateur n'est donc plus contraint de se connecter *via* un support informatique unique et peut utiliser une plateforme en ligne[1058], ou tout dispositif dont l'authentification nécessaire est considérée être effectuée « à distance ». Ces caractéristiques coïncident avec celles de la signature *via blockchain*, ce qui la rend admissible sous réserve de réunir les éléments constitutifs de la signature « qualifiée »[1059].

Toutefois, et malgré toutes les qualités vivement avancées par la communauté[1060], encore faut-il, pour qu'elle puisse exercer en tant que « prestataire de services de

---

[1054] MARRAUD DES GROTTES (Gaëlle), « DEEP : prochaine étape de régulation, la valeur légale de la preuve blockchain ? », *Wolters Kluwer* [en ligne], 2 sept. 2019, Wolters Kluwer France > Actualités Du Droit > Tech&Droit > Blockchain, https://www.actualitesdudroit.fr/browse/tech-droit/blockchain/23230/deep-prochaine-etape-de-regulation-la-valeur-legale-de-la-preuve-blockchain.

[1055] Rapp. AN n° 1501, préc., p. 88.

[1056] *Ibid*., Annexe II, §3. – V. également, POULLET (Yves), JACQUEMIN (Hervé), « Blockchain : une révolution pour le droit ? », *Journal des Tribunaux*, n° 6748, 10 nov. 2018, p. 812.

[1057] *Ibid.*, art. 26, c) et Annexe II, §1, d).

[1058] CAPRIOLI (Éric), « Signature électronique - Décret n° 2017-1416 du 28 sept. 2017 relatif à la présomption de fiabilité de la signature électronique », *Comm. com. électr*. 2017, n° 11, comm. 92.

[1059] POULLET (Yves), JACQUEMIN (Hervé), art. cit., *loc. cit.*

[1060] Au regard des exigences communautaires, v., Règl. (UE) n° 910/2014, préc., Annexe II : « 1. Les dispositifs de création de signature électronique qualifiés garantissent au moins, par des moyens techniques et des procédures appropriés, que : a) la confidentialité des données de création de signature électronique utilisées pour créer la signature électronique est suffisamment assurée ; b) les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être pratiquement établies qu'une seule fois ; c) l'on peut avoir l'assurance suffisante que les données de création de signature électronique utilisées pour créer la signature électronique ne peuvent être trouvées par déduction et que la signature électronique est protégée de manière fiable contre toute falsification par les moyens techniques

confiance » (PSCo) et même « prestataire de services de confiance qualifié », que la technologie *blockchain* soit identifiée comme tel. Elle doit donc non seulement obtenir la reconnaissance de son statut de PSCo et de la conformité des services qu'elle fournit par les organismes d'évaluation de la conformité désignés par l'État français ainsi que par l'ANSSI[1061], mais également être en mesure de délivrer des certificats conformes à l'art. 32 du règlement (UE) 910/2014. Bien que le référentiel d'exigences applicables aux moyens d'identification électronique soit actuellement en cours d'élaboration, l'ANSSI, en coopération avec la CNIL, a élaboré une série de cahiers des charges relevant les attentes du rapport d'évaluation de la conformité applicables aux prestataires de services de confiance qualifiés et aux services de confiance qualifiés qu'ils rendent[1062]. Force est de constater à la lecture de ce document qu'à partir du moment où un système de signature électronique respecte l'ensemble des préconisations de ce cahier, la certification doit, en principe, lui être accordée. D'ailleurs, l'ANSSI mentionne expressément que la conformité à certaines normes, par exemple, la norme [EN_ 319_401][1063] et les compléments précisés dans le Chapitre II du cahier des charges en ce qui concerne les PSCo qualifiés[1064], emporte présomption de conformité aux exigences fixées par le règlement et par les décrets précités. Ainsi, dans le but de rendre le procédé *blockchain* « *compliant* », c'est-à-dire compatible avec les obligations conventionnelles, et ainsi augmenter ses chances d'être reconnu fiable voire peut-être d'être qualifié « conforme […] aux exigences de l'article 29 dudit règlement, [et reposant] sur un certificat qualifié de signature électronique répondant aux exigences de l'article 28 »[1065], il pourrait s'agir de la rendre conforme aux normes et certifications ETSI et ISO actuellement admises en la matière[1066]. Pour cela, il semble primordial d'envisager, au même titre que pour

actuellement disponibles ; d) les données de création de signature électronique utilisées pour créer la signature électronique peuvent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres. »

[1061] Règl. (UE) n° 910/2014, préc., art. 30 et 31, §1.

[1062] V. le site officiel de l'ANSSI > Documents publiés par l'ANSSI [https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-reglement-eidas/documents-publies-par-lanssi/]. Il s'agit, par exemple, d'exigences portant sur les « dispositifs de création de signature / cachet électronique qualifiés v.1 » [https://www.ssi.gouv.fr/uploads/2017/01/eidas-certificationconformiteqscd_v1.0_anssi.pdf] ; les « prestataires de services de confiance qualifiés » [https://www.ssi.gouv.fr/uploads/2017/01/eidas_psc-qualifies_v1.2_anssi.pdf].

[1063] NF EN 319401, Z85-401, [en ligne], oct. 2018, https://www.boutique.afnor.org/norme/nf-en-319401/signatures-electroniques-et-infrastructures-esi-exigences-de-politique-generale-des-prestataires-de-service-de-confiance-v221/article/905012/fa192090.

[1064] « Prestataires de services de confiance qualifiés : Critères d'évaluation de la conformité au règlement eIDAS », ANSSI, version 1.2, 5 juill. 2017, Chapitre II.2, p. 6 et Chapitre II.3, p. 7.

[1065] Décr. n° 2017-1416, préc., art. 1er.

[1066] Il s'agit, par exemple, des normes et certifications publiées respectivement par l'Institut luxembourgeois de la normalisation de l'accréditation, de la sécurité et qualité des services (ILNAS) et l'Organisation Internationale de Normalisation (ISO) ; ETSI EN 319 411-1 V1.1.1 à EN 319 412-4 V1.1.1, « Electronic Signatures and Infrastructures (ESI) », ETSI, févr. 2016 [https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.01.01_60/en_31941101v010101p.pdf] ; ISO/IEC 27001:2013, Catalogue 35.030

certaines suites logicielles de signature électronique classiques, la mise en place d'audits de performance et de sécurité.

Cependant, il reste un principe que la *blockchain* ne pourra, semble-t-il, pas honorer sans soulever certaines difficultés. Il s'agit du principe de la responsabilité du tiers de confiance – et les obligations qui lui sont attachées – en matière de signature électronique non qualifiée[1067] et qualifiée[1068]. Bien qu'il soit envisageable de prévoir des limites expresses à cette responsabilité[1069], elle représente malgré tout un poids qui ne pourra évidemment pas être porté par une *blockchain*[1070].

138. Bien qu'il ne soit pas certain que la qualité de « signature électronique qualifiée » lui soit reconnue sans modification des dispositions légales applicables en la matière[1071], la possibilité pour la technologie de démontrer sa fiabilité technique et d'être admise au cours d'un litige constitue une avancée majeure. Les tiers de confiance – principalement les autorités d'enregistrement, de certification, de création de signature, de vérification – ne sont ainsi pas absolument nécessaires puisque la *blockchain* est capable de fournir les mêmes services seule, de manière automatisée. Il sera simplement important pour les contractants d'élire le degré de sécurité de signature en fonction du domaine d'application et du but escompté et ce, en effectuant notamment des analyses des risques tant technologiques que juridiques. D'ailleurs, il apparaît d'une manière générale, qu'en raison d'une complexité accrue et d'un coût de fonctionnement souvent jugé trop élevé, la signature électronique « qualifiée » est, en réalité, rarement utilisée[1072], ou n'est simplement pas techniquement disponible[1073]. Finalement, si la technologie *blockchain*

« Sécurité des technologies de l'information », ISO, oct. 2013 [https://www.iso.org/fr/standard/54534.html].

[1067] V., POULLET (Yves), JACQUEMIN (Hervé), art. cit., *loc. cit*. S'agissant des PSCo (non qualifiés), les obligations concernent notamment les questions relatives aux traitements de données à caractère personnel (Règl. (UE) n° 910/2014, préc., art. 5 ; pour une étude détaillée de la législation sur les données à caractère personnel analysée sous le prisme du fonctionnement des protocoles des *blockchains*, *infra* n^{os} 184 et s.), à l'accessibilité aux personnes handicapées (même texte, art. 15) et à la sécurité (même texte, art. 19).

[1068] Règl. (UE) n° 910/2014, préc., art. 13, §1.

[1069] *Ibid.*, art. 13, §2.

[1070] En effet, la plupart des applications et des logiciels actuellement sur le marché sont couverts par un contrat d'assurance responsabilité civile professionnelle souscrit par l'entreprise gestionnaire et sont par ailleurs dotés d'un capital propre à l'entreprise les mettant en œuvre [v., « Certificate Policy and Public Certificate Practice Statement », préc., pp. 59-62].

[1071] Rapp. AN n° 1501, préc., p. 88 ; MIS (Jean-Michel), « Les technologies de rupture à l'aune du droit », *D. IP/IT* 2019, n° 7-8, p. 425 ; MARRAUD DES GROTTES (Gaëlle), « DEEP : prochaine étape de régulation, la valeur légale de la preuve blockchain ? », art. cit.

[1072] NETTER (Emmanuel), *Numérique et grandes notions de droit privé*, éd. CEPRISCA, coll. Essais, 2019, n° 280.

[1073] Forum Fintech ACPR-AMF, « Pôle Fintech-Innovation : publication du rapport du groupe de travail sur la vérification d'identité à distance des personnes physiques », ACPR [en ligne], 20 sept. 2019, p. 1,

n'entend remplacer ni les procédés de signature électronique ni les PSCOs existants, elle dévoile une alliance de performances et de sécurité capable de se positionner en tant que concurrente directe à ceux-ci. L'union de l'entreprise DocuSign avec l'Enterprise Ethereum Alliance dans le but de moderniser ses pratiques en fournissant des solutions reposant sur la *blockchain* témoigne de cette prise de conscience[1074]. Un autre indicateur repose dans le projet *Self-Sovereign Identity* (SSI) de la Commission européenne visant à redonner aux utilisateurs du web le contrôle de leurs propres données[1075]. Dans sa démarche de réédification de la confiance sur Internet, la Commission européenne envisage de s'appuyer sur la technologie *blockchain* pour créer une identité décentralisée et sécurisée[1076].

Ainsi, si les évolutions attendues de la *blockchain* suggèrent qu'elle soit capable, à l'avenir, de se conformer aux exigences probatoires attachées aux signatures électroniques, la question de sa reconnaissance en tant que mode de preuve à part entière soulève de multiples divergences selon la qualité du contrat considéré.

https://acpr.banque-france.fr/sites/default/files/medias/documents/20190919_synthese_verification_identite_distance_personnes_physiques.pdf.

[1074] V. le *tweet* officiel du *leader* mondial, https://twitter.com/DocuSign/status/1051208724184993794?ref_src=twsrc%5Etfw. – V. également, « DocuSign intègre la preuve de signature numérique sur Ethereum », *Journal du Coin* [en ligne], 15 oct. 2018, https://journalducoin.com/blockchain/docusign-preuve-signature-numerique-blockchain-ethereum/.

[1075] V. notamment le site officiel du projet, https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about ; DOMINGO (Ignacio Alamillo), « SSI eIDAS Legal Report How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market », joinup [online], Apr. 2020, https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI-eIDAS-legal-report-final-0.pdf.

[1076] *Ibid.*, pp. 12 et s. ; AGOSTI (Pascal), « Identité numérique, eIDAS et blockchain...Vers un nouveau paradigme centré sur l'utilisateur », *L'Usine Digitale* [en ligne], 26 mai 2020, https://www.usine-digitale.fr/article/identite-numerique-eidas-et-blockchain-vers-un-nouveau-paradigme-centre-sur-l-utilisateur.N968186.

Chapitre 2. Une variété de preuve algorithmique naissante

139. Conformément à l'art. 1363 du C. civ., « nul ne peut se constituer de titre à soi-même ». Exception directe à la règle, l'article suivant dispose qu'en matière de preuve d'actes juridiques, le juge admet que les parties se préconstituent une preuve de leur accord sous la forme d'un écrit, spécialement dressé dans l'optique d'apporter la preuve de l'opération[1077]. L'article précise qu'il peut prendre la forme d'un acte authentique ou d'un acte sous signature privée, en revanche sa force probante demeure assujettie à la condition « qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité »[1078].

Bien qu'elle ne présente pas la même structure que les moyens de stockage en ligne traditionnels, à l'instar d'un *cloud* par exemple, la technologie des blocs sous sa forme de registre décentralisé évoque une prochaine évolution des pratiques juridiques actuelles, ce qui pourrait en particulier intéresser les parties auxquelles la charge de la preuve incombe. La *blockchain* dispose de capacités de nature à sécuriser et à garantir l'intégrité des informations qu'elle contient, si bien qu'elle apparaît, sur certains points, plus performante et elle constitue en cela une innovation probatoire dans les relations synallagmatiques entre personnes privées (Section 1). Toutefois, il s'avèrera qu'en matière d'actes authentiques, l'évolution technologique n'est pas formellement synonyme de substitution, mais plutôt d'optimisation (Section 2).

Section 1. Une innovation probatoire dans les relations synallagmatiques entre personnes privées

140. D'après l'adage latin « *idem est non esse et non probari* », autrement dit « avoir un droit sans le prouver revient à ne pas avoir de droit ». Ainsi, si le processus d'inscription sur la chaîne de blocs a dévoilé un fort potentiel en matière

[1077] Une auteure précise que « pour les faits, le droit français reconnaît le principe de la liberté de la preuve. La règle est plus subtile s'agissant de la preuve des actes : à moins qu'ils soient de faible valeur, la preuve des actes se fait par écrit et doit répondre à un certain nombre de conditions strictes ». Sur l'histoire et les caractères des règles de preuve, v., MAGNIER (Véronique), « Enjeux de la blockchain en matière de propriété intellectuelle et articulation avec les principes généraux de la preuve », *D. IP/IT* 2019, n° 2, pp. 76-77.

[1078] C. civ., art. 1366.

d'authentification, il se révèle tout aussi prometteur à deux égards. D'une part, il peut contribuer à la sécurisation des relations entre les parties *via* une nouvelle forme d'archivage décentralisé (§ 1) et, d'autre part, il s'avère en mesure d'assurer l'opposabilité de toute inscription – de document, d'acte ou de constat d'un fait – sur la chaîne vis-à-vis des tiers *via* un registre de preuve instantané et infaillible (§ 2). Toutefois, il apparaît que la conception originelle que le droit probatoire a de la conservation intègre de documents est quelque peu différente puisqu'en termes de *blockchain*, un moyen de stockage sécurisé de l'intégralité du document n'est plus indispensable pour constituer une preuve de son intégrité. En effet, seule son inscription sur la chaîne suffit. L'unique condition étant, non plus de garantir l'intégrité du document, mais sa pérennité et son accessibilité. Force sera donc de reconnaître que l'essor de la *blockchain* est presqu'essentiellement associé à son admission par le système juridique, et donc conditionné par le facteur de confiance.

§ 1. Entre les parties, la sécurisation des relations *via* une nouvelle forme d'archivage décentralisé

141. Une fois que l'expéditeur a émis la « transaction » au profit de son cocontractant, c'est-à-dire une fois qu'il l'a signée grâce aux techniques de hachage utilisées par le protocole d'une *blockchain*[1079], ladite transaction n'est pas inscrite instantanément sur la chaîne puisque s'ensuivent quatre étapes, aussi cruciales que complexes, au cours desquelles vont intervenir les nœuds-mineurs du système *blockchain*. Ce mécanisme permet en pratique de sécuriser et de rendre inaltérable le document inscrit, et finalement de créer une preuve d'intégrité de celui-ci (A). Mêlé aux principes de décentralisation et de distribution, ce mécanisme de hachage contribue à renforcer les caractères infalsifiable et immuable qui caractérisent la chaîne de blocs. Cela permet, en matière d'actes sous signature privée, d'assurer par un nouveau dispositif probatoire rapide et sécurisé, non pas l'archivage à proprement dit d'un document, mais la conservation de la preuve inaltérable et inviolable de son intégrité (B).

A. Un mécanisme de création de preuve d'intégrité

142. L'inscription d'une transaction, ou comment le protocole fige définitivement les obligations auxquelles chaque partie a consenti. Lorsqu'une « transaction » *blockchain* –

[1079] Sur les techniques de hachage, *supra* n°s 103-105.

contrat accepté par deux utilisateurs de la chaîne[1080] – est initiée, celle-ci est d'abord transmise aux nœuds du réseau pour vérification individuelle, puis localement hachée et placée dans un bloc aux côtés d'autres transactions[1081]. Le premier nœud réussissant à valider sa version de bloc est considéré comme étant vainqueur, et transmet aux autres mineurs son bloc pour que les transactions y figurant soient définitivement validées par tous et finalement scellées à la suite du dernier bloc inscrit.

143. Première étape : vérification des transactions. Chaque transaction *blockchain* est placée dès sa création avec d'autres transactions au sein d'une liste d'attente que l'écosystème appelle le *memory pool*[1082]. La vitesse de propagation n'est pas la même pour toutes les transactions *blockchain*, par conséquent l'ordre d'apparition des transactions dans les listes détenues par les nœuds est différent d'un mineur à un autre. La phase de création d'un bloc sera également impactée par cette règle. À partir de leurs *memory pools* respectifs, les nœuds opèrent sur la transaction renfermant l'acte conclu entre les parties une vérification isolée.

La phase spécifique de vérification d'une transaction comporte trois étapes. La première est primordiale puisqu'elle sert à confirmer l'identité des parties et l'intégrité du contenu de la transaction en recherchant le lien entre les deux adresses-utilisateur et la demande de transaction[1083]. La deuxième, dont la finalité est davantage financière, vise à vérifier que l'émetteur possède suffisamment de cryptoactifs pour effectuer la transaction. Autrement dit, il s'agit de contrôler la solvabilité de l'émetteur. Ce processus est remplacé par la vérification de la possession d'un nombre suffisant de *gas*, qui correspond à une sorte de carburant permettant de payer les mineurs pour leur travail de vérification en ce qui concerne la validation de *smart contracts* sur *Ethereum*. Enfin la troisième étape, en prolongement de la deuxième, est à bien des égards la plus importante pour la chaîne puisqu'elle va permettre de s'assurer de l'intégrité du paiement, soit de l'absence de « double dépense ». Cette phase consiste à inspecter la « balance financière » de l'émetteur[1084], ce qui correspond techniquement à calculer le montant de la différence de toutes les entrées (*input*) et sorties (*output*) de transactions sur son ou ses adresses, pour

[1080] Sur la notion d'échange de consentement lors d'une transaction *via blockchain*, *supra* n° 101.
[1081] MARIN-DAGANNAUD (Gautier), « Comprendre la blockchain Ethereum – Article 1 : Bitcoin, première implémentation de la blockchain (2/2) », *Ethereum France* [en ligne], 30 mai 2017, https://www.ethereum-france.com/comprendre-la-blockchain-ethereum-article-1-bitcoin-premiere-imple mentation-de-la-blockchain-22/.
[1082] V., Annexe n° 8. Schéma de validation de blocs sur *blockchain* : l'exemple de *Bitcoin*, p. 440.
[1083] DELAHAYE (Jean-Paul), *Mathématiques et mystères*, éd. Belin, coll. Pour la science, 2016, pp. 45-46.
[1084] GUILHAUDIS (Élise), « Comprendre la blockchain à travers l'étude d'un cas pratique : le covoiturage "Blockcar" », *RLDI* 2017/12, nº 143, p. 3.

s'assurer que l'émetteur dispose véritablement des fonds qu'il veut dépenser[1085]. Il s'agit au fil de ces différentes étapes de s'assurer finalement de la sincérité du contenu de l'acte inscrit sur la chaîne avant de le sécuriser définitivement. D'ailleurs, cette vérification s'opère à grande échelle puisque chaque nœud, appartenant à un réseau inaltérable puisqu'entièrement décentralisé, inspecte le contenu de chaque transaction avant de la valider.

144. Deuxième étape : regroupement des transactions. Une fois ces étapes passées, les nœuds regroupent les transactions qu'ils ont respectivement vérifiées et forment leur propre version de bloc. Cependant, aussi longtemps qu'un certain travail n'a pas été effectué sur le bloc, ce dernier ne peut être définitivement scellé à la *blockchain*[1086].

145. Troisième étape : hachages et calculs d'empreintes infalsifiables. Plusieurs méthodes de prise en compte de ce travail existent, il en va ainsi de la preuve de travail (*Proof of Work*, PoW), de la preuve de participation (*Proof of Stake*, PoS), ou encore du consensus fédéré. En règle générale, la méthode la plus utilisée correspond à celle du *mining* (« minage »)[1087]. Équivalente à la preuve de travail, elle consiste en la résolution d'un problème de mathématiques[1088]. Toutefois, une étape préalable – sorte de préparation au travail – est nécessaire et recoupe deux techniques[1089], à savoir, la fonction de hachage, et l'arbre de Merkle[1090].

En pratique, le dispositif de l'arbre de Merkle est un préalable à la résolution du problème de mathématiques précité puisqu'il fournit un élément essentiel au calcul de celui-ci. Un bloc est composé de deux éléments comprenant un en-tête ou *Header*, ainsi qu'une liste de transactions, le *Body*. L'intégrité du contenu du *Body* va ainsi être assurée par la méthode du *Merkle Tree*[1091]. Cette méthode permet à la fois de structurer et de

---

[1085] V., Annexe n° 9. Traduction d'une chaîne de transactions sur *blockchain* : l'exemple de *Bitcoin*, p. 441. – MARIN-DAGANNAUD (Gautier), « Comprendre la blockchain Ethereum – Article 1 : Bitcoin, première implémentation de la blockchain (2/2) », art. cit. : « Il est important de ne pas confondre la chaine de bloc et la chaine de transaction […]. Chaque transaction contenue dans un bloc référence en entrée une ou plusieurs transactions ayant été incluses dans des blocs précédents, formant une chaîne de transaction dont les branches sont multiples. »

[1086] *Id.*

[1087] BERBAIN (Côme), « La blockchain : concept, technologies, acteurs et usages », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 8.

[1088] *Supra* n° 95.

[1089] FLORI (Jean-Pierre), « Sécurité et insécurité de la blockchain et des smart contracts », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 98.

[1090] Du nom de son inventeur, Ralph Merkle.

[1091] DE QUENETAIN (Stanislas), « L'arbre de Merkle : la Colonne Vertébrale de la Blockchain », *Blockchains Experts* [en ligne], 2015, https://www.blockchains-expert.com/larbre-de-merkle-colonne-vertebrale-de-blockchain/.

vérifier plus rapidement l'intégrité des données dans un environnement P2P. Schématiquement, il est possible de visualiser un arbre renversé – sinon une pyramide – avec l'optique qu'à la fin de l'opération, un élément unique se trouve seul suspendu en haut. L'arbre de Merkle forme une première ligne de groupes de deux transactions (« feuilles »), et calcule leur *hash* commun qui crée alors une nouvelle feuille au-dessus des deux autres. Puis, avec les nouvelles feuilles (*hashs*), il reforme à nouveau des groupes de deux, calcule leurs *hashs* qui forment des feuilles nouvelles. Et ainsi de suite jusqu'à n'obtenir plus qu'une seule feuille en haut de l'arbre inversé, désignée alors comme étant la « racine » de l'arbre ou *Merkle Root*, et inscrite dans le *Header* du bloc. Finalement, en plus du *hash* de la signature qui est vraiment *la* condition de forme essentielle de l'acte sous signature privée en ce sens qu'elle manifeste la volonté des parties de s'engager autant qu'elle est indispensable à la force probante de l'acte[1092], la *blockchain* met en œuvre une donnée qui a la capacité de figer à un instant *t* l'intégralité du contenu du bloc à enchaîner au reste de la chaîne. De cette manière, le protocole est capable de prouver la sincérité du *hash* de l'acte et, *a fortiori*, celle de l'acte[1093]. À travers ce procédé, toute contestation selon laquelle certaines mentions de l'acte auraient été, par exemple, ajoutées, modifiées ou supprimées, à l'insu d'une partie et postérieurement à la signature durant l'archivage, se révèle *ipso facto* un moyen inopérant puisque dès l'acte reconnu sincère, tant sa régularité matérielle que le respect de la volonté des parties sont supposés. Placée au cœur du dispositif mathématique de validation et préalable impératif à l'épreuve du *Proof of Work*, l'obtention de cette donnée se révèle être une preuve de sincérité supplémentaire aussi difficile à falsifier qu'à contester.

L'apport de la preuve de travail est, quant à elle, considérable en matière de sécurité puisqu'elle scelle définitivement l'acte entre les parties. Pour cela, chaque nœud est convié à résoudre un problème de mathématiques dont l'extrême complexité assure la sûreté du mécanisme. Il consiste pour chaque nœud à trouver le *hash* du *Header* du bloc[1094], qui est constitué de six éléments[1095], à savoir, la version du bloc, l'empreinte du bloc précédent, le *Merkle Root* précédemment calculé, la date, la difficulté et le *nonce*. En pratique, ce sont ces deux derniers éléments qui composent le problème à résoudre puisque chaque nœud doit calculer le *nonce* du *Header* en fonction de la difficulté fixée par le protocole. Pour que la preuve de travail soit valide, le *hash* du *Header* calculé contenant la valeur du *nonce* doit fournir un résultat inférieur à un nombre fixé par la

[1092] C. civ., art. 1367, al. 1er. – *Supra* n°s 94 et s.
[1093] C. civ., art. 1372.
[1094] BARRAUD (Boris), « Les blockchains et le droit », *RLDI* 2018/4, n° 147, p. 14.
[1095] V., Annexe n° 10. Schéma du contenu d'un bloc d'une *blockchain* : l'exemple de *Bitcoin* (blocs n°s 549 313 à 549 315), p. 442.

difficulté et nommé « seuil »[1096]. Autrement dit, le *hash* doit commencer par une série de « 0 »[1097] dont le nombre est fixé par la difficulté. Cependant, puisqu'à chaque nouveau bloc les quatre premiers éléments le constituant ne sont jamais les mêmes, il est impossible de prédire la valeur de ce *hash*. Or, c'est justement le rôle du *nonce* que de permettre au *hash* de se « transformer »[1098] et de prendre des valeurs différentes jusqu'à, selon sa valeur, obtenir une séquence respectant la difficulté fixée. Par conséquent, il est presqu'impossible de vraiment « calculer » le *hash*. La seule solution est de tester, une à une, différentes valeurs de *nonce* jusqu'à obtenir un *hash* répondant à cette difficulté[1099]. En pratique, chaque nœud y travaille isolément, en faisant appel à la puissance de calcul de ses processeurs, jusqu'à ce que l'un d'entre eux trouve une valeur correspondante.

146. Quatrième étape : ancrage définitif de la transaction et diffusion de la version de bloc validée. Le premier nœud qui trouve une valeur de *nonce* correcte peut, après confirmation des autres pairs à la majorité des 51 % d'entre eux[1100], sceller sa propre version du bloc sur la chaîne, et en parallèle être rétribué pour son travail. Il s'agit de la « validation par consensus », qui constitue une seconde vérification de la validité du bloc, mais cette fois effectuée conjointement par l'ensemble des mineurs[1101]. Le choix du consensus résulte de la volonté de mettre fin aux risques de « *double-spend attack* ». En

[1096] MARIN-DAGANNAUD (Gautier), « Comprendre la blockchain Ethereum – Article 1 : Bitcoin, première implémentation de la blockchain (2/2) », art. cit.
[1097] *Id.*
[1098] GUILHAUDIS (Élise), art. cit., pp. 3-4.
[1099] FLORI (Jean-Pierre), art. cit., p. 98 : « Le problème mathématique repose sur une fonction de hachage, à savoir une fonction qui prend une séquence de lettres et de chiffres x de longueur arbitraire, et en tire une autre y de longueur fixe. La propriété des fonctions de hachage est qu'il est relativement facile de calculer y à partir de x, mais impossible de retrouver x à partir de y, de même qu'il est difficile de factoriser un grand nombre, mais facile de vérifier qu'une factorisation est correcte. Le problème mathématique est alors le suivant : étant donné l'entête du bloc le plus récent x, il faut trouver un nombre n (dit valeur de circonstance) tel que le hachage y de la séquence (x, n) satisfasse une certaine condition : par exemple les vingt-cinq premiers caractères doivent être des zéros. Comme il n'est pas possible d'aller à l'envers et de calculer n, la seule méthode consiste à essayer des nombres n les uns après les autres, jusqu'à ce que l'on trouve un y qui réponde à la condition. » – VELDE (François R.), « Bitcoin pour remplacer les devises », *Rev. éco. fin*. 2015/4, n° 120, p. 105 : « Étant donné le hache H(Bi-1) du bloc précédent de la blockchain, ainsi que les données à intégrer au nouveau bloc Bi (une liste Li de transactions à valider dans le cadre de *bitcoin*), il s'agit essentiellement de trouver un préfixe Ni, tel que le nouveau bloc Bi=(Ni, H(Bi-1), Li) constitue de la concaténation de ces éléments satisfasse la condition que le hache H(Bi) commence par i bits nuls. ».
[1100] En pratique, cette vérification est plus simple et plus rapide car il suffit de faire le calcul inverse du *hash* en utilisant la valeur de *nonce* proposée par le nœud potentiellement vainqueur [ANTONOPOULOS (Andreas M.), *Mastering Bitcoin*, ed. O'Reilly, 2nd edition, 2017, p. 21 : « *Crucially, while it is very difficult and computing intensive to solve this task, it is very easy for all other users to verify that the solution is correct - as we will see below, an intuitive comparison is to a puzzle game which takes a lot of time and effort to assemble, but everyone can with just a look at it confirm if the result is correct* »]. – Pour plus de précisions techniques sur le sujet, v., MARIN-DAGANNAUD (Gautier), « Comprendre la blockchain Ethereum – Article 1 : Bitcoin, première implémentation de la blockchain (2/2) », art. cit. ; DE QUENETAIN (Stanislas), « 4 étapes pour comprendre une transaction bitcoin », *Blockchains Experts* [en ligne], 2017, https://www.blockchains-expert.com/4-etapes-pour-comprendre-une-transaction-bitcoin/.
[1101] LEGEAIS (Dominique), « Blockchain », *JCl. Sociétés Traité*, fasc. 2160, n° 8.

effet, un système sans consensus serait beaucoup trop facile à manipuler car un simple changement de date/heure par un utilisateur malveillant pourrait tromper le réseau entier et falsifier les données y figurant[1102]. Cette dernière étape accomplie, la mise à jour de la chaîne peut et doit intervenir sur l'ensemble des versions du registre détenues par chaque nœud du réseau.

B. Un dispositif de conservation de preuve d'intégrité

147. Les avantages d'un système en réseau P2P décentralisé. L'innovation technologique représentée par la *blockchain* découle non seulement de l'exploitation d'un réseau distribué et décentralisé, source de son immuabilité, mais également d'une combinaison de processus de sécurisation cryptologique efficaces. La difficulté, le travail effectué et l'incitation par rétribution constituent autant d'invitations à œuvrer pour le réseau plutôt que contre. Contrôlée par personne mais vérifiée par tous, la *blockchain* constitue une base de données en principe inaltérable et inviolable[1103], offrant, par le biais de la technique, une sécurité juridique plus importante[1104]. Le protocole est fondé sur un principe de consensus de sorte à donner à l'architecture de la chaîne une image de sûreté, prémices de tout sentiment de confiance. *A contrario*, cela induit qu'une intervention centralisée ou hiérarchique serait *de facto* sans objet. Finalement, la définition donnée d'un « grand livre comptable ouvert et infalsifiable, que chacun peut consulter, où l'on peut écrire sous le contrôle et à la vue de tous, mais qui ne peut pas être effacé »[1105] reflète parfaitement les caractéristiques essentielles de la technologie appliquée au domaine probatoire. Reprises de blocs en blocs, les données cryptées sur la *blockchain* scellent l'existence d'une preuve sécurisée de l'intégrité de l'acte liant les parties.

148. Un système de conservation de preuve différent de celui du coffre-fort numérique. Bien que la technologie soit capable de certifier tant de l'intégrité du contenu que de son origine, il s'agit de ne pas assimiler son fonctionnement à celui du « coffre-fort numérique » de l'art. L. 137 du CPCE, ni à celui du règlement eIDAS[1106]. En effet,

[1102] Pour plus de précisions sur l'importance d'un consensus dans un réseau distribué et décentralisé, v., MARIN-DAGANNAUD (Gautier), « Comprendre la blockchain Ethereum – Article 1 : Bitcoin, première implémentation de la blockchain (2/2) », art. cit.
[1103] THÉOCHARIDI (Eva), « La conclusion des smart contracts : révolution ou simple adaptation ? », *RLDA* 2018/6, n° 138.
[1104] COIFFARD (Didier), « Entretien du mois : La Blockchain a un sens pour répartir une partie de la confiance en rendant une information infalsifiable mais cette confiance est très en deçà de celle conférée par le notaire », *RLDC* 2017/4, n° 147.
[1105] COHEN-HADRIA (Yaël), « Blockchain : révolution ou évolution ? », *D. IP/IT* 2016, n° 11, p. 537.
[1106] Règl. (UE) n° 910/2014, préc.

la technologie *blockchain* est basée sur un protocole techniquement non-ouvert en ce qu'il a pour principe d'inscrire durablement l'objet de la « transaction » émise sur la chaîne sous forme de *hash*[1107], et non de stocker un document tel que le ferait un coffre-fort numérique[1108]. Ainsi, s'il s'agit d'inscrire l'accord final conclu à la suite d'une période de négociations, c'est le *hash* de l'acte qui fait véritablement l'objet d'une inscription, et non l'acte lui-même. Le processus probatoire traditionnel qui opère à partir de l'acte original pour ensuite apporter la preuve de l'authenticité de celui-ci est presque inversé pour laisser place à un nouveau processus laissant apprécier d'abord la preuve de l'intégrité et de l'existence de l'acte, avant celle du document qui en est le support. Par conséquent, il convient de se demander si la technologie de la chaîne de blocs n'est pas également capable de fournir un élément de preuve présentant « des garanties suffisantes d'authenticité, d'impartialité et de sincérité concernant tant sa date que son contenu », tel qu'avait précisé la Cour d'appel d'Aix-en-Provence en 1994 à propos de la licéité d'une preuve tirée d'un enregistrement vidéo[1109], d'autant plus qu'il s'agit de qualités spécifiques à la technologie.

149. Admissibilité de principe du support électronique et application au dispositif des *blockchains*. Depuis le 13 mars 2000[1110], le législateur a décidé de dissocier la preuve littérale de son support pour rendre son appréciation juridique pleinement indépendante de la suprématie des supports traditionnels papiers et des exigences d'écrits rédigés et signés « de [la] main » du signataire[1111]. Corolaire de l'introduction à l'échelle de l'UE de principes en faveur de la reconnaissance de la signature électronique, l'équivalence est donc prônée entre écrits en version papier et écrits en version électronique[1112]. Autrement dit, l'admissibilité de la preuve ne sera en principe pas atrophiée en raison d'une preuve numérique d'un contrat conclu *via blockchain* et ce, à partir du moment où les exigences

[1107] *Supra* n°s 132-134.
[1108] CPCE, art. L. 137, al. 1er, 1° et 5°. En effet, tant le 1° que le 5° du 1er al. de l'art. L. 137 du CPCE se révèlent techniquement en rupture avec la technologie *blockchain.* Tandis que le 1° évoque « le stockage, la suppression et la transmission de données ou documents électroniques », le 5° prévoit « de donner la possibilité à l'utilisateur de récupérer les documents et les données stockées dans un standard ouvert aisément réutilisable et exploitable par un système de traitement automatisé de données, sauf dans le cas des documents initialement déposés dans un format non ouvert ou non aisément réutilisable qui peuvent être restitués dans leur format d'origine ».
[1109] CA Aix-en-Provence, 4 janv. 1994, « Perez c/ Beli Intermarché (SA) », JurisData n° 600578, *JCP* 1995. II. 22514, n. Colonna J.
[1110] L. n° 2000-230, 13 mars 2000, portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, *JORF* n° 62, 14 mars 2000, p. 3968, texte n° 1.
[1111] C. civ., art. 1326 (ancien).
[1112] MASON (Stephen), *L'utilisation des preuves électroniques dans les procédures civiles et administratives et son impact sur les règles et modes de preuves. Étude comparative et analyse, rapport préparé par Stephen Mason, avec le concours de Uwe Rasmussen*, Strasbourg, 27 juill. 2016, CDCJ(2015)14-final [en ligne], p. 36, https://rm.coe.int/16807007ca.

en matière de conservation ont été respectées[1113]. Hormis, d'une part, l'existence d'une étude, à la demande du Conseil de l'Europe, concernant l'impact de la preuve électronique sur les règles et modes de preuve en vigueur dans toute l'UE[1114], qui a, d'autre part, mené le Comité des Ministres du Conseil de l'Europe à ériger une liste de 35 lignes directrices à l'attention des États membres et de leurs instances juridictionnelles sur les preuves électroniques dans les procédures civiles et administratives, les exigences en matière d'archivage électronique en UE ne sont pas uniformes et relèvent de la législation nationale de chaque État[1115].

En vertu des exigences françaises en la matière, la preuve ainsi stockée *via blockchain* doit être « établi[e] et conservé[e] de façon à garantir son intégrité »[1116]. Si la technologie en garde du *hash* de l'acte semble répondre à ces exigences, en parallèle il s'avère qu'il appartienne désormais au contractant de veiller à stocker l'acte lui-même en lieu sûr de sorte à préserver tant sa pérennité que son accessibilité. Érigée en 2018, la norme NF Z42-013 de l'AFNOR, désormais ISO 14641-1[1117], a vocation à guider les professionnels dans la compréhension et le respect des exigences de pérennité, de sécurité et d'intégrité concernant les documents électroniques archivés. Investie d'une large portée, cette norme s'applique, par exemple, à une entreprise ou à un organisme qui souhaite mettre en œuvre des systèmes d'archivage électroniques (SAE), à un éditeur de SAE, ou encore à un tiers archiveur souhaitant assurer un service d'archivage *via* SAE. Les spécifications de la norme ISO 14641-1 impliquent que, dans le cadre d'une action judiciaire, les parties soient disposées à apporter la preuve de la vérité dont l'acte est porteur, d'autant plus qu'en cas de conflit de preuves, le juge détermine par tous moyens le titre le plus vraisemblable[1118]. Toutefois, il apparaît qu'aucune indication de procédure – que ce soit civile ou administrative – n'est susceptible de guider les parties ou les tribunaux quant à la saisie des preuves électroniques, et *a fortiori* des preuves conservées par une *blockchain*. Il convient donc de réaliser un état des lieux du régime juridique de l'archivage électronique à la lumière des spécificités de la technologie.

[1113] C. civ., art. 1365 et 1366 ; MASON (Stephen), RASMUSSEN (Uwe), préc., pp. 28, 36 ; Lignes directrices du Comité des Ministres du Conseil de l'Europe n° CM(2018)169-add1final, 30 janv. 2019, sur les preuves électroniques dans les procédures civiles et administratives, n°s 6-9, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902dc9.

[1114] MASON (Stephen), RASMUSSEN (Uwe), préc.

[1115] DELAHAYE (Philippe), « eIDAS bouscule les codes en matière d'archivage électronique », *archimag.com* [en ligne], 23 janv. 2017, https://www.archimag.com/archives-patrimoine/2017/01/23/eidas-cdc-arkhineo-signature-confiance-tribune.

[1116] C. civ., art. 1366.

[1117] ISO 14641:2018, « Archivage électronique – Conception et exploitation d'un système informatique pour la conservation intègre de documents électroniques », juin 2018.

[1118] C. civ., art. 1368.

150. Typologie des méthodes d'archivage pouvant être mises en œuvre par une *blockchain*. Basé sur un objectif de précaution probatoire voulant que les parties puissent être en mesure de faire valoir leurs droits en cas de litige, l'archivage électronique représente pour son utilisateur, qu'il s'agisse d'une entreprise, d'un avocat[1119], ou bien encore d'un particulier, la « conservation de la mémoire de son entreprise »[1120]. Seulement, face à la dématérialisation, il convient bien souvent de se demander comment reprendre possession d'un document numérique qui, dans le cas d'une conservation sur *blockchain*, a été transformé en un *hash* de chiffres et de lettres, tout en garantissant l'intégrité et la fiabilité du procédé de conservation comme du document. Partant de là, deux situations peuvent se présenter. Elles consistent, d'une part, à numériser la preuve puis à l'inscrire sur une *blockchain* et, d'autre part, à créer *ab initio* cette preuve lors de l'inscription sur la chaîne.

En ce qui concerne tout d'abord les éléments de preuve dématérialisés, il s'agit pour les parties à un acte juridique de contracter selon les engagements consentis et de signer, puis de constituer une preuve de l'accord qui les lie en numérisant celui-ci et en l'inscrivant au sein d'une transaction *blockchain*. En d'autres termes, l'inscription de la preuve fait office de copie numérisée de l'original papier. Elle n'est toutefois admissible à titre de preuve au cours d'une action judiciaire qu'à la condition de correspondre à « la reproduction non seulement fidèle mais durable » de l'original papier (C. civ., art. 1348, al. 2). L'acte ne doit subir aucune modification au cours de la numérisation ; son contenu doit demeurer intègre[1121] et la copie doit être fiable. Le législateur, renvoyant à un décret en Conseil d'État, énumère une série d'exigences au sein de l'art. 1379 du C. civ. qui permettent de conférer une présomption de fiabilité probatoire à la copie produite. Ainsi, est présumée fiable toute « reproduction à l'identique de la forme et du contenu de l'acte, et dont l'intégrité est garantie dans le temps »[1122] « en cas de reproduction par voie électronique, [par] un procédé qui répond aux conditions prévues aux articles 2 à 6 du présent décret »[1123].

Or, la technologie *blockchain* semble capable de répondre à ces exigences. *Primo*, en inscrivant le *hash* de l'écrit sur la chaîne, il est techniquement possible d'ajouter des données contextuelles de quelques caractères à l'inscription concernant la reproduction

[1119] V., par exemple, « La blockchain : l'outil du futur au service des avocats », *Dossiers d'actualité LexisNexis*, 1er mars 2021.
[1120] FÉRAL-SCHUHL (Christiane), *CyberDroit : Le droit à l'épreuve de l'Internet*, éd. Dalloz, coll. Praxis Dalloz, 8e édition, 2020, p. 1178.
[1121] *Ibid.*, pp. 1142, 1159, 1178.
[1122] C. civ., art. 1379, al. 2.
[1123] Décr. n° 2016-1673, 5 déc. 2016, relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil, *JORF* n° 0283, 6 déc. 2016, texte n° 61, art. 1.

par voie électronique[1124], permettant à la fois d'identifier et de dater la copie[1125]. Il est également possible, *deuxio*, grâce à ce *hash*, de produire la preuve d'intégrité résultant d'une « empreinte électronique » – cryptographique dans le cas de la *blockchain* – et d'apporter la preuve que la copie est produite par un dispositif sécurisé[1126]. En effet, quel que soit le choix du mode de stockage du document électronique à l'origine du *hash*, il est impossible qu'une modification survienne, que ce soit sur la *blockchain* puisqu'elle constitue un registre perpétuel et inaltérable de l'ensemble des transactions inscrites dans ses blocs, ou au sein du document puisqu'un simple changement dans la ponctuation ou même une modification du format de l'acte serait immédiatement repérable[1127]. Par conséquent, le *hash* prouve naturellement que la copie de l'acte est conservée dans des conditions « garantissant l'absence d'altération »[1128]. Il pourra être intéressant, pour répondre à la condition de contrôle de la qualité du procédé de copie du second al. de l'art. 2 du décret précité, de solliciter, en vertu de l'art. 143 du CPC, l'expertise d'un huissier ou d'un expert. À défaut, la fiabilité de la copie est laissée à l'appréciation du juge qui pourra de lui-même requérir une expertise pouvant certifier de la fiabilité du procédé *blockchain*[1129].

Par ailleurs, si la preuve n'est pas numérisée mais est créée *ab initio* lors de l'inscription sur la chaîne, cela signifie que l'acte juridique est conclu électroniquement, qu'il est transmis à signature *via blockchain* et donc que la signature se trouve sur la chaîne. Toutefois, conformément à l'art. 1366 du C. civ., l'écrit électronique doit « dûment identifi[er] la personne dont il émane et établi[r] et [être] conservé dans des conditions de nature à en garantir l'intégrité ». Les exigences d'intégrité et d'identification dérivent sur un autre impératif, à savoir que l'acte archivé doit représenter la traduction exacte de la volonté des contractants[1130]. De ces constatations ressort le lien inextricable entre l'acte conservé et sa signature qui le perfectionne. Corolaire de l'acte, la signature numérique obtenue *via blockchain* et ledit acte devraient alors être conservés de manière indivisible, de sorte que les stocker séparément apparaît de prime abord dénué de sens[1131].

[1124] *Supra* n° 122, le message joint peut contenir jusqu'à 80 octets de caractères.
[1125] *Ibid*., art. 2.
[1126] *Ibid*., art. 6.
[1127] *Supra* n° 100.
[1128] *Ibid*., art. 4.
[1129] Lignes directrices du Comité des Ministres du Conseil de l'Europe n° CM(2018)169-add1final, préc., n° 18. – Depuis 2010, l'AFNOR a par ailleurs publié une norme dont l'objet est d'éclairer les huissiers de justice quant à la méthode à utiliser pour leurs expertises d'un système électronique. V. en ce sens, AFNOR, NF Z67-147 « Mode opératoire de procès-verbal de constat sur internet effectué par Huissier de justice », 1er sept. 2010. – V. également, CA Paris, 1ère Ch., 27 février 2013, *RLDI* 2013/92, n° 3058. Dans cet arrêt les juges d'appel ont écarté les griefs portant exclusivement sur la non-conformité à la norme NF Z67-147 pour effectuer un examen autonome et parvenir à une appréciation propre de l'expertise menée.
[1130] C. civ., art. 1367, al. 1er.
[1131] DELAHAYE (Philippe), art. cit.

Pourtant, bien que la conservation de l'acte semble directement liée à celle de sa signature électronique, la loi ne précise pas s'il est nécessaire, pour en garantir l'intégrité, qu'ils soient archivés ensemble ou, du moins, aucun indice propre à infirmer ce constat ne semble loger les dispositions légales actuelles. Au contraire, le second al. de l'art. 1367 du C. civ. sur la signature électronique paraît laisser la possibilité d'un détachement entre l'acte et sa signature électronique, pourvu que chacun d'eux présentent des garanties d'intégrité l'un envers l'autre ; l'art. précise que « [la signature électronique] consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache ».

Or, ces garanties mutuelles sont effectivement remplies par le procédé *blockchain* puisque, d'une part, la preuve de l'intégrité du document réside dans le *hash* inscrit sur la chaîne et ce dernier lui est indissociable, et, d'autre part, l'utilité du *hash* inscrit siège dans l'existence dudit document à l'origine de la « transaction » dont il garantit l'intégrité. Autrement dit, l'archivage électronique *via blockchain* n'est pas tant celui de l'acte mais bien davantage celui de sa preuve d'intégrité. Il s'agit de l'archivage sécurisé de son empreinte mais, pour autant, les deux sont indissociables. D'ailleurs, le procédé ainsi présenté de la *blockchain* rejoint des indications données par la loi type de la CNUDCI du 16 décembre 1996 qui préconise que la personne elle-même ou un intermédiaire dont les services ont été requis peuvent[1132], à défaut de conserver le document « sous la forme sous laquelle il a été créé, envoyé ou reçu », le conserver « sous une forme dont il peut être démontré qu'elle représente avec précision les informations créées, envoyées ou reçues »[1133]. La *blockchain* présente la sécurité et la fiabilité nécessaire pour répondre à ces exigences. En contrepartie, mais également dans l'optique de respecter l'obligation de lisibilité de la preuve électronique en rendant sa lecture possible[1134], chaque contractant devrait veiller tant à la sécurité qu'à la confidentialité de l'acte dont il disposerait après avoir inscrit son *hash* sur la chaîne[1135]. Une plateforme pourrait ainsi être reliée à une *blockchain* et mettre en place un service d'archivage intégré et sécurisé, qui gèrerait les risques de la conservation pour l'utilisateur-contractant, tel que le fait actuellement le tiers archiveur. Une telle configuration contribuerait à autonomiser l'utilisation de ces services pour les utilisateurs. L'AFNOR met d'ailleurs à disposition une certification qui permet aux utilisateurs d'un SAE de s'assurer et de

[1132] Nations Unies, « Loi type de la CNUDCI sur le commerce électronique », United Nations Publications [en ligne], 1999, art. 10, § 3, https://www.uncitral.org/pdf/french/texts/electcom/05-89451_Ebook.pdf.
[1133] *Ibid.*, art. 10, § 1, b).
[1134] C. civ., art. 1365.
[1135] CAPRIOLI (Éric A.), « Introduction au droit de la sécurité des systèmes d'information », *in Droit et technique - Études à la mémoire du Professeur Xavier Linant de Bellefonds*, éd. Litec, 2007, p. 75.

pouvoir, dès lors, assurer de leur conformité vis-à-vis des prescriptions légales actuelles[1136].

Finalement, à condition que des mesures de sécurité adéquates soient mises en place par les contractants, la formalité du double signé, qu'impose l'art. 1375 du C. civ. à raison de priver *l'instrumentum* de la force probante qui lui est attachée, semble facilitée par le procédé de la chaîne. En effet, celle-ci laisse perpétuellement apparente, et donc accessible à l'ensemble des utilisateurs, l'intégralité des signatures électroniques qu'elle contient. Autrement dit, elles sont accessibles aux contractants, mais aussi à toute autorité qui pourrait légalement en requérir l'accès[1137], sans possibilité de fraude et sans toutefois contrevenir à la confidentialité des données ou à l'intégrité des signatures en cause car le document lié demeure, quant à lui, non-apparent. Pour remplir l'exigence de la remise du double en elle-même, il semble qu'il suffirait aux contractants de s'échanger de manière sécurisée l'acte final sur le point de faire l'objet ou ayant fait l'objet d'une inscription sur la chaîne – qu'il s'agisse donc du contrat numérisé ou du contrat créé *ab initio* – à l'instar du dispositif mis en œuvre par *ContractChain*[1138]. Cela leur permettrait également de pouvoir restituer le document instantanément sur demande de l'administration fiscale, qui disposerait alors d'une preuve fiable et sécurisée de leur intégrité. Finalement, un tel SAE *via blockchain* pourrait être mis en place en interne dans les entreprises et autres organismes tel que dans les cabinets d'avocats[1139], ce qui leur permettrait, à moindre coût de stockage[1140] et avec des garanties supérieures de conservation intègre et durable[1141], de se placer sans difficulté, mais aussi et surtout sans l'aide d'un tiers, en conformité avec les exigences d'archivage et de durées légales de conservation[1142]. En poursuivant

---

[1136] AFNOR, NF 461 « Systèmes d'archivage électronique », juin 2012.

[1137] CGI, ann. II, art. 36, I.

[1138] V., https://www.contractchain.io/. D'après son fondateur, Christophe Carminati, « les différentes parties conservent leurs habitudes de travail, échangent des documents, négocient, modifient les points techniques et contractuels du projet » et, « au moment de rédiger le contrat, [les] clients authentifient les documents qui doivent y être inclus, créent une version numérique et la transmettent à leur cosignataire » [V., NICOLAS (Julie), « Signer vite et sans se tromper avec la blockchain », *Le Moniteur* [en ligne], 2 nov. 2018, https://www.lemoniteur.fr/article/signer-vite-et-sans-se-tromper-avec-la-blockchain.2001414].

[1139] Pour plus de précisions sur l'acte d'avocat électronique, v., FÉRAL-SCHUHL (Christiane), *op. cit.*, p. 1144 ; BABONNEAU (Marine), « L'acte d'avocat sera dématérialisé », *Dalloz actualité*, 23 juill. 2013.

[1140] *Supra* n° 108 sur les avantages de la signature *via blockchain* sur la signature électronique classique en matière de stockage et capacités de stockage.

[1141] CANTERO (Anne), CAPRIOLI (Eric A.), LE CERF (Xavier), « Commerce électronique », *Le Lamy droit des médias et de la communication*, n°468-107 ; MASON (Stephen), RASMUSSEN (Uwe), préc., p. 47.

[1142] À défaut de disposition contraire, les délais variant de cinq à trente ans de la L. n° 2008-561, 17 juin 2008, portant réforme de la prescription en matière civile, *JORF* n° 0141, 18 juin 2008, s'appliquent. En matière de factures de clients, la prescription en matière fiscale est de six ans en vertu de l'art. 96 F de l'annexe II du CGI et concerne la conservation de trois éléments, à savoir, la facture, la signature électronique et le certificat d'identification qui lui est attaché. La prescription en matière commerciale est de dix ans conformément à l'art. L. 123-22 du C. com. Par ailleurs, en ce qui concerne par exemple l'archivage des contrats électroniques conclus en B2C (*Business to Customer*), l'art. L. 213-1 du C. consom. impose au contractant professionnel de prendre la responsabilité de l'archivage pour un délai de deux ans « lorsque le contrat est conclu par voie électronique et qu'il porte sur une somme égale ou supérieure à [120

l'objectif de « doter l'Union européenne d'une cybersécurité solide »[1143], il semble même que la technologie pourrait contribuer au développement de l'outil eEDES d'échange de preuves numériques entre États membres, et ainsi soutenir le projet de l'Union consistant en la numérisation des systèmes judiciaires[1144].

151. Au-delà de pourvoir l'acte entre les parties d'une valeur juridique, il importe de le rendre opposable aux tiers. Or, les protocoles des *blockchains* et notamment celui de *Bitcoin*, imposent, au cours de la phase de création d'un bloc, que celui-ci inscrive de manière ordonnée et horodatée les opérations effectuées. En tant que registre de preuve instantané et infaillible, le protocole d'une *blockchain* pourrait être en mesure d'assurer cette opposabilité, tout en garantissant la bonne foi des conventions passées.

§ 2. Vis-à-vis des tiers, l'horodatage des conventions *via* la création de preuves d'antériorité

152. En quelques secondes, voire quelques minutes[1145], un nouveau bloc est ajouté à la chaîne, date et heure déterminées avec précision. Capable de certifier de l'intégrité d'un document, de confirmer ou d'infirmer l'identité de son propriétaire et finalement de lui conférer date et heure certaine, en plus d'un registre de conservation de preuve la *blockchain* est capable de fournir une véritable preuve d'antériorité. Non moins important au sein du dispositif probatoire, dans la pratique des *blockchains* l'horodatage contribue à renforcer la sécurité et l'inaltérabilité des données inscrites. Le potentiel de la technologie *blockchain* en la matière (A) contribue ainsi au développement de son mécanisme de création de preuve d'antériorité en matière d'actes juridiques (B), lequel a

---

euros] » (montant et délai fixé par le Décr. n° 2016-884, 29 juin 2016, relatif à la partie réglementaire du code de la consommation, *JORF* n° 0151, 30 juin 2016). – Sur le même sujet, v., TABAKA (Benoît), « L'archivage des contrats électroniques désormais opérationnels », *RLDI* 2005/3, nº 3 ; CAPRIOLI (Éric A.), « Vademecum juridique de la digitalisation des documents », Fédération des Tiers de Confiance [en ligne], 29 nov. 2016, pp. 28-32, https://fntc-numerique.com/upload/file/guides-fntc/Vademecum_Juridique.pdf. – Pour plus de précisions et d'exemples sur le sujet, v., *Ibid.*, pp. 34-54.

[1143] MAUBANT (Thierry), « UE : nouvelles mesures pour accélérer la numérisation des systèmes judiciaires et la formation des professionnels », *ActuIA* [en ligne], 3 déc. 2020, https://www.actuia.com/actualite/ue-nouvelles-mesures-pour-accelerer-la-numerisation-des-systemes-judiciaires-et-la-formation-des-professionnels/?u%E2%80%A6.

[1144] Conclusions n° 4435/17 du Secrétariat général du Conseil de l'Union Européenne, 20 nov. 2017, sur la communication conjointe au Parlement européen et au Conseil - Résilience, dissuasion et défense : doter l'Union européenne d'une cybersécurité solide.

[1145] Il est question, par exemple, de dix minutes pour *Bitcoin*, deux minutes et trente secondes pour *Litecoin*, et cinq secondes pour *Ethereum*. V. notamment, « Tutoriel complet pour miner sur la blockchain Ethereum – mai 2017 », *Ethereum France* [en ligne], 6 avr. 2018, https://www.ethereum-france.com/tutoriel-complet-pour-miner-sur-la-blockchain-ethereum-mai-2017/.

déjà été investi par un certain nombre de *start-ups*, notamment dans l'univers de la propriété intellectuelle.

A. Potentiel de l'horodatage blockchain

153. L'importance d'établir la date et l'heure d'un contrat. La pratique contractuelle révèle, elle-aussi, l'importance d'un horodatage fiable et précis. La précision dans la chronologie des évènements contractuels est primordiale en matière de prescription, de respect des délais, mais également dans des contentieux mettant en cause une créance, une acquisition ou une cession, par exemple[1146]. Bien qu'en principe la date ne soit pas exigée dans les relations découlant de contrats conclus sous signature privée[1147], dans de nombreux cas son absence se révèle, à terme, souvent préjudiciable, à tout le moins à l'une des parties. En témoignent Marcel Planiol et Georges Ripert qui constataient qu' « en fait la date est un élément indispensable et on ne manque jamais de l'insérer que par oubli ou maladresse »[1148]. Ainsi, au-delà des délais et prescriptions, la date est effectivement indispensable pour des questions d'antériorité, de capacité et, de manière générale, de régime applicable[1149].

Si l'heure ne bénéficie pas toujours de la même importance que la date aux yeux de la doctrine, il y a longtemps que pour certains auteurs la précision de l'heure prend toute sa dimension lorsqu'une pluralité d'actes sous signature privée ont acquis concomitamment date certaine[1150]. Dans ces diverses situations, l'objectif premier doit être d'éviter tant le risque de postdate que d'antidate, ainsi que l'évoque le Doyen Carbonnier[1151]. La fraude des parties consistant à détourner la vérité de la date ne doit pas pouvoir jouer contre les tiers, en d'autres termes ne doit pas les préjudicier[1152].

Par ailleurs, lorsqu'aucune date n'est mentionnée, la preuve de la date appartient à celui qui désire s'en prévaloir[1153]. Or, en pratique, cette preuve peut parfois se révéler

---

[1146] MEKKI (Mustapha), « Les mystères de la blockchain », *D*. 2017, n° 37, pp. 2160 et s., n° 14.
[1147] Hormis dans le cas du contrat de louage de choses, lequel n'est opposable à l'acquéreur de l'immeuble qu'à condition qu'il ait date certaine (C. civ., art. 1743). V., GUÉVEL (Didier), « Force probante de la date d'un acte sous seing(s) privé(s) : Date certaine », *JCl. Civil Code*, fasc. unique : Contrats et obligations, 2011 (actualisation : 2018), n° 1. – *A contrario*, son absence entraîne la nullité des actes notariés en vertu de l'art. 1370 du C. civ.
[1148] PLANIOL (Marcel), RIPERT (Georges), *Traité pratique de droit civil français*, éd. LGDJ, t. III, 1931, n° 1460, p. 796.
[1149] GUÉVEL (Didier), *op. cit.*, n° 2.
[1150] DEMOLOMBE (Charles), *Cours de Code Napoléon*, éd. Auguste Durand & Louis Hachette, vol. 29, t. VI, n° 502, 1876, pp. 426 et s.
[1151] CARBONNIER (Jean), *Droit civil*, t. II, éd. PUF, Coll. Thémis, 5e édition, 1967, n° 129.
[1152] TOULLIER (Charles Bonaventure Marie), *Le droit civil français suivant l'ordre du Code*, t. VIII, éd. Jules Renouard et Cie, 4e édition, 1824, n° 260, p. 394.
[1153] Cass. Civ. 1ère, 11 avr. 1964, *Bull. civ.* 1964, I, n° 180.

aussi difficile que préjudiciable[1154]. L'art. 1377 du C. civ. prévoit de rendre certaine la date d'un acte non-daté ou dont la date mentionnée est fausse au jour où ledit acte a été, et s'il l'a été, enregistré par un organisme tiers fiable ou constaté dans sa substance dans un acte dressé par un officier public, ou du jour de la mort d'un signataire. En parallèle, certaines règles particulières relativement éparses en matière d'opposabilité exigent des mesures supplémentaires de publicité, telles que, notamment, les art. L. 141-12 et s. du C. com. s'appliquant aux ventes de fonds de commerce[1155], l'art. R. 144-1 du C. com. relatif à la conclusion ou à la fin de contrats de location-gérance de fonds de commerce, l'art. L. 526-1 du C. com. relatif à la déclaration d'insaisissabilité de l'entrepreneur individuel, ou encore l'art. 1690 du C. civ. en ce qui concerne les cessions de créances. Ce constat mène à interroger l'aptitude de la technologie de la chaîne de blocs à simplifier et, éventuellement, à accélérer les processus de certification de la date nécessaires à ces différents actes, tout en assurant une sécurité suffisante aux informations qu'elle inscrit au sein de ses blocs.

D'une manière générale, anticiper se révèle donc indispensable, mais il est essentiel dans ce cas que la mention de la date et/ou de l'heure emporte la conviction du juge. Pour cela, le système d'horodatage doit être fiable.

154. L'efficacité de l'horodatage de la *blockchain*. L'horodatage de chaque transaction figure en clair sur la chaîne, à la date et à l'heure précises auxquelles le bloc la contenant a été définitivement validé et inscrit par les mineurs sur la chaîne et transféré sur le réseau. À l'instar des dispositifs de certification de contenu et de conservation de preuve d'intégrité, l'horodatage mis en œuvre ne peut ni être modifié, ni être supprimé. Immuable car ancré dans le protocole de la *blockchain*, le dispositif de contremarque de temps s'avère donc impénétrable. La technologie pourrait alors à la fois aider les parties à établir de manière certaine la date et l'heure auxquelles elles se sont obligées l'une envers l'autre, certifier ces informations vis-à-vis des tiers, et en contrepartie protéger ces derniers contre la mauvaise foi des parties et le risque de fausse date. En plus d'être potentiellement capable de prouver le lien existant entre un utilisateur et l'opération qu'il a initiée[1156], force est de constater que la technologie *blockchain* renferme donc un système de conservation lié à un mécanisme d'horodatage infaillible. Aussi robuste qu'un coffre-fort, elle semble autant capable de certifier du contenu que d'affirmer date et heure

[1154] GUÉVEL (Didier), *op. cit.*, n° 23.
[1155] Également, l'art. R. 144-1 du C. com. relatif à la conclusion ou à la fin de contrats de location-gérance de fonds de commerce.
[1156] *Supra* n°s 99-101.

certaines des données qu'elle enchaîne. Plus encore, la confidentialité n'est pas compromise car lors de l'enregistrement d'informations sur une *blockchain*, les seules informations disponibles publiquement sont le résultat de l'opération de hachage et l'horodatage. Il apparaît en ce sens indéniable qu'elle possède les qualités de registre de preuve d'antériorité de documents.

155. Vers une application en matière d'horodatage d'actes juridiques ? En 2016, le législateur français a conféré la même valeur que les écrits à des inscriptions financières de type minibons sur une *blockchain*[1157]. En 2019, il a décidé d'offrir aux *Initial Coin Offerings* (ICOs) un régime autonome intégré au Code monétaire et financier[1158]. En parallèle de cette reconnaissance graduelle du potentiel des inscriptions sur *blockchain*, divers acteurs expriment un besoin de confiance et requièrent pour cela une certaine traçabilité dans le déroulé de leurs activités[1159].

Par ailleurs, outre les questions concernant la qualité de contrat électronique et la valeur probante associée, la preuve d'un acte juridique peut être apportée par tous moyens (C. civ., art. 1358 et 1101) à condition qu'il n'excède pas 1 500 euros, autrement la rédaction d'un écrit est exigée[1160]. La preuve des obligations contractuelles est donc libre dans la limite du montant fixé, à l'instar de la preuve de faits juridiques[1161]. Il est donc malgré tout possible d'anticiper le contentieux et de se ménager des preuves. Bien que l'absence de reconnaissance légale de la *blockchain* comme mode de preuve soit susceptible de compliquer son admissibilité, la force probante des éléments de preuve produits dépend de leur capacité à être assimilés à des preuves électroniques ou du moins existantes[1162], et de la conviction du juge. La *blockchain* pourrait donc représenter un atout dans le domaine, qu'il s'agisse de prouver un acte juridique portant sur une somme, ou une valeur, excédant ou non 1 500 euros.

Certaines entreprises, en particulier du secteur industriel, commercial, culturel, de la recherche, et bien encore, ont d'ores et déjà pris la mesure du développement de la

[1157] Ord. n° 2016-520, préc., art.2. – BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 15.
[1158] L. nº 2019-486, préc., art. 85 et 88.
[1159] PEYRAT (Olivier), LEGENDRE (Jean-François), « Pourquoi la normalisation s'intéresse-t-elle à la blockchain ? », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 94.
[1160] C. civ., art. 1359.
[1161] Une auteure précise que « pour les faits, le droit français reconnaît le principe de la liberté de la preuve. La règle est plus subtile s'agissant de la preuve des actes : à moins qu'ils soient de faible valeur, la preuve des actes se fait par écrit et doit répondre à un certain nombre de conditions strictes ». Sur l'histoire et les caractères des règles de preuve, v., MAGNIER (Véronique), « Enjeux de la blockchain en matière de propriété intellectuelle et articulation avec les principes généraux de la preuve », art. cit., *loc. cit*.
[1162] MAGNIER (Véronique), « Enjeux de la blockchain en matière de propriété intellectuelle et articulation avec les principes généraux de la preuve », art. cit., p. 78.

technologie, et estiment que la fiabilité et l'intégrité de son horodatage est susceptible de renforcer leurs droits de propriété intellectuelle[1163].

156. L'impact de la preuve d'antériorité de la *blockchain* dans le renforcement des droits de propriété intellectuelle. Le triptyque des droits patrimoniaux des auteurs – à savoir, les droits de reproduction, de représentation, et de suite[1164] – a souvent été malmené ces dernières années[1165]. En lien avec l'arrivée imprévue d'Internet, prédécesseur de la *blockchain* dans le domaine du partage en réseau P2P, la diffusion d'œuvres notamment musicales est devenue incontrôlable et a, à terme, déstabilisé l'industrie culturelle[1166]. Pour autant, le législateur n'a jamais laissé impunis ces actes puisque la contrefaçon d'œuvres de l'esprit, qu'il s'agisse de musiques, de photographies, d'écrits, de vidéos, etc., est passible de trois ans d'emprisonnement et de 300 000 euros d'amende[1167], avec possibilité de prononcer des peines complémentaires spécifiquement prévues en matière de téléchargement illégal par la loi « HADOPI II » de 2009[1168]. De plus, protéger un droit d'auteur paraît *a priori* simple puisque le « seul fait de sa création » est propre à conférer « un droit de propriété incorporelle exclusif et opposable à tous »[1169]. Aucune formalité ni dépôt n'est en principe exigé car il s'agit d'une « protection automatique »[1170] qui découle d'ailleurs d'un principe fondamental historique reconnu par la Convention de Berne adoptée en 1886 et relative à la protection des œuvres et des droits des auteurs[1171]. Toutefois, la pratique révèle que, d'une manière générale, agir en justice contre un plagiaire ou un contrefacteur s'avère souvent laborieux au niveau probatoire.

[1163] NEUER (Laurence), « Créations : "La blockchain démocratise le recours à la preuve" », *Le Point* [en ligne], 8 janv. 2018, http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/creations-la-blockchain-democratise-le-recours-a-la-preuve-18-12-2017-2180835_56.php.
[1164] CPI, art. L. 122-2, L. 122-4.
[1165] Direction de l'information légale et administrative, « La protection des droits d'auteur », *Vie publique* [en ligne], 11 sept. 2012, https://www.vie-publique.fr/politiques-publiques/etat-internet/droits-auteur/.
[1166] OUSTRY (François), « Blockchain et Propriété Intellectuelle », *Medium* [en ligne], 4 avr. 2018, https://medium.com/@foustry/blockchain-et-propri%C3%A9t%C3%A9-intellectuelle-47dac0e2c59b.
[1167] CPI, art. L. 335-2.
[1168] L. n° 2009-1311, 28 oct. 2009, relative à la protection pénale de la propriété littéraire et artistique sur internet, *JORF* n° 0251, 29 octobre 2009, p. 18290. – V. également, CPI, art. L. 331-21-1, L. 335-2, L. 335-3, L. 335-4, L. 335-7, L. 335-7-1, et L. 335-7-2.
[1169] CPI, art. L. 111-1, al. 1er et 2.
[1170] DAHAN (Véronique), BARBET-MASSIN (Alice), « Les apports de la blockchain en matière de droit d'auteur », *August Debouzy* [en ligne], Technologies > Media > IP, 14 juin 2018, https://www.august-debouzy.com/en/blog/1190-les-apports-de-la-blockchain-en-matiere-de-droits-dauteur.
[1171] Conv. Berne, 9 sept. 1886 (modifiée le 28 sept. 1979), pour la protection des œuvres littéraires et artistiques, art. 5. 2. 5 : « La jouissance et l'exercice de ces droits ne sont subordonnés à aucune formalité ; cette jouissance et cet exercice sont indépendants de l'existence de la protection dans le pays d'origine de l'œuvre. »

En effet, cela implique d'être en mesure de prouver ses droits en cas de contentieux[1172], ce qui n'est, au surplus, pas chose aisée lorsque ce qui sépare le véritable auteur d'un contrefacteur repose sur un nom[1173] et une date[1174]. La preuve de l'antériorité d'une œuvre peut être apportée « par tous moyens »[1175], mais elle reste une preuve redoutable. Antériorité, authenticité et traçabilité sont les maîtres-mots de cette preuve[1176], et dater les œuvres est *de facto* devenu indispensable[1177]. Plusieurs moyens ont été mis en place pour faciliter une telle preuve, par exemple, l'enveloppe Soleau de l'INPI (Institut National de la Propriété Industrielle), les constatations d'huissier, le dépôt notarial ou effectué auprès d'une société d'auteurs. Un faisceau d'indices peut également être constitué. Cependant, préconstituer une telle preuve s'avère à la fois contraignant, et parfois même aléatoire[1178].

C'est dans ce contexte que la technologie de la chaîne de blocs peut se révéler être un atout probatoire. Pré-prouver l'antériorité des droits sur sa création peut se traduire en un dépôt simple et rapide du *hash* unique de son œuvre avec sa signature sur une *blockchain*[1179], et quel que soit son type – qu'il s'agisse d'une *blockchain* de crypto-actifs, de registre ou de *smart contracts*[1180]. Aussitôt, la propriété de l'œuvre se trouverait horodatée, sécurisée et scellée dans un registre public, décentralisé et immuable.

B. Perspectives de développement de la preuve d'antériorité

157. Admissibilité de la méthode d'horodatage de la *blockchain*. L'horodatage électronique fait lui aussi l'objet du règlement eIDAS[1181]. Il peut en outre être « qualifié » dans toute l'UE à condition qu'il repose sur une signature électronique avancée et qu'il satisfait aux exigences d'intégrité liant son contenu, la date et l'heure « de manière à

[1172] C. civ., art. 1353. – NCPC, art. 9.
[1173] Cass. Civ. 1ère, 15 janvier 2015, « Prada c/ SARL Cupidon », n° 13.22-798 (« [les auteurs] ne démontraient pas être titulaires [antérieur] des droits qu'ils invoquaient ; d'où il suit que le moyen ne peut être accueilli »).
[1174] CPI, art. L. 113-1 : « la qualité d'auteur appartient, sauf preuve contraire, à celui ou à ceux sous le nom de qui l'œuvre est divulguée ».
[1175] C. civ., art. 1358.
[1176] BAYLE (Aurélie) *et al.*, « Smart contracts : études de cas et réflexions juridiques », *ECAN* [en ligne], 19 sept. 2017, pp. 13-14, https://ecan.fr/Smart-Contracts-Etudes.pdf.
[1177] DAHAN (Véronique), BARBET-MASSIN (Alice), « Les apports de la blockchain en matière de droit d'auteur », art. cit.
[1178] *Id.*
[1179] *Supra* n°s 92 et s.
[1180] OUSTRY (François), art. cit.
[1181] Règl. (UE) n° 910/2014, préc., considérant n° 33, définit : « "horodatage électronique", [comme correspondant à] des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant ».

raisonnablement exclure la possibilité de modification indétectable des données »[1182]. Il peut également faire l'objet d'une convention de preuve consistant à anticiper la valeur probante de la preuve par *blockchain* si les parties l'utilisant ont décidé de faire confiance à la technologie. Mais il peut également, à l'instar de la signature électronique, être admis en justice en vertu du principe de non-discrimination entre les techniques d'horodatage électronique[1183]. Le considérant n° 62 du règlement eIDAS fait état de la prise de conscience du développement de l'innovation en la matière et envisage ainsi la possibilité pour les prestataires de services de demander la reconnaissance d'une nouvelle méthode d'horodatage électronique équivalente[1184].

158. L'anticipation des *start-ups* en propriété intellectuelle : exemples d'applications. Nombreuses *start-ups* proposent d'ores et déjà des services de préconstitution de preuves en propriété intellectuelle par le biais d'un protocole *blockchain*. Leur objectif est de pérenniser, et finalement de rendre aux auteurs leurs droits.

Il en va ainsi, par exemple, d'Ascribe[1185]. Mise en œuvre à destination des artistes et créateurs, la plateforme éponyme identifie le dépositaire, horodate, puis enregistre les œuvres sur une chaîne de blocs propre. *Bernstein*, quant à elle, intervient dans les milieux sociétaires[1186]. Elle fournit des certificats de preuve automatiquement horodatés à partir de l'enregistrement, sur *Bitcoin*, de l'empreinte cryptographique (*hash*) de secrets commerciaux et industriels, d'inventions[1187], de designs ou encore de preuves d'utilisation[1188]. L'application permet également aux entreprises de se préconstituer une preuve des contrats conclus par les gestionnaires dans leurs relations, par exemple, avec les employés, les partenaires, les clients, et les fournisseurs[1189]. L'avantage de l'utilisation d'une *blockchain* est de créer une preuve permanente des créations et de disposer d'un

[1182] Règl. (UE) n° 910/2014, préc., art. 42.
[1183] Règl. (UE) n° 910/2014, préc., art. 41, § 1 : « l'effet juridique et la recevabilité d'un horodatage électronique comme preuve en justice ne peuvent être refusés au seul motif que cet horodatage se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences de l'horodatage électronique qualifié ».
[1184] Certains suggèrent d'ailleurs qu' « il serait opportun aussi que l'Agence nationale de la sécurité des systèmes d'information (ANSSI) prenne position sur des bonnes pratiques à adopter permettant d'agréer les algorithmes de la *blockchain* et d'offrir une certaine sécurité juridique aux opérateurs quant au cadre applicable. De même, il pourrait être envisagé de mettre en place un système de labellisation des *blockchains* au même titre que celui de la Commission Nationale de l'Informatique et des Libertés (CNIL) en ce qui concerne la conformité des produits et procédures quant au traitement de données à caractère personnel » [v. notamment, DAHAN (Véronique), BARBET-MASSIN (Alice), « Les apports de la *blockchain* en matière de droit d'auteur », art. cit.].
[1185] https://www.ascribe.io/.
[1186] https://www.bernstein.io/, Home > Use cases.
[1187] *Ibid.*, Home > Use Cases > Trade secrets.
[1188] *Ibid.*, Home > Use Cases > Fashion and Design.
[1189] *Ibid.*, Home > Use Cases > NDA and contracts.

enregistrement incontestable du processus de conception valable en cas de litige[1190]. Fondée sur le même concept, *Binded* met également les qualités de la chaîne aux services du milieu de la photographie et en particulier aux systèmes de *copyrights* en fournissant des *copyrights certificates* comme preuve des droits admissible devant les tribunaux[1191].

En France, incubée au sein du cabinet d'avocats Deprez Guignot et Associés (DDG), la *start-up* BlockchainyourIp vise les créations des entreprises de tous secteurs confondus. Elle a pour objectif d'intégrer l'usage de la preuve par *blockchain* tant dans la vie des affaires que devant les tribunaux[1192] et a mené, pour cela, une collaboration avec un huissier de justice spécialisé dans le droit des technologies avancées[1193]. L'entreprise a ainsi établi les conditions d'établissement par huissier de justice d'un procès-verbal de constat d'une preuve d'antériorité en matière de propriété intellectuelle, préconstituée *via Bitcoin*, qui répondrait aux attentes des tribunaux et encouragerait ainsi leur admission[1194]. Elle propose désormais de fournir un certificat de preuve attestant de l'inscription sur la chaîne du *hash* de la création, indiquant la date de la création (horodatage), l'identité de son ou ses auteurs et ses caractéristiques[1195]. BlockchainyourIp prévoit par ailleurs, en cas de besoin, la possibilité d'une vérification *a posteriori* de la preuve *blockchain* par l'huissier afin d'attester la conformité de celle-ci devant les juges[1196]. Elle présente l'avantage de fournir aux créateurs une preuve à la fois rapide, efficace, peu onéreuse et accessible à tous. Alors que selon son cofondateur, « il ne reste plus qu'à attendre la première décision de justice qui constatera une création sur la base d'un certificat *blockchain* »[1197], fin 2017, a été portée devant les tribunaux français l' « affaire BlockchainyourIp »[1198]. Reste à savoir désormais si, en reconnaissant la

---

[1190] *Id.*

[1191] https://binded.com/. – D'autres existent, v., notamment, OUSTRY (François), « Blockchain et Propriété Intellectuelle », art. cit.

[1192] FAUCHOUX (William), « La startup qui voulait révolutionner la preuve des créations et des innovations », *BlockchainyourIp* [en ligne], 9 oct. 2017, https://blockchainyourip.com/startup-voulait-revolutionner-preuve-creations-innovations/.

[1193] « BlockchainyourIp veut révolutionner la preuve des créations et des innovations », *Le monde du Droit* [en ligne], 16 oct. 2017, https://www.lemondedudroit.fr/on-en-parle/54042-blockchainyourip-la-startup-qui-voulait-r%C3%A9volutionner-la-preuve-des-cr%C3%A9ations-et-des-innovations.html.

[1194] MARRAUD DES GROTTES (Gaëlle), « Vincent FAUCHOUX, co-fondateur de BlockchainyourIp : "En matière de propriété intellectuelle, la blockchain présente l'avantage de couvrir toute la zone de l'avant-brevet" », *Wolters Kluwer* [en ligne], 18 oct. 2017, https://www.actualitesdudroit.fr/browse/tech-droit/blockchain/9566/vincent-fauchoux-co-fondateur-de-blockchainyourip-en-matiere-de-propriete-intellectuelle-la-blockchain-presente-l-avantage-de-couvrir-toute-la-zone-de-l-avant-brevet, Wolters Kluwer France > Actualités Du Droit > Tech&Droit > Blockchain.

[1195] *Id.*

[1196] *Id*.

[1197] FAUCHOUX (William), art. cit.

[1198] DAHAN (Véronique), BARBET-MASSIN (Alice), « Le droit de la preuve en matière de propriété intellectuelle : quelle place pour la blockchain ? », *Marketing-Professionnels* [en ligne], 1er déc. 2017, http://www.marketing-professionnel.fr/tribune-libre/droit-preuve-propriete-intellectuelle-blockchain-2017 12.html.

validité de ce certificat, le juge établira la validité de la preuve par inscription dans les *blockchains* publiques d'empreintes cryptographiques horodatées de documents. La question se pose également pour les preuves d'antériorité des créations fournies par *Filecys.fr*, plateforme développée par la Chambre nationale des commissaires de justice[1199].

Basée sur les mêmes fondements, la *start-up* rennaise Woleet permet d'utiliser la *blockchain Bitcoin* pour sécuriser de multiples données, documents et signatures, des entreprises, leur conférer une force probante et leur permettre ainsi de mettre un terme à l'archivage papier[1200]. Elle propose ainsi de créer des « preuves universelles, inaltérables et horodatées »[1201], mais également peu coûteuses puisque *via* l'interface web « *Proofdesk* » de Woleet, le coût d'un fichier horodaté et stocké sur la *blockchain* est de 0,2 euros, contre 1,5 à 2 euros auprès d'un fournisseur d'archivage actuel[1202].

Partant du constat que l'utilisation de systèmes déclaratifs, à l'instar du dispositif d'enveloppe Soleau, reste un facteur de risque vis-à-vis des problématiques d'usurpation d'identité[1203], certains projets de *blockchains* envisagent de « lier un faisceau de preuve d'identité, de manière confidentielle, à une adresse *blockchain* »[1204], témoignant ainsi, à nouveau, de l'importance des solutions d'identification[1205].

159. Chine : l'utilisation de la *blockchain* comme mode de preuve. Le 28 juin 2018, la Chine a été l'un des premiers États à se positionner officiellement pour une reconnaissance de la validité de la preuve par *blockchain* à la suite d'une affaire concernant le droit de la propriété intellectuelle[1206]. En l'espèce, une plainte avait été

[1199] https://www.filecys.fr/.

[1200] MAGNIN (Olivier), « Des preuves universelles et inaltérables sur la blockchain Bitcoin », *Hub One* [en ligne], 1er août 2018, https://www.hubone.fr/oneblog/des-preuves-universelles-et-inalterables-sur-la-blockchain-bitcoin/?cn-reloaded=1.

[1201] *Id.*

[1202] *Id.*

[1203] LEGRAND (Stéphanie), « Enjeux de la blockchain du point de vue du praticien », *D. IP/IT* 2019, n° 2, p. 85.

[1204] V., par exemple, BERGÉ-LEFRANC (Clément), « La blockchain est une technologie très efficace pour se préconstituer une preuve », *RLDC* 2017/7, n° 150 ; MARRAUD DES GROTTES (Gaëlle), « Clément Bergé-Lefranc, co-fondateur de Ledgys Solutions : "La blockchain est une technologie très efficace pour se préconstituer une preuve" », *Wolters Kluwer* [en ligne], 20 juill. 2017, Actualités du droit > Tech& Droit > Blockchain, https://www.actualitesdudroit.fr/browse/tech-droit/blockchain/8244/clement-berge-lefranc-co-fondateur-de-ledgys-solutions-la-blockchain-est-une-technologie-tres-efficace-pour-se-preconstituer-une-preuve#:~:text=de%20preuves%20consid%C3%A9rable.-,La%20blockchain%20est%20une%20technologie%20tr%C3%A8s%20efficace%20pour%20se%20pr%C3%A9constituer,mais%20des%20milliers%20de%20personnes.

[1205] Sur la recherche de solutions permettant l'identification sécurisée des utilisateurs de *blockchain*, *supra* n°s 132 et s., notamment n°s 134-135.

[1206] VERDON (Antoine), « La justice chinoise reconnaît la blockchain comme moyen de preuve », *Le Temps* [en ligne], 6 juill. 2018, https://www.letemps.ch/economie/justice-chinoise-reconnait-blockchain-moyen-preuve.

déposée devant le Tribunal chinois spécialisé dans le domaine de l'Internet – le Tribunal de Hangzhou – par la société de médias locale Hangzhou Huatai Yimei Culture Media Co., Ltd. (« Huatai ») contre la société de technologie Shenzhen Daotong Technology Development Co., Ltd. (« Daotong ») pour violation du droit d'auteur et contrefaçon[1207]. Dans le but de se préserver la preuve de la violation commise *via* le site de la société Daotong, la société Huatai avait pris l'initiative de faire appel aux services de la plate-forme *Baoquan.com* qui permet de stocker les éléments de preuve sur les chaînes de blocs *FACTOM* et *Bitcoin*[1208]. Partant de là, il convenait de se demander si le Tribunal de Hangzhou allait admettre l'utilisation de données électroniques conservées par le bais de la technologie *blockchain* comme preuve dans un litige. La dernière modification de la loi de procédure civile de la République populaire de Chine autorisait, en tant que moyen de preuve, les données électroniques[1209]. Cependant, aucune précision n'y figurait concernant la donnée « blockchaînée ». La Cour a donc décidé d'examiner les preuves électroniques en utilisant une approche pratique, concluant que pour les données électroniques perpétuées et préservées par des systèmes de *blockchain* ou par des moyens techniques similaires, le tribunal devrait et devra par la suite adopter une attitude ouverte et neutre, et analyser puis décider au cas par cas[1210]. En outre, afin de déterminer si la méthode de préservation de la preuve de l'entreprise Huatai était conforme à la loi et subsidiairement de déterminer l'admissibilité et la valeur probante de la preuve électronique par *blockchain*, la Cour a examiné notamment trois éléments. Ella a tout d'abord pris en compte (1) la fiabilité de la plateforme de préservation de la preuve[1211] puis, (2) le caractère approprié des moyens techniques de collecte des données des pages

[1207] SONG (Ying), ZHAN (Hao), « Blockchain evidence accepted in judicial proceedings for first time », *International Law Office* [online], 23 Nov. 2018, https://www.internationallawoffice.com/Newsletters/Tech-Data-Telecoms-Media/China/AnJie-Law-Firm/Blockchain-evidence-accepted-in-judicial-proceedings-for-first-time.

[1208] Le plaignant a procédé par captures d'écran des sites web violés tout en enregistrant leur code source, puis il a téléchargé les données sur la plate-forme, créant ainsi un enregistrement immuable de la violation du droit d'auteur dont il a argué avoir été victime. V., TSO (Han-Mei), YI (Jude), « The First Case in China Using Blockchain Technology to Preserve Electronic Evidence », *Osha Liang* [online], 1st Aug. 2018, https://oshaliang.com/newsletter/the-first-case-in-china-using-blockchain-technology-to-preserve-electronic-evidence/.

[1209] L. de procédure civile de la République populaire de Chine (modifiée par la Déc. du 31 août 2012 portant modification du code de procédure civile de la République populaire de Chine), (trad. de : 中华人民共和国民事诉讼法（于2012年8月31日根据《关于修改〈中华人民共和国民事诉讼法〉的决定》修正), art. 63. Disponible en ligne (version avec outil de traduction automatique) : https://www.wipo.int/wipolex/fr/text.jsp?file_id=296344.

[1210] TSO (Han-Mei), YI (Jude), art. cit.

[1211] Interprétation judiciaire de la Cour populaire suprême de Chine (CPS), relative à l'audition d'affaires par les tribunaux Internet nouvellement créés dans le pays (trad. de : 最高人民法院关于互联网法院审理案件若干问题的规定), 7 sept. 2018, art. 11, 1). Disponible en ligne [version en chinois] : http://www.court.gov.cn/zixun-xiangqing-116981.html.

web contrefaisantes en tant que preuve[1212], et (3) la crédibilité de la méthode utilisée afin de conserver mais également de transmettre un contenu et un horodatage clair, objectif et précis[1213]. Compte tenu des diverses réponses apportées à ces examens[1214], la Cour en a conclu que les tribunaux Internet chinois devraient admettre les données numériques présentées comme éléments de preuve à deux conditions. D'une part, il est essentiel que les parties concernées les aient collectées et stockées *via* une *blockchain* munie d'un système de signatures numériques, d'horodatages fiables et de vérification des valeurs de hachage, ou bien *via* une plateforme de dépôt numérique présentant les mêmes caractéristiques. D'autre part, il est nécessaire que les parties puissent prouver l'authenticité de la technologie utilisée[1215]. Finalement, par sa décision, la Cour a prescrit un dispositif complet et précis d'analyse du processus électronique présenté en tant que preuve, dispositif qui pourrait éventuellement inspirer d'autres tribunaux internationaux en la matière.

160. Vers une reconnaissance juridique officielle ? La mise en œuvre de la *blockchain* en matière d'archivage et de preuve d'antériorité pour lutter contre les contrefaçons et autres infractions propres au domaine culturel témoigne de son potentiel, à la fois dans ce secteur mais également, d'une manière générale, dans le secteur de la preuve libre voire de la preuve légale. Aux États-Unis, certains États ont légiféré sur la question dès 2015 et ce, afin de donner un cadre juridique aux *smart contracts* et à la preuve *via blockchains.* Il s'agit des « *Blockchain friendly Bill* », adoptées par,

[1212] *Ibid.*, art. 11, 3).
[1213] *Ibid.*, art. 11, 2, 4, 5, 6.
[1214] Pour une analyse détaillée des motifs de la Cour, v., TSO (Han-Mei), YI (Jude), art. cit.
[1215] RAMA, « Blockchain Records get status of Legal Evidence as per China's Supreme Court Ruling », *Market Mongers* [online], 14 Sept. 2018, https://marketmongers.com/blockchain-records-get-status-of-legal-evidence-as-per-chinas-supreme-court-ruling/. – V. également, ZHANG (Laney), « Global Legal Monitor », *The Law Library of Congress* [online], 14 Sept. 2018, http://www.loc.gov/law/foreign-news/article/china-supreme-court-issues-rules-on-internet-courts-allowing-for-blockchain-evidence/.

notamment[1216], les États du Vermont[1217], de l'Ohio[1218], d'Arizona[1219], du Tennessee[1220], et du Nevada[1221]. L'État du Nevada par exemple, bien qu'ambigu sur certains points[1222], a amendé l'*Uniform Electronic Transactions Act*[1223] pour inclure une définition de la *blockchain* mettant en exergue ses capacités en matière d'archivage[1224]. L'État du Vermont a, quant à lui, créé des présomptions légales réfutables d'authenticité pour les enregistrements utilisant la technologie *blockchain*[1225]. Dans ces États, la *blockchain* et les *smart contracts* peuvent, en principe, être utilisés en tant que documents juridiques ou documents de preuve horodatés d'un droit de propriété, ou en tant que systèmes de conservation sûrs des données en cas de contentieux. Reste à savoir si les juges américains recevront la preuve par *blockchain*. L'État italien a, pour sa part, juridiquement consacré l'horodatage *blockchain* par l'art. 8 ter, 3º, de la loi relative au soutien et à la simplification des entreprises et de l'administration publique[1226]. La Principauté de

[1216] MORTON (Heather), « Blockchain State Legislation », *National Conference of State Legislatures* [online], 28 Mar. 2019, http://www.ncsl.org/research/financial-services-and-commerce/the-fundamentals-of-risk-management-and-insurance-viewed-through-the-lens-of-emerging-technology-webinar.aspx.

[1217] Vermont Act No. 157 (H.868), An act relating to miscellaneous economic development provisions, 2 Feb. 2016. Disponible en ligne : https://legislature.vermont.gov/Documents/2016/Docs/ACTS/ACT157/ACT157%20As%20Enacted.pdf.

[1218] Senate Bill 300, 23 May 2018, Revise Electronic Transactions Act/blockchain/smart contracts. Disponible en ligne : https://legiscan.com/OH/text/SB300/id/1795258/Ohio-2017-SB300-Introduced.pdf. – G. (Thomas), « Les smart contracts ont désormais une valeur légale dans l'Ohio », *Le journal du coin* [en ligne], 1er juin 2018, https://journalducoin.com/regulation/smart-contracts-valeur-legale-ohio/.

[1219] Arizona House Bill 1022, 12 Apr. 2018, Running nodes; blockchain; regulation prohibition. Disponible en ligne : https://legiscan.com/AZ/text/HB2602/2018.

[1220] KRAMER (Melanie), « Smart Contracts are Seeping into U.S Law – Tennessee Passes Bill », *Bitcoinist* [online], 2 Apr. 2018, https://bitcoinist.com/smart-contracts-are-seeping-into-u-s-law-tennessee-passes-bill/.

[1221] Nevada Senate Bill No. 398, 6 May 2017, Establishes various provisions relating to the use of blockchain technology, BDR 59-158. Disponible en ligne : https://legiscan.com/NV/text/SB398/id/1626453/Nevada-2017-SB398-Enrolled.pdf.

[1222] RODA (Jean-Christophe), « Smart contracts, dumb contracts ? », *D. IP/IT* 2018, n° 2, p. 397, n° 11.

[1223] National Conference of Commissioners on Uniform State Laws, 23-30 Jul. 1999, Uniform Electronic Transactions Act (UETA), Approved and Recommended for Enactment in All the States at its Annual Conference Meeting in its One-Hundred-and-Eighth Year in Denver, Colorado, http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta_final_99.pdf.

[1224] « [La *blockchain* est] un système d'enregistrement électronique de transactions ou d'autres données qui sont : - Ordonnées de manière uniforme ; - maintenus ou traités de manière redondante par un ou plusieurs ordinateurs ou machines pour garantir la cohérence ou la non-répudiation que ce soit des transactions enregistrées ou d'autres données ; - Validé en utilisant la cryptographie. » [« *An electronic record of transactions or other data which is: - Uniformly ordered; - redundantly maintained or processed by one or more computers or machines to guarantee the consistency or non-repudiation of the recorded transactions or other data; - Validated by using cryptography*. » [notre trad.], Nevada Senate Bill No. 398, préc., § 719.045].

[1225] Vermont Act No. 157 (H.868), préc., Sec. I.1., § 1913, b).

[1226] Legge n. 12, 11 feb. 2019, Conversione in legge, con modificazioni, del decreto-legge 14 dicembre 2018, n. 135, recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione. (19G00017) (GU Serie Generale n. 36 del 12 febbraio 2019). – V. notamment, BARBET-MASSIN (Alice), « Réflexions autour de la reconnaissance juridique de l'horodatage blockchain par le législateur italien », *RLDI* 2019/3, n° 157.

Monaco est actuellement en phase de réflexion concernant un projet de loi en ce sens[1227], alors que la France soulignait en 2018 qu' « à court terme, il est possible d'adopter une réforme visant à renforcer, dans le Code civil, la force probante des informations figurant sur une *blockchain* selon des modalités techniques à préciser »[1228].

En l'état actuel, bien qu'elle ne soit pas mentionnée en tant que mode de preuve dans les dispositions législatives ou réglementaires, la *blockchain* semble s'imposer *via* la liberté laissée par le régime probatoire, et notamment celui de la protection du droit d'auteur. Dans ce domaine, elle pourrait concurrencer – voire parvenir à remplacer – les méthodes de preuve précitées, jusqu'ici utilisées en matière de propriété intellectuelle et nécessitant l'intermédiation d'un tiers de confiance. Elle pourrait peut-être se voir un jour reconnaître la valeur d'un mode de preuve à part entière par les tribunaux, voire par le législateur, ou encore se voir reconnaître le statut d'autorité certifiée de confiance pour émettre des certificats d'horodatage à l'instar des certificats de signatures électroniques qualifiés, ce qui lui permettrait d'assurer une valeur probante à tous les actes juridiques inscrits, sans distinction de régime probatoire[1229].

161. En ce qui concerne les transactions dites « consensuelles », non soumises à un formalisme strict, la technologie de la chaîne de blocs semble disposer des outils techniques et technologiques pour pouvoir, à terme, s'imposer. Selon un auteur, le projet *Self-Sovereign Identity* est une première étape, le règlement eIDAS devra tôt ou tard évoluer pour prendre en compte les innovations technologiques apparues depuis 2014, en particulier dans les domaines de l'archivage électronique et des inscriptions de données et de transactions sur *blockchains*[1230]. Dès lors que son utilisation produira des effets juridiques aux données inscrites, soit en permettant de les prouver, soit en leur conférant date certaine, soit les deux, une évolution des pratiques pourra réellement s'opérer à grande échelle. En parallèle, lorsqu'une opération est inscrite, chacun peut en prendre connaissance et la vérifier et ce, sans intermédiaire. La *blockchain* constitue en cela un outil autonome de conservation. D'une manière générale, ces caractéristiques intéressent les secteurs d'activité dépendants de la tenue d'un registre et assumant des fonctions de

[1227] LEGEAIS (Dominique), *op. cit.*, n° 29 : « Il existe par exemple un projet de loi en ce sens pour Monaco. En son article 6 il énonce que "L'inscription d'un acte juridique dans une chaîne de blocs est présumée constituer une copie fidèle, opposable et durable de l'original, portant une date certaine". »
[1228] France stratégie, « Les enjeux des blockchains », *France stratégie* [en ligne], 21 juin 2018, p. 86, https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-rapport-blockchain-21-juin-2018.pdf.
[1229] ROUJA (Robin), « Enveloppe Soleau ou Blockchain ? », *legalstart.fr* [en ligne], 23 août 2017, https://www.legalstart.fr/fiches-pratiques/proteger-une-creation/enveloppe-soleau/.
[1230] CAPRIOLI (Éric A.), « Vers une révision du règlement eIDAS ? », *L'Usine Digitale* [en ligne], 15 oct. 2019, https://www.usine-digitale.fr/article/vers-une-revision-du-reglement-eidas.N894429.

« notarisation »[1231]. Toutes les professions dont l'activité principale repose sur l'authenticité des actes sont potentiellement visées par cette technologie disruptive, à savoir les huissiers, les juges, les experts, les arbitres, les préfets, etc.[1232]. Parmi ces différentes professions, c'est en particulier celle du notaire qui prête le plus à discussion. Pourtant, bien que la rapidité des bits fournisse un avantage incomparable au processus *blockchain*[1233], il ne semble pas *a priori* que la *blockchain* soit capable de faire plus que ce qu'accomplit déjà le notaire, ne serait-ce qu'en matière de publicité ou de force exécutoire des actes, assurée en binôme avec le juge.

Somme toute, alors que certains prétendent pouvoir entièrement remplacer les notaires par la technologie[1234], les notaires eux-mêmes comptent sur elle pour optimiser leur efficacité[1235].

Section 2. Une solution d'optimisation plus que de substitution en matière d'actes authentiques

162. L'architecture naturellement sécurisée et intègre des *blockchains* permet d'envisager la certification de n'importe quelle inscription quant à son existence et son contenu[1236]. C'est à la suite de ce constat qu'a été exprimée la volonté de déployer une *blockchain* dans le secteur. Dans un premier temps il était question de suppléer le monopole des notaires en la matière, à l'image du projet *Notary Ledgers* d'IBM testé au Brésil[1237], ouvrant ainsi de nouveaux champs d'investigation. Pour espérer toutefois atteindre la même reconnaissance juridique que les actes notariés et jouir d'une certaine autonomie vis-à-vis de la fonction notariale, la technologie doit être en mesure de

[1231] BARBRY (Éric), « Smart contracts... Aspects juridiques ! », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 79.
[1232] « La technologie Blockchain : une révolution aux nombreux problèmes juridiques », *Dalloz actualité*, 31 mai 2016, obs. Hielle O.
[1233] MANAS (Arnaud), BOSC-HADDAD (Yoram), « La (ou les) blockchain(s), une réponse technologique à la crise de confiance », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 104 : « [le] temps de latence pour l'enregistrement (de quelques mois aujourd'hui, pour la publicité foncière, a quelques millisecondes, demain, avec un contrat automatique) ; il et, sans doute encore davantage, d'accès transparent et immédiat a une information authentifiée. Ignorer le foisonnement créatif (ou, pire, le combattre) serait donc prendre le risque de passer à cote du potentiel élevé d'innovation des briques technologiques de la *blockchain* ».
[1234] GOSSA (Julien), « Les blockchains et smart contracts pour les juristes », *D. IP/IT* 2018, n° 7-8, p. 393.
[1235] BARBRY (Éric), art. cit., *loc. cit.*
[1236] STREIFF (Vivien), « Blockchain et authenticité : pour copie non certifiée conforme », *D. IP/IT* 2020, n° 2, p. 96.
[1237] FELIX (Bruno), « Brasil registra primeiro contrato via blockchain », *Olhar Digital* [conectados], 10 de dez. de 2020, https://olhardigital.com.br/2020/12/10/noticias/brtasil-registra-primeiro-contrato-via-blockchain/ ; SOUZA MENDES GUIMARÃES (Thiago), « Innovative Blockchain for Notary's Offices », *GrowthTech* [online], 2019, https://growthtech.com.br/innovative-blockchain-for-notarys-offices/.

répondre aux exigences de l'authenticité, voire de dépasser les mécanismes actuels en faisant valoir un avantage comparatif. Or, bien que l'apport de cette technologie soit évident en ce qui concerne la constitution, la conservation et la restitution intègre de preuves[1238], elle s'avère, en l'état actuel, incapable d'égaler l'œuvre du notaire français, que ce soit en matière de publicité (*ledger*) ou même d'exécution (*smart contract*). *A fortiori*, la *blockchain* ne bénéficie pas du même accueil que dans le domaine des actes sous signature privée, de sorte qu'elle n'est pas encore capable de remplacer dans sa fonction le notaire eu égard aux spécificités des tâches qui lui sont assignées et au pouvoir dont il est investi (§ 1). Si le statut d'acte authentique ne représente pour la technologie qu'un idéal inaccessible, la profession a pourtant, dans un second temps, pris la mesure de l'importance de son développement et a mis en place diverses solutions permettant de mettre à profit ses qualités (§ 2).

§ 1. Les spécificités de l'interlocuteur humain : un remplacement délicat

163. En vertu de l'art. 1369 du C. civ., « l'acte authentique est celui qui a été reçu, avec les solennités requises, par un officier public ayant compétence et qualité pour instrumenter ». D'ailleurs, la loi exige l'authenticité pour un certain nombre de conventions conclues entre particuliers et confère par conséquent ce monopole de la preuve authentique complétée des « solennités requises » à un officier publique spécifique. Plus qu'un simple statut, le notaire *est* et *reste* un tiers de confiance qu'il est difficile de remplacer pleinement. Du fait de ses prérogatives, il a le devoir de conseiller et d'assister les parties afin de les mettre en garde sur les dangers de tel acte ou de telle situation, ainsi que de veiller à la protection des droits et intérêts de chacun, ce qu'un algorithme ne peut expérimenter seul, au risque d'entraîner la perte du caractère authentique de l'acte, voire sa nullité s'il s'agissait d'un acte solennel dont les exigences d'authenticité sont requises *ad validitatem* (C. civ., art. 1370). Tout à la fois authentificateur et conseiller, le notaire est investi d'obligations professionnelles pour lesquelles il est responsable envers ses clients en cas de manquement. C'est pourquoi, lorsqu'il intervient pour instrumenter un acte, le notaire dispose de qualités (A) et fournit des garanties (B) en réalité inhérentes à sa fonction.

[1238] Notaires du Grand Paris, « Présentation de la BlockChain Notariale. Dossier de Presse », *Notaires du Grand Paris* [en ligne], 7 juill. 2020, p. 4, https://notairesdugrandparis.fr/sites/default/files/2020-07-07%20-%20DP%20-%20Pr%C3%A9sentation%20de%20la%20Blockchain%20Notariale%20VF2.pdf.

164. Un office fondamental. La loi du 25 ventôse an XI[1239], réformée par l'ordonnance du 2 novembre 1945[1240], témoigne du caractère tant historique que fondamental du métier de ces officiers. L'art. 1er de l'ordonnance dispose que « les notaires sont des officiers publics, établis pour recevoir tous les actes et contrats auxquels les parties doivent ou veulent faire donner le caractère d'authenticité attaché aux actes de l'autorité publique, et pour en assurer la date, en conserver le dépôt, en délivrer des Grosses et expéditions ». Un auteur rappelle par ailleurs que sa fonction d'officier public est une « qualité indispensable pour manier la formule exécutoire »[1241]. Investi de la fonction d'authentification, il résulte de la pratique que sa mission dépasse son rôle de rédacteur d'actes à la fois conformes aux exigences de forme, générales[1242] et spéciales[1243], applicables en la matière, et enregistrés[1244], conservés et éventuellement publiés[1245] par ses soins. En d'autres termes, le notaire doit donner les « vertus de l'authenticité »[1246] à des actes tant valables que sûrs[1247]. Une auteure souligne en effet que le notaire « n'est pas un simple scribe chargé de retranscrire les conventions des parties. Sa fonction est de rédiger des actes authentiques dont la fiabilité est telle que la sécurité des transactions juridiques est ainsi assurée »[1248].

165. Du devoir d'authentification au devoir de conseil : étendue de l'office du notaire. Conférer l'authenticité aux actes juridiques suppose donc nombre d'autres charges qui se révèlent essentielles voire indispensables à l'effectivité de ces actes[1249]. Il

---

[1239] L. n° 1803-3-16 (loi 25 ventôse an XI), 16 mars 1803, contenant organisation du notariat, *Bulletin des Lois*, 3ème S., B. 258, n° 2440.
[1240] Ord. n° 45-2590, 2 nov. 1945, relative au statut du notariat, *JORF*, 3 nov. 1945, p. 7160, et son décret d'application le Décr. n° 45-0117, 19 déc. 1945, pris pour l'application du statut du notariat, *JORF* n° 0302, 22 déc. 1945, p. 8478, dont la dernière modification fut opérée par les Décr. n° 71-942, 26 nov. 1971, relatif aux créations, transferts et suppressions d'office de notaire, à la compétence d'instrumentation et à la résidence des notaires, à la garde et à la transmission des minutes et registres professionnels des notaires, *JORF* n° 0281, 3 déc. 1971, p. 11796, et Décr. n° 73-1202, 28 déc. 1973, relatif à la discipline et au statut des officiers publics ou ministériels, *JORF*, 30 déc. 1973, p. 14137.
[1241] JULIENNE (Maxime), « Pratique notariale et numérique : état des lieux », *D. IP/IT* 2019, n° 2, p. 96, n° 13.
[1242] V. notamment, Décr. n° 71-941, préc., art. 7, 10 et 23.
[1243] DE POULPIQUET (Jeanne), « Exercice de la fonction notariale », *RDI* 2009 (actualisation : avr. 2020), pp. 284-296.
[1244] V. notamment, CGI, art. 1705, 1°.
[1245] La liste des actes soumis à la publicité obligatoire figure à l'art. 28 du Décr. n° 55-22, 4 janv. 1955 portant réforme de la publicité foncière, *JORF*, 7 janv. 1955, p. 346.
[1246] DE POULPIQUET (Jeanne), art. cit., p. 252.
[1247] *Ibid.*, n°s 272 et s.
[1248] *Ibid.*, n° 295.
[1249] Notaires de France, « Le rôle du notaire et ses principaux domaines d'intervention », *notaires.fr* [en ligne], 2 avr. 2013, https://www.notaires.fr/fr/profession-notaire/r%C3%B4le-du-notaire-et-ses-principaux-domaines-dintervention/le-r%C3%B4le-du-notaire.

en va ainsi, par exemple, de l'obligation de contrôle de l'identité[1250], de la capacité, des pouvoirs[1251], du libre consentement des parties[1252], ainsi que de la date des documents[1253]. Plus encore, parce que le notaire est « tenu d'éclairer les parties et de s'assurer de la validité et de l'efficacité des actes rédigés par lui »[1254], il est investi d'un devoir général d'information[1255]. Ce devoir consiste à les avertir de la légalité des conventions, de leur conformité aux lois et règlements en vigueur[1256]. Plus encore, le notaire doit guider les parties contractantes dans des situations juridiques ou jurisprudentielles incertaines, y compris si cela signifie pour le notaire de les dissuader de conclure l'acte envisagé[1257], mais il a également l'obligation de les avertir de toute disproportion manifeste dans les termes contractuels[1258] et de vérifier l'opportunité-même de l'opération[1259], notamment en s'assurant de découvrir et de respecter la volonté et l'intérêt des parties[1260]. L'office du notaire s'avère donc primordial, non seulement à l'égard de l'*instrumentum*, mais également à l'égard du *negotium*[1261]. Cette importante mission qui lui est confiée est de plus protégée par le caractère « impartial et désintéressé » de son office[1262]. Le devoir de

[1250] Décr. n° 71-942, préc. art. 5.
[1251] *Id.* – V. également, Cass. Civ. 1ère, 25 nov. 1969, *Bull. civ*. I, n° 364 (« l'action en responsabilité formée contre un notaire par une partie qui, suivant acte authentique a prêté à deux époux une certaine somme et, après la faillite de son débiteur, a appris que la personne qui avait signé l'acte avec celui-ci était non pas sa femme, divorcée depuis quelques semaines, mais sa concubine, […] le notaire a commis une faute »).
[1252] *Ibid.*, art. 6.
[1253] Décr. n° 73-1202, préc., art. 48.
[1254] Cass. Civ. 1ère, 11 oct. 1966, *D.* 1967, 209, note M. Ancel, *JCP N* 1966, II, 14703.
[1255] Sur l'origine prétorienne du devoir de conseil du notaire, V. DE POULPIQUET (Jeanne), art. cit., pp. 252-253, 296 et s. La première apparition de cette obligation professionnelle du notaire dans la jurisprudence remonte à un arrêt de la Cour de cassation en date du 21 juillet 1921. Les juges ont considéré que « les notaires, institués pour donner aux conventions des parties les formes légales et l'authenticité qui en est la conséquence, ont également pour mission de renseigner les clients sur les conséquences des engagements qu'ils contractent, responsables en vertu de l'article 1382 [ancien, art. 1240 nouveau] du Code civil, ils ne peuvent stipuler l'immunité de leurs fautes et par suite décliner le principe de leur responsabilité en alléguant qu'ils se sont bornés à donner la forme authentique aux conventions des parties ». – V. également, PHILIP (Alexia), « Le devoir de conseil du notaire mis à rudes épreuves », *Le Petit Juriste* [en ligne], 14 janv. 2011, https://www.lepetitjuriste.fr/droit-civil/droit-de-la-responsabilite-delictuelle/le-devoir-de-conseil-du-notaire-mis-a-rudes-epreuves/.
[1256] COIFFARD (Didier), art. cit., n° 147.
[1257] Cass. Civ. 3e, 2 juill. 1970, n° 68-12.523, *Bull. civ*. III, n° 463, p. 336 ; Cass. Civ. 1ère, 3 avr. 2007, n° 06-13.304, *Bull. civ*. I, n° 143. – V. également, DE POULPIQUET (Jeanne), art. cit., p. 252.
[1258] V. en ce sens, Cass. Civ. 1ère, 25 mars 2009, n° 07-20.774 (qui tout en limitant l'étendue de la responsabilité du notaire, en fixe le cadre : « encourt la cassation l'arrêt qui, après avoir condamné des collatéraux à restituer à l'héritier réservataire les sommes qu'ils avaient indûment perçues à l'issue d'un partage successoral, condamne le notaire, ayant commis une faute dans le règlement de la succession, à payer à cet héritier des dommages-intérêts d'un montant égal à celui de l'actif successoral, diminué des droits de succession, puisque cette somme comprend une partie de l'actif successoral devant faire l'objet d'une restitution et qu'une telle restitution ne constitue pas en elle-même un préjudice indemnisable, le notaire pouvant seulement être condamné à la garantir à la mesure de l'insolvabilité des collatéraux tenus à restitution »).
[1259] Notaires de France, « Le rôle du notaire et ses principaux domaines d'intervention », préc.
[1260] DE POULPIQUET (Jeanne), art. cit., p. 309-312.
[1261] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., *loc. cit.*
[1262] Conseil Supérieur du Notariat, « Règlement national, Approuvé par arrêté de Madame la Garde des Sceaux, Ministre de la justice en date du 22 juill. 2014, JO du 1er août 2014 », *Conseil Supérieur du Notariat*

conseil qui incombe au notaire est un devoir absolu[1263], insusceptible d'atténuation[1264]. Il représente en cela l'élément essentiel de la fonction notariale car garant de l'efficacité et de la validité des actes dressés, autrement dit des « vertus intrinsèques » de l'acte authentique que sont la force probante et la force exécutoire[1265], par ailleurs garanties grâce à l'assistance du juge[1266].

Or, comme le constate Mustapha Mekki, « dans une *blockchain*, aucune vérification de ce type n'est opérée »[1267]. Consentement libre et éclairé, mise en garde, capacité, légalité, proportion, prestation et contre-prestation, protection de la partie faible, accessibilité et faisabilité du projet, ... sont autant d'éléments constitutifs de l'opération contractuelle qu'en l'état de l'art la technologie ne contrôle pas, du moins pas seule, à la différence – manifeste – du notaire[1268]. Selon un auteur, « lier la place particulière occupée par l'authenticité dans la hiérarchie de la preuve au seul respect de solennités, si nombreuses et précises soient-elles, fait en réalité l'impasse sur l'action du notaire dans la construction de l'acte authentique »[1269]. Ce constat n'est cependant pas sans soulever quelques difficultés. Un auteur évoque ainsi le cas général d'un adolescent qui aurait perdu un pari sportif sur la *blockchain* et, sans qu'il puisse s'y opposer, le *smart contract* précédemment conclu aurait versé automatiquement au vainqueur son gain[1270]. Il se pourrait même qu'en cas d'impossibilité de paiement, le *smart contract* somme l'adolescent de recharger son compte dans les dix jours afin de pouvoir effectivement verser la somme due, l'informant que dans le cas contraire, une pénalité serait prononcée à son encontre. Les jeux d'argent ne sont-ils pourtant pas interdits aux mineurs en vertu des art. 1128 du C. civ., et 5, al. 3, de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne[1271] ? En réalité, ils le sont en France, or la *blockchain* ne semble pas, en l'état actuel, prendre en compte ni la loi des États ni l'âge ou la nationalité de l'utilisateur, et n'est de

---

[en ligne], p. 5, https://www.notaires.fr/sites/default/files/reglement_national_-_reglement_intercours_-_arrete_du_22_07_2014_-_jo_du_01_08_2014.pdf.

[1263] *Ibid.*, n° 322.

[1264] DE POULPIQUET (Jeanne), art. cit., pp. 322-325.

[1265] COIFFARD (Didier), art. cit., n° 147.

[1266] *Id.*

[1267] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., *loc. cit.*

[1268] JULIENNE (Maxime), art. cit., n° 14 : « les outils d'automatisation dont on dispose aujourd'hui portent essentiellement sur des vérifications factuelles (ex. date, identité des parties) ou documentaires (ex. présence d'une annexe, mentions portées sur un fichier), mais ils ne permettent pas de s'assurer que le signataire comprend réellement ce qu'il fait, que l'acte correspond bien à sa volonté, qu'il est licite, efficace et respectueux des droits des tiers ».

[1269] STREIFF (Vivien), « Blockchain et authenticité : pour copie non certifiée conforme », art. cit., p. 95.

[1270] Exemple donné par Gaëtan Guerlin, v., GUERLIN (Gaëtan), « Considérations sur les smart contracts », *D. IP/IT* 2017, n° 10, p. 512.

[1271] L. n° 2010-476, 12 mai 2010, relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne, *JORF* n° 0110, 13 mai 2010, p. 8881.

surcroît pas exclusivement circonscrite aux frontières de l'hexagone. Un rapport signalait d'ailleurs « qu'on le veuille ou non, les règles de droit ne sont pas conçues et formulées en vue de leur application par des automates mais en vue d'une solution juste que seule l'intervention d'un Homme peut pleinement apporter »[1272]. Bien que vivement humanisante, force est de constater que, en matière d'actes notariés du moins, cette affirmation se trouve confortée par le rôle indispensable de l'officier publique, qui n'est pas plus un « témoin passif de l'accord des parties »[1273] que le simple respect des solennités est suffisant pour déclarer authentique une feuille de papier.

166. La disponibilité et l'accessibilité du notaire. Par ailleurs, le fait qu'en pratique le notaire soit tenu de se rendre disponible pour les besoins de ses clients, notamment pour délivrer des copies des actes qu'il conserve[1274], constitue une autre spécificité de la fonction notariale qui contraste avec les propres fonctionnalités de la technologie. Bien qu'elle soit dématérialisée et distribuée, la *blockchain* ne peut en effet pas répondre à l'une quelconque des requêtes de ses clients hormis ce que lui permet son protocole, c'est-à-dire d'initier ou d'accepter une transaction, et ce que proposent les explorateurs de *blockchain*, c'est-à-dire d'accéder aux informations disponibles en clair concernant les blocs d'une chaîne, ou encore de rechercher des transactions et des adresses publiques de *wallets*[1275].

De cette manière, si un client perdait l'*instrumentum* notarié, il ne perdrait en aucun cas le bénéfice des droits qui y figuraient. Plus encore, il pourrait, de même que toute partie concernée, ainsi que leurs héritiers ou ayants droit, obtenir une copie de l'acte auprès du notaire qui l'a établi (C. civ., art. 1435-1441), puisque ce dernier a l'obligation de conserver au sein de son étude tout acte qu'il authentifie[1276] pour une durée pouvant aller jusqu'à soixante-quinze ans, voire cent ans s'il se rapporte à une personne mineure (C. patr., art. L. 213-2, I, 4°-5°)[1277]. En revanche, s'il advenait que l'utilisateur d'une *blockchain* perde sa clé privée, il n'aurait aucun recours[1278], et les qualités d'immuabilité

[1272] GIJSBERS (Charles) *et al*., « Les fondamentaux du notariat confrontés à l'intelligence artificielle », *JCP N* 2018, n° 10, act. 1111.
[1273] STREIFF (Vivien), « Blockchain et authenticité : pour copie non certifiée conforme », art. cit., *loc. cit*.
[1274] Décr. n° 71-941, préc., art. 32-37, modifiés par le Décr. n° 2005-973, 10 août 2005, modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires, *JORF* n° 186, 11 août 2005, p.13096, texte n° 34, art. 4.
[1275] Sur les informations disponibles en clair concernant chacun de ces éléments, v., notamment, G. (Thomas), « Tutorial : comment lire un explorateur de blockchain Bitcoin ? », *Journal du Coin* [en ligne], 11 mai 2019, https://journalducoin.com/bitcoin/actualites-bitcoin/comment-lire-un-explorateur-de-blockchain/.
[1276] Décr. n° 71-941, préc., art. 32-37.
[1277] Notaires de France, « Le rôle du notaire et ses principaux domaines d'intervention », préc.
[1278] Par exemple, en 2013, le britannique James Howells a « perdu » l'intégralité de son *wallet* d'une valeur de 7 500 *bitcoins* (soit 42 604 685,13 euros au cours du 26 août 2018) en se débarrassant

et d'intégrité de la chaîne de blocs n'y changeraient rien. À condition que le tiers qui en a la gestion soit aussi digne de confiance que l'est le notaire[1279], la solution serait d'utiliser un *wallet*, qui est un portefeuille électronique de gestion d'adresses et de clés associées, à l'instar de « *Ledger Nano S* »[1280].

167. Finalement, garant de la validité, de l'efficacité autant que de l'opportunité d'un acte authentique, le notaire est plus qu'un simple scribe aux fonctions d'enregistrement à date certaine : il est un délégataire de la puissance publique, et de cette mission émane une pyramide de responsabilités justifiant l'existence de garanties inhérentes à son intervention.

B. Garanties inhérentes à l'intervention du notaire

168. La possibilité d'engager la responsabilité professionnelle et collective des notaires. Un auteur constate que « les attributs attachés à l'acte authentique trouvent leur origine dans une délégation de puissance publique, laquelle est compensée par la soumission du notaire à un contrôle des actes qu'il reçoit, pour s'étendre à l'ensemble de son activité, y compris celle relevant de faits extra professionnels »[1281]. Les devoirs attachés à la fonction notariale sont à la fois multiples et de diverses natures. Eu égard à son rôle de « délégataire de puissance publique », le notaire fait lui-même l'objet d'un contrôle dans l'exercice de ses fonctions. En cas d'impair, il engage sa responsabilité civile professionnelle en raison de son fait, de sa faute ou de sa négligence, soit dans la pratique tantôt contractuelle ou extracontractuelle tantôt délictuelle ou quasi-délictuelle en fonction des circonstances[1282]. Mais il engage également, d'un point de vue financier et selon l'opération, la responsabilité collective de tous ses confrères *via* l'assurance obligatoirement souscrite par chacun[1283]. L'Institut National des Formations Notariales

malencontreusement d'un des disques durs de son PC contenant les codes dudit portefeuille *Bitcoin*. V. en ce sens, HERN (Alex), « Missing: hard drive containing Bitcoins worth £4m in Newport landfill site », *The Guardian* [online], 27 Nov. 2013, https://www.theguardian.com/technology/2013/nov/27/hard-drive-bitcoin-landfill-site).

[1279] Aucun recours possible n'est en effet techniquement prévu en cas de *bug* ou d'attaques malveillantes, sur le sujet, *infra* n^{os} 326 et s. – V. également, FLORI (Jean-Pierre), art. cit., p. 101 ; HELLEU (Guillaume), MASURE (Anthony), « Total Record. Les protocoles blockchain face au post-capitalisme », *Multitudes* 2018/2, n° 71, p. 76.

[1280] TYCHEY (Jde), « uPort ou la gestion de l'identité par la blockchain », *Ethereum France* [en ligne], 27 sept. 2016 (mis à jour : 30 mai 2017), https://www.ethereum-france.com/uport-ou-la-gestion-de-lidentite-par-la-blockchain/.

[1281] STREIFF (Vivien), « Blockchain et propriété immobilière : une technologie qui prétend casser les codes », *Dr. & Patr.* oct. 2016, n° 262, p. 25.

[1282] DE POULPIQUET (Jeanne), art. cit., pp. 256-269.

[1283] En vertu de l'art. 12, al. 2 et 3, du Décr. n° 55-604, 20 mai 1955, relatif aux officiers publics ou ministériels et à certains auxiliaires de justice, *JORF*, 22 mai 1955, p. 5136, la garantie collective

constatait que, depuis 2006, « sur les 4,5 millions d'actes que les notaires reçoivent en France, à peine 0,1 pour mille donne lieu à contentieux, ce qui témoigne de la grande sécurité de l'intervention notariale »[1284].

En parallèle, il apparaît que la technologie *blockchain* ne fasse, pour sa part, l'objet d'aucun contrôle ni d'aucune sanction de quelque nature que ce soit[1285].

169. Le contrôle de l'efficacité des actes dressés par le notaire : les subtilités de l'obligation de vérification. Sécurisée et immuable, la technologie de la chaîne de blocs semble capable de remplacer les registres de publicité en matière immobilière. Seulement, dans la pratique, l'authentification et la publication d'actes constitutifs, translatifs ou extinctifs de droits réels immobiliers répond à un corps de règles juridiques spécifiques[1286] qui nécessitent une attention qui dépasse l'entendement de l'individu lambda ou la capacité de transposition d'un langage de programmation. Il en va ainsi, par exemple, des vérifications préalables à toute publication officielle d'un acte notarié portant sur le transfert de propriété d'un bien immobilier[1287]. Lorsque le notaire instrumente et archive les actes qu'il reçoit[1288], il n'agit pas en tant que modeste « tamponneur » – ou « *public notary* » – tel que le ferait probablement la *blockchain* en la matière[1289]. Le notaire est dans l'obligation de mener une enquête sérieuse et efficace[1290], d'aller au-delà de l'accord, des déclarations[1291] et des connaissances des

« s'applique au remboursement des sommes d'argent, à la restitution des titres et valeurs quelconques reçus par les notaires à l'occasion des actes de leur ministère ou des opérations dont ils sont chargés en raison de leurs fonctions » et « s'étend aux conséquences pécuniaires de la responsabilité civile encourue par les notaires dans l'exercice normal de leurs fonctions à raison de leur fait, de leur faute ou de leur négligence, ou du fait, de la faute ou de la négligence de leur personnel ».

[1284] « Les garanties apportées par le Notaire », *Institut National des Formations Notariales* [en ligne], http://www.ecole-notariat.fr/home/qu-est-ce-qu-un-notaire/94-les-garanties-apportees-par-le-notaire.

[1285] BAYLE (Aurélie) *et al.*, art. cit., p. 26.

[1286] STREIFF (Vivien), « Blockchain et propriété immobilière : une technologie qui prétend casser les codes », art. cit., p. 24.

[1287] Décr. n° 55-22, 4 janv. 1955, portant réforme de la publicité foncière, *JORF*, 7 janv. 2955, art. 28.

[1288] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., *loc. cit.*

[1289] *Id.*

[1290] V. par exemple, Cass. Civ. 1ère, 13 nov. 1991, n° 89-15.011, *Bull. civ.* I, n° 310, p. 202 (« commet une faute professionnelle grave le notaire qui reçoit l'acte de vente d'un terrain sans procéder à des recherches suffisantes sur l'origine de propriété de ce terrain ») ; Cass. Civ. 1ère, 18 janv. 1978, n° 76-13.046, *Bull. civ.* I, n° 28, p. 23 (« le notaire rédacteur de l'acte de vente d'un immeuble a l'obligation […] de contrôler les déclarations des parties, procéder à des recherches sur la situation des biens, plus particulièrement vérifier les origines de propriété de l'immeuble vendu, s'assurer des droits du vendeur en se référant notamment aux actes de son étude et contrôler au fichier mobilier les mutations intervenues. Les juges du fond ont dès lors pu estimer qu'en négligeant de procéder à ces vérifications, le notaire, rédacteur de l'acte, avait commis une faute engageant sa responsabilité »).

[1291] V. par exemple, Cass. Civ. 1ère, 6 janv. 1994, n° 92-11.459 (« le notaire chargé d'une vente a l'obligation de vérifier les droits de propriété, les titres du vendeur et d'établir l'origine de propriété trentenaire, que ces vérifications doivent être d'autant plus minutieuses que les titres laissent apparaître, comme en l'espèce, une importante discordance ») ; Cass. Civ. 1ère, 3 mai 1983, *Bull. civ.* I, n° 136.

parties[1292], « afin de dissiper toute équivoque »[1293]. Il doit refuser de s'investir lorsque le processus d'authentification est susceptible de contrarier l'ordre public ou les droits des tiers[1294]. Au moindre doute, l'officier engage sa responsabilité professionnelle[1295]. Dans le cas par exemple d'une vente immobilière, un *smart contract* est capable d'automatiser les échanges de documents[1296], d'exécuter les transferts de fonds, de notifier les étapes essentielles de la contractualisation[1297] et même d'appliquer le délai de rétractation légale[1298]. Mais il restera difficile pour un programme de vérifier si le bien immobilier objet de la vente appartient véritablement à celui qui entend s'en séparer ou encore de contrôler la contenance des droits de propriété sur ce bien, par exemple les questions de bornage de terrains limitrophes. En effet, il est possible de devenir propriétaire sans passer par un contrat *via* l'accession, l'usucapion ou la théorie de l'apparence (C. civ., art. 712), qui sont des notions aussi importantes que communes en droit immobilier. Prétendre que la *blockchain* puisse valoir preuve certaine d'un titre de propriété peut donc se révéler délicat. Le régime de la propriété foncière présente de multiples particularités de nature à la rendre inaccessible, tant pour la technologie des *smart contracts* que pour l'individu lambda qui se servirait de la fonction *ledger* de la *blockchain* pour enregistrer un acte authentique. En effet, s'il s'avère qu'un conflit se soulève entre acquéreurs successifs disposant de titres contradictoires, l'horodatage de la *blockchain* sera-t-il seul compétent, sans conseil juridique d'un professionnel, pour départager les potentiels propriétaires[1299] ? Les devoirs de vérification et de conseil du notaire suggèrent, à peine de responsabilité, que son intervention aboutira à des actes valables et sûrs, et à des transactions juridiques sécurisées. Ce sont ses obligations statutaires et sa mission de « dispensateur de sécurité juridique »[1300] qui font de l'officier public un intermédiaire difficilement substituable.

[1292] V. par exemple, Cass. Civ. 1ère, 25 nov. 1997, n° 95-18.618, *Bull. civ*. I, n° 329, p. 223 (« les compétences personnelles du client [professionnel des questions immobilières] ne dispensent pas le notaire de son devoir de conseil ») ; Cass. Civ. 1ère, 19 mai 1999, n° 96-22.892, *Bull. civ*. I, n° 166, p. 110 (il s'agissait en l'espèce « d'un gérant de sociétés, qualifié dans les autres actes de promoteur immobilier, voire de conseiller fiscal ») ; Cass. Civ. 1ère, 3 avr. 2007, n° 06-12.831, *Bull. civ*. I, n° 142, *D*. 2007, *AJ*, p. 1271 (il s'agissait en l'espèce d'un notaire).

[1293] DE POULPIQUET (Jeanne), art. cit., p. 302.

[1294] STREIFF (Vivien), « Blockchain et authenticité : pour copie non certifiée conforme », art. cit., p. 98.

[1295] V. notamment sur le sujet, BESSON (Marie-Laure), « La responsabilité du rédacteur d'actes immobiliers à l'ère du numérique », *AJDI* 2021, n° 3, pp. 171-182.

[1296] Notamment en ce qui concerne les documents prévus aux art. L. 721-2 et L. 721-3 du CCH.

[1297] À partir du moment où une offre d'achat a été programmée *via* un *smart contract*, celui-ci peut inclure une date limite de validité de l'offre, ou au contraire une fonction de rédaction et conclusion immédiate d'un compromis de vente ou d'une promesse de vente dès lors que l'offre est acceptée.

[1298] Notamment s'agissant du droit de rétractation de l'art. L. 271-1 du CCH.

[1299] Pour plus de précisions sur le sujet, v., BAYLE (Aurélie) *et al.*, art. cit., pp. 26 et s.

[1300] DE POULPIQUET (Jeanne), art. cit., p. 323.

170. Le notaire, le maillon de la confiance. Bien que la technologie de la chaîne de blocs ait cette particularité d'instaurer par défaut un climat de confiance, ce sentiment de sécurité se révèle relativement abstrait. Or, la rigueur nécessaire en matière d'actes authentique suggère que l'intermédiaire authentificateur, réel ou virtuel, soit assez convainquant pour que les individus lui confient leurs biens. La fonction du notaire est telle qu'il apparaît difficile de substituer à son intervention une inscription, même automatisée, sur un registre décentralisé. Le rôle exercé par le notaire dans les diverses missions qui lui sont attribuées s'avère primordial en termes de garantie, ce qui fait du notaire un tiers difficilement imitable. Il est un passage indispensable pour l'authentification de nombreux actes tels que les contrats de mariage, les donations entre époux, les donations partage[1301]. Le notaire est la personnification de la confiance authentique. C'est son statut de délégataire de la puissance publique, strictement encadré par des règles déontologiques[1302] extrêmement contraignantes[1303], qui lui confèrent cette qualité de « témoin privilégié »[1304]. La confiance en sa fonction est le fondement de la validité et de l'efficacité de son travail.

Finalement, la *blockchain* est à la frontière entre « certifier » et « authentifier » en ce sens qu'elle peut certifier d'actes sous signature privée mais qu'elle ne peut les authentifier, du moins pas sans l'intervention du notaire.

§ 2. L'inaccessibilité du statut d'acte authentique : des solutions *blockchain* divergentes

171. Qu'il s'agisse d'actes ou de relations juridiques consignés dans un acte authentique conformément aux exigences légales ou qu'il s'agisse d'actes pour lesquels l'authentification est le fruit de la volonté des parties, il semble impossible, en l'état actuel, que leur inscription sur une *blockchain* ait la même valeur juridique qu'un acte notarié. D'autant plus que les notaires semblent vraisemblablement résolus à protéger leur parcelle d'autorité. Cependant, force est de constater que la technologie n'est pas sans ressources puisque sa mise en œuvre dans le domaine pourrait, à de multiples égards, profiter à la preuve authentique autant qu'aux notaires[1305]. Lorsqu'il s'est agi d'organiser

[1301] Notaires de France, « Le rôle du notaire et ses principaux domaines d'intervention », préc.
[1302] Conseil Supérieur du Notariat, *Règlement national*, préc.
[1303] COIFFARD (Didier), art. cit., n° 147.
[1304] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., *loc. cit.*
[1305] Un auteur souligne d'ailleurs que, « sitôt que l'on admet que l'architecture de la *blockchain* permet de garantir l'intégrité d'un registre en le préservant d'une éventuelle altération de la part de l'un des nœuds du réseau, il n'est pas déraisonnable de soutenir que les transactions qui y sont stockées sont certifiées quant à leur existence et leur contenu » [STREIFF (Vivien), « Blockchain et authenticité : pour copie non certifiée conforme », art. cit., p. 95].

un travail commun entre le notaire et la chaîne de blocs, deux solutions ont été mises en exergue par la doctrine. D'une part, il s'agissait de corriger les lacunes de la technologie par le biais de l'intervention du notaire. D'autre part, il était question de permettre au notaire d'optimiser son activité grâce à elle.

Partant du constat que la profession refuse de devenir l'assistant de la technologie et que, par voie de conséquence, c'est à elle de s'adapter (A), un projet a été élaboré par les notaires eux-mêmes, faisant de la *blockchain* un outil au service de l'authenticité (B).

A. Du refus de l'assistance humaine à l'adaptation de la technologie

172. Parfaire le fonctionnement de la *blockchain* : le notaire comme assistant physique aux fonctions multiples. Une auteure propose que, pour corriger les défauts de la technologie *blockchain* en matière d'authenticité, le notaire soit investi de la mission de prestataire de confiance qualifié au sens du règlement eIDAS[1306]. D'autres auteurs considèrent que le notaire pourrait devenir le « fournisseur d'identité » de la *blockchain*[1307], ou encore l'organe externe à la chaîne, cet « Oracle » – intermédiaire physique – dont la mission implique d'entrer manuellement dans la *blockchain* des données captées dans le monde physique pour que celle-ci puisse s'exécuter[1308]. Par ce biais, le notaire recueillerait et saisirait les informations nécessaires à la rédaction d'un acte, telles que les nom et lieu d'établissement de son étude, les noms, prénoms, domiciles des parties ainsi que de tous les signataires et éventuels témoins, mais également le lieu où est signé l'acte[1309]. Par ailleurs, en tant que juriste le notaire apporterait sa connaissance de la loi, à la fois pour maintenir la *blockchain* conforme à la législation en vigueur et pour répondre au devoir de conseil et d'information qu'exige le processus d'authentification. La teneur de certaines mentions spécifiques et obligatoires lors de la rédaction d'un acte authentique pourrait ainsi faire l'objet d'un contrôle par le notaire, en particulier en ce qui concerne les contrats portant sur la vente d'un immeuble, la cession d'un fonds de commerce, d'un bail, d'une promesse de bail (CGI, art. 850)[1310], ou d'un

[1306] GUILHAUDIS (Élise), art. cit., p. 10.
[1307] DOUVILLE (Thibault), VERBIEST (Thibault), « Blockchain et tiers de confiance : incompatibilité ou complémentarité ? », *D.* 2018, n° 5, p. 1144.
[1308] COIFFARD (Didier), art. cit., *loc. cit*. – V. également, MEKKI (Mustapha), « Blockchain, smart contracts et notariat », *JCP N* 2018, n° 27-599, pp. 8-10.
[1309] Décr. n° 73-1202, préc., art. 48.
[1310] CGI, art. 850 : « l'acte ou la déclaration [doit être terminée] par une mention ainsi conçue : "Les parties affirment, sous les peines édictées par l'article 1837 du code général des impôts que le présent acte (ou la présente déclaration) exprime l'intégralité du prix ou de la soulte convenue" ».

office ministériel (CGI, art. 864)[1311]. Passerelle entre les inscriptions de la *blockchain* et le monde physique, il pourrait de surcroît lui permettre de répondre à certaines obligations légales que ne peut, en principe, remplir un algorithme. Il en va ainsi, par exemple, des exigences relatives au mode de réalisation de la copie de l'acte (CPC, art. 1435-1441), et plus particulièrement celles attachées à la reproduction de l'original destiné à la conservation des hypothèques[1312]. En contrepartie, le notaire bénéficierait de l'instantanéité de la technologie lors de l'exécution de son obligation de communication dans des délais raisonnables[1313]. Toutefois, cette solution prête à discussion.

173. Certifier n'est pas authentifier. Du point de vue des notaires, la chaîne de blocs est effectivement une technologie de certification, mais elle ne peut cependant être davantage[1314]. Cette restriction formelle trouve son origine dans la recherche constante de rigueur juridique, principalement due à la noblesse de l'acte en question, exigeant justesse et précision lexicale afin d'éviter toute confusion. Selon eux, contrairement à ce que signifie juridiquement le mot « authentifier »[1315], la définition classique renvoie principalement à l'idée de désigner l'auteur d'un écrit, discours ou œuvre[1316]. Or, lorsqu'il mentionne les caractéristiques des *blockchains*, l'écosystème utilise le terme « authentifier » dans son acception courante, constituant pour le protocole la faculté de rattacher *x* ou *y* inscription ou signature à son auteur réel, et non de lui conférer l'authenticité à l'instar du sens que le droit donne à un acte juridique[1317]. Ainsi, cette acception de l'authentification « commune » se rapproche de la notion de « certification », consistant, pour une autorité, à « rendre certain un acte ou un fait en affirmant, après vérification, sa véracité, son authenticité, son origine, sa conformité »[1318]. Par ailleurs, une autre cause possible de la confusion concernant le rôle réel de la

[1311] CGI, art. 864 : le notaire doit faire mention que l'acte « n'est modifié ou contredit par aucune contre-lettre contenant une augmentation du prix ou de la soulte ».
[1312] MOURALIS (Jean-Louis), « Preuve : Modes de preuve », *Rép. civ. Dalloz*, v° Preuve, 2011, n° 102.
[1313] MARGUÉNAUD (Jean-Pierre), « La Convention européenne des droits de l'homme et le notariat », *Defrénois* 15 déc. 1999, n° AD1999DEF1281N1, pp. 1293-1294. – V. également, CEDH, Cour (3e Section), 3 oct. 2000, n° 35589/97 (décision fondée sur l'art. 6, § er de la Conv. EDH qui prévoit que « toute personne a droit à ce que sa cause soit entendue […] dans un délai raisonnable, par un tribunal […] qui décidera […] des contestations sur ses droits et obligations de caractère civil »). Jean-Pierre Marguénaud a d'ailleurs commenté cette décision à la lumière de l'obligation de délivrance du notaire dans un délai raisonnable.
[1314] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 10 ; STREIFF (Vivien), « Blockchain et authenticité : pour copie non certifiée conforme », art. cit., p. 95.
[1315] PUIGELIER (Catherine) (dir.), *Dictionnaire juridique*, éd. Bruylant, 2e édition, 2017, Section 4 : « Authentifier (verbe) (Droit de la preuve) – Conférer l'authenticité à un acte. Attester l'authenticité d'un document ou d'un écrit. », étant donné que l'authenticité constitue la « qualité dont est revêtu un acte du fait qu'il est reçu ou, au moins, dressé par un officier public compétent, suivant les solennités requises ».
[1316] Dictionnaire Larousse [en ligne], v° Authentification, https://www.larousse.fr/dictionnaires/francais/authentification/6559.
[1317] BARRAUD (Boris), « Les blockchains et le droit », art. cit., *loc. cit.*
[1318] *Id.*

blockchain chez les auteurs français apparaît dans la traduction en langue anglaise des notions « authentifier » et « certifier », qui se réunissent en un mot unique, « *authenticate* ».

Il n'en demeure pas moins que l'authentification juridique représente bien plus que l'action de certifier par écrit un contenu à une date certaine[1319]. Il manque à la certification ce que certains auteurs décrivent comme la « dimension intellectuelle attachée à l'authenticité »[1320]. Or, dans l'hypothèse d'une *blockchain* d'authentification des actes, cette dimension est donnée – et ne peut l'être que – par l'intervention du notaire, si bien que ce dernier refuse d'être présenté dans un rôle d'apparence subalterne à la technologie.

174. La solution du clerc de *blockchain* : résistances, conciliation et adaptations. Un autre élément sujet à discussion réside dans la fonction qu'assumerait le notaire dans un système d'authentification des actes juridiques *via blockchains*. En comblant les lacunes de la chaîne avec l'expérience et l'intervention de l'officier public, son statut serait disrupté alors même que sans lui la technologie ne pourrait, au plus, que certifier l'origine et le contenu d'un acte. Eu égard à la spécificité et à la rigueur du domaine de l'authenticité, l'acte authentique reste un écrit au statut pour le moment inaccessible et le notariat une fonction difficilement égalable. Ses exigences égalent ses vertus, en témoigne d'abord l'abandon d'une proposition d'amendement en date du 1er juin 2016 ayant pour objet de reconnaître à l'inscription sur *blockchain* la même force probante que les actes électroniques authentiques[1321], ensuite la promesse faite aux notaires par le Garde des Sceaux le 6 juin que la loi ne permettra pas à la technologie de les remplacer[1322].

[1319] CNRTL [en ligne], v° Certification, https://www.cnrtl.fr/definition/certification.

[1320] COIFFARD (Didier), art. cit., n° 147.

[1321] Amendement n° 227, 1er juin 2016, relatif à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (n° 3785), présenté par la députée Laure de La Raudière *et al.* : « Après le deuxième alinéa de l'article L. 330‑1 du code monétaire et financier, il est inséré un alinéa ainsi rédigé : "Les opérations effectuées au sein d'un système organisé selon un registre décentralisé permanent et infalsifiable de chaîne de blocs de transactions constituent des actes authentiques au sens du deuxième aliéna de l'article 1317 du code civil." »

[1322] « Blockchains publiques : l'inquiétude des notaires », *bitcoin.fr* [en ligne], 9 juin 2016, https://bitcoin.fr/blockchains-publiques-linquietude-des-notaires/. – Extrait du discours de Jean-Jacques Urvoas, Garde des Sceaux, ministre de la Justice à la séance solennelle d'ouverture du 112ème Congrès des Notaires de France à Nantes le lundi 6 juin 2016 : « Parce que l'acte authentique n'est pas qu'une procédure, la *blockchain* ne pourra pas se substituer à lui. Cette technologie de stockage numérique et de transmission à coût minime n'est qu'une technique et ce n'est pas cela qui fait l'acte authentique. C'est l'intervention du détenteur d'une parcelle d'autorité publique. Et ceux que l'on appelle les mineurs, ouvriers de la *blockchain*, n'en sont pas pourvus. J'en profite pour confirmer que dans le cadre du projet de loi sur la transparence, la lutte contre la corruption et la modernisation de la vie économique, le gouvernement s'opposera à tout amendement qui sacrifierait sur l'autel du numérique toute la puissance publique et par voie de conséquence, les délégations des officiers publics et ministériels. J'ai en effet, observé une volonté d'une parlementaire de l'opposition de "permettre à la France de prendre une avance juridique en ce qui concerne la reconnaissance des effets juridiques de l'utilisation de la *blockchain* dans les opérations sur instruments

Fermement décidés à protéger leur parcelle d'autorité[1323], les notaires soulignent à cette occasion l'importance d'agir sans précipitation alors que la technologie n'en est qu'à ses balbutiements. De plus, en instituant le notaire comme l'assistant de la technologie, cela reviendrait à déclarer, indûment, que la technologie *blockchain* est fondamentalement limitée, alors même qu'elle ne demande qu'à s'adapter. Une solution de conciliation s'avère nécessaire. Il convient donc de donner la possibilité à la technologie de se déployer et de se perfectionner selon un modèle à la fois productif et enrichissant pour l'un comme pour l'autre – notaire et *blockchain* –, qui consisterait en une coopération et un échange d'expérience et de savoir-faire. Force est de reconnaître que la rapidité, le moindre coût et la souplesse de l'outil algorithmique contribuent à le présenter comme une opportunité à explorer pour tous les notaires[1324]. Mais, comme le souligne un auteur, « il faut pour cela identifier, dans les diverses tâches qu'assume le notaire au quotidien, celles dans lesquelles il pourra le mieux tirer profit des outils numériques, et celles qu'un recours excessif à la technologie risquerait de dénaturer »[1325].

D'ailleurs, nombre d'entre eux réfléchissent depuis quelques années à la meilleure façon de tirer parti de ses compétences[1326]. Partant du constat que si le code informatique ne peut pas encore se substituer au code juridique et à la fonction notariale en particulier, il est toutefois capable de s'intégrer et de s'investir en tant que nouvel outil au service du « notaire 2.0 »[1327], ce qui exigera en outre une collaboration étroite entre juristes et programmeurs.

B. Le projet d'un outil au service de l'authenticité

175. Le projet d'un notaire 2.0 : optimiser la sécurité et l'efficacité de la mission du notaire par le biais de la *blockchain*. Les derniers travaux des notaires tendent à la fois vers l'appropriation et l'adaptation de la technologie pour une optimisation des tâches notariales. Le Conseil supérieur du notariat (CSN), en collaboration avec les *start-ups* Belem et Hyperledger Fabric, ont travaillé sur une *proof of concept* (POC) ayant pour objectif d' « assurer la pérennité et la circulation [des copies authentiques électroniques

financiers et devises". Son amendement porte en réalité un bouleversement non contrôlé de notre système de droit, en visant spécifiquement votre profession. »

[1323] STREIFF (Vivien), « Blockchain et authenticité : pour copie non certifiée conforme », art. cit., *loc. cit.*

[1324] JULIENNE (Maxime), art. cit., n° 14.

[1325] *Ibid.*, n° 3.

[1326] Notaires de France, « Propriété immobilière : entre progrès et confiance », Compte-rendu des travaux du 112e Congrès des notaires de France [en ligne], Nantes, 5-8 juin 2016, https://www.congresdesnotaires.fr/media/uploads/compte_rendu_complet_relu_version_finale_mise_en_ligne.pdf. – BERBAIN (Côme), art. cit., p. 9.

[1327] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., n° 17.

et copies exécutoires électroniques], en toute sécurité »[1328] entre les multiples acteurs du domaine afin de déployer des nouvelles offres de services numériques à la clientèle des notaires[1329].

176. L'immuabilité des *blockchains* au service de la pérennité des actes notariés. Le projet du CSN propose de mettre à disposition de la profession, ainsi qu'aux huissiers et aux banquiers, un registre notarial distribué par le biais d'une *blockchain*. La fonction *ledger* de la technologie peut en effet permettre aux officiers publics de bénéficier de ses facultés en termes de rapidité et de sécurité. Un collaborateur indique que, « passés par la *blockchain*, les documents pourront être annexés à des actes authentiques de manière plus sereine et certaine, leur intégrité étant vérifiée depuis leur réception jusqu'à leur intégration dans la *blockchain* »[1330]. De plus, alors qu'enregistrer, par exemple, au registre foncier un bien peut nécessiter quelques mois, avec un registre notarial accessible *via* une chaîne de blocs il ne s'agirait de patienter, au plus, que quelques minutes[1331]. À l'image du dépôt au rang des minutes, les parties pourraient instantanément déposer leur acte au rang des inscriptions du notaire afin qu'il fasse l'objet d'un contrôle par l'officier, tant sur la forme que sur le fond, avant de se voir accorder l'authenticité[1332]. À cette occasion, le notaire pourrait faire usage du système de signature électronique fourni par le protocole et ainsi bénéficier de ses multiples avantages, notamment en termes de rapidité, de sécurité, de coût, mais aussi et surtout d'intégrité et de pérennité puisque l'un des défauts des dispositifs électroniques actuels réside dans leur durée de vie limitée, laquelle est, en règle générale, de deux ans[1333]. Alors que la solution aux impasses techniques actuelles de la création d'un « document électronique unique », « non reproductible »[1334] et par

---

[1328] MARRAUD DES GROTTES (Gaëlle), « Blockchain : POC en vue pour les notaires… », *Wolters Kluwer* [en ligne], 11 sept. 2018, https://www.actualitesdudroit.fr/browse/techdroit/blockchain/15632/blockchain-poc-en-vue-pour-les-notaires.

[1329] MARRAUD DES GROTTES (Gaëlle), « Stéphane Adler, vice-président de la Chambre des notaires de Paris : "Notre volonté est d'être une autorité de confiance numérique notariale pour la fourniture de services blockchain" », *Wolters Kluwer* [en ligne], 16 juill. 2020, https://www.actualitesdudroit.fr/browse/tech-droit/blockchain/28301/stephane-adler-vice-president-de-la-chambre-des-notaires-de-paris-notre-volonte-est-d-etre-une-autorite-de-confiance-numerique-notariale-pour-la-fourniture-de-services-blockchain. V. également, Notaires du Grand Paris, « Présentation de la BlockChain Notariale. Dossier de Presse », préc.

[1330] « Le notariat à l'heure de la blockchain », *AJ fam*. 2018, p. 260.

[1331] MANAS (Arnaud), BOSC-HADDAD (Yoram), art. cit., p. 105.

[1332] MOURALIS (Jean-Louis), *op. cit.*, n° 42.

[1333] MARRAUD DES GROTTES (Gaëlle), « Blockchain : POC en vue pour les notaires… », art. cit. : « aujourd'hui, un notaire peut faire un acte authentique électronique, mais quand il délivre la copie de l'acte, pour qu'elle soit authentique, il doit imprimer l'acte, puis placer un sceau et une signature. Le point de faiblesse vient précisément de la signature numérique : le cachet de signature électronique a une durée de vie limitée : au bout de 2 ans, Adobe Acrobat Reader signale que la signature est valide, mais expirée ».

[1334] FAVIER (Jacques), TAKKAL BATAILLE (Adli), *Bitcoin. La monnaie acéphale*, éd. CNRS, coll. Économie Droit, 2017, pp. 1 et s. – Sur la distinction entre Internet et *blockchains* concernant la création de biens électroniques non reproductibles, *supra* n° 6.

conséquent non falsifiable, apparaît au travers de la technique du hachage de la technologie des blocs, un auteur constate que « le meilleur moyen de pérenniser un document dans le temps et surtout d'en garantir qui en est le détenteur légitime à un instant "t", c'est d'utiliser une *blockchain* »[1335]. Il faudra simplement pour cela que la signature obtenue *via blockchain* remplisse les conditions d'intégrité de l'art. 1379 du C. civ. et de son décret d'application[1336] concernant les copies exécutoires ou authentiques d'un écrit authentique. La fiabilité du procédé de signature des *blockchains* pourrait également contribuer à faciliter et à simplifier les formalités d'apostille permettant d'attester l'intégrité d'un acte notarié destiné à une autorité étrangère[1337], et éventuellement à réduire les coûts communément supportés[1338]. D'une manière générale, le mécanisme de signature et d'inscription avec obtention d'un *hash via* la chaîne de blocs peut se révéler être à la fois un moyen de limiter les risques d'altération du contenu des actes notariés[1339] et d'accélérer la procédure de signature de l'acte en ce sens que la signature de la *blockchain* suffirait à sceller chaque feuillet de l'acte de manière à le rendre infalsifiable. D'ailleurs, conscient du caractère fastidieux de l'opération en fonction des actes à instrumenter, le législateur avait déjà tenté en 1971 d'alléger cette obligation de paraphe en exemptant les parties à un acte dont « les feuilles […] sont, lors de la signature par les parties, réunies par un procédé empêchant toute substitution ou addition »[1340]. Seulement, le législateur comme le notaire n'avaient pas encore trouvé le moyen d'y parvenir[1341]. En enregistrant sur la *blockchain* un acte à authentifier, celui-ci serait, dans son intégralité et quel que soit son nombre de feuilles, immuable, à l'instar d'un acte « rédigé sur une feuille unique » et lequel « se trouve authentifié par la signature finale du notaire apposée à côté de celles des parties ». Si bien que le paraphe serait jugé inutile[1342].

[1335] MARRAUD DES GROTTES (Gaëlle), « Blockchain : POC en vue pour les notaires… », art. cit.
[1336] Décr. n° 2016-1673, 5 déc. 2016, relatif à la fiabilité des copies et pris pour l'application de l'article 1379 du code civil, *JORF* n° 0283, 6 déc. 2016, texte n° 61. – Pour une étude détaillée sur la question de la validité de la signature électronique *via blockchain*, *supra* n°s 95 et s.
[1337] Décr. n° 65-67, 22 janv. 1965, portant publication de la convention du 5 octobre 1961 supprimant l'exigence de la légalisation des actes publics étrangers, *JORF* n° 0023, 28 janv. 1965.
[1338] À titre d'indication, le prix pour une légalisation à la demande d'un particulier est de 10 euros par document (v., https://www.service-public.fr/particuliers/vosdroits/F1400).
[1339] Décr. n° 2005-973, 10 août 2005, modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires, *JORF* n° 186, 11 août 2005, texte n° 34, art. 14, 4°.
[1340] Décr. n°71-941, 26 nov. 1971, relatif aux actes établis par les notaires, *JORF*, 3 déc. 1971, p. 11795, art. 34, 3°, modifié par le Décr. n° 2005-973, 10 août 2005, modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires, *JORF* n° 186, 11 août 2005, p. 13096, texte n° 34, art. 4.
[1341] MOURALIS (Jean-Louis), *op. cit*., n° 101.
[1342] Cass. Civ. 1ère, 20 mars 1973, *Bull. civ*. I, n° 108.

177. La décentralisation des *blockchains* au service de l'exploitation des données et de la circulation des actes notariés. Le projet permettrait, à partir d'une « *blockchain* de consortium »[1343], c'est-à-dire fondée sur un protocole géré que par un nombre déterminé de nœuds[1344], de répartir la tenue des registres décentralisés entre l'ensemble des offices notariaux, et de faciliter et de sécuriser les échanges de documents[1345] et ce, en conformité avec les dispositions du décret du 26 novembre 1971 régissant la transmission des copies d'actes authentiques par voie électronique[1346]. En exigeant, de surcroît, une interopérabilité des systèmes de communication d'informations mis en œuvre entre tous les notaires, mais également entre notaires et organismes auxquels ils doivent transmettre des données[1347] par le biais d'un réseau VPN dédié[1348], la *blockchain* propose de simplifier l'instrumentation et le contrôle de l'intégrité des actes[1349]. Il peut d'ailleurs s'agir d'actes établis sur support papier et numérisés à l'identique sur support électronique[1350], ou au contraire d'actes établis par voie électronique et reproduits sur support papier, accompagnés de la signature électronique du notaire et l'empreinte du sceau, de la mention de la date et de la conformité de la copie exécutoire ou de la copie authentique avec l'original[1351]. En associant les qualités de fiabilité et d'intégrité de la technologie à celles de l'authentique professionnel de la confiance, l'effectivité de la fonction notariale serait ainsi renforcée.

Par ailleurs, la décentralisation de la *blockchain*, l'accessibilité de son *ledger* et son dispositif de signature électronique pourraient simplifier, voire rendre possible, l'exécution de certaines obligations légales, en particulier celles requérant l'intervention et la signature d'un second notaire[1352]. Bien qu'il en aille ainsi pour un nombre limitativement énuméré de situations, telles qu'en matière de testament authentique

---

[1343] Pour une définition plus complète de la *blockchain* de consortium, *infra* n° 262.
[1344] Les mineurs de la *blockchain* notariale sont des offices notariaux localisés en Ile-de-France. – V., MARRAUD DES GROTTES (Gaëlle), « Stéphane Adler, vice-président de la Chambre des notaires de Paris : "Notre volonté est d'être une autorité de confiance numérique notariale pour la fourniture de services blockchain" », art. cit.
[1345] COIFFARD (Didier), art. cit., n° 147.
[1346] Décr. n° 71-941, préc., art. 36-37 : « Les copies exécutoires et les copies authentiques peuvent être transmises par voie électronique dans des conditions garantissant l'intégrité de l'acte, la confidentialité de la transmission, l'identité de l'expéditeur et celle du destinataire. »
[1347] Décr. n° 71-941, préc., modifié par le Décr. n° 2005-973, préc., art. 16, 2°.
[1348] MARRAUD DES GROTTES (Gaëlle), « Stéphane Adler, vice-président de la Chambre des notaires de Paris : "Notre volonté est d'être une autorité de confiance numérique notariale pour la fourniture de services blockchain" », art. cit.
[1349] Décr. n° 71-941, préc., modifié par le Décr. n° 2005-973, préc., art. 16, 1°.
[1350] *Ibid.*, art. 37.
[1351] *Ibid.*, art. 34, 4°, 36.
[1352] JULIENNE (Maxime), art. cit., n° 5.

électronique[1353] ou encore de révocation de testament[1354], recevoir et signer un tel acte sous forme dématérialisée demeurait jusqu'à présent impossible pour le système exploité[1355]. La *blockchain* pourrait y remédier. Un auteur constate d'ailleurs que, « bien que la profession se montre encore prudente sur ces questions, il est clair que l'évolution se fera dans le sens d'une dématérialisation accrue »[1356]. En témoigne la création de la possibilité d'émettre une procuration notariée à distance depuis le décret n° 2020-1422 du 20 novembre 2020 ayant pris en considération les conséquences de la crise sanitaire de 2020[1357].

Au-delà de faciliter la collaboration interprofessionnelle, telle que l'envisage et l'encourage d'ailleurs la nouvelle présidence du Conseil des notariats de l'Union européenne (CNUE)[1358], la possibilité de tracer les mouvements des documents notariés, signés et inscris au sein de transactions grâce à des empreintes numériques uniques et infalsifiables, puis transmis entre les acteurs – clients, notaires, banques, huissiers, etc. – représente un avantage décisif pour la fonction.

178. La mise à disposition de services de confiance reposant sur la *blockchain* notariale : vers la dématérialisation de la relation client. L' « acte fondateur » de la *blockchain* notariale, consistant en la signature le 16 juin 2020 de la « Politique de confiance de la Blockchain Notariale (BCN) » par les présidents des Chambres des notaires d'Ile-de-France[1359], incarne son déploiement officiel au sein des offices notariaux et sa prochaine mise en application auprès de leurs clientèles. Devant prendre la forme d'applications métiers ou clients, le dispositif devrait permettre la remise de copies exécutoires numériques, la consultation et le transfert de documents entre les clients et les notaires, mais aussi entre individus qui auraient un intérêt à disposer d'un dispositif

[1353] C. civ., art. 971. – V., GRIMALDI (Michel), « Le testament et le cyber-notaire », *in Mélanges Jérôme Huet*, éd. Lextenso, 2018, p. 211, n° 3.
[1354] Loi 25 ventôse an XI, préc., art. 9, 2°.
[1355] Le système de signature électronique exploité par les officiers publics repose sur un certificat de signature qualifié, lequel associe, d'une part, une clé Real et, d'autre part, un code personnel délivré aux notaires [JULIENNE (Maxime), art. cit., *loc. cit.*]. Pour plus de précisions sur la Clé Real, v., CSN, « Conditions générales d'utilisation de la Clé Real et des certificats associés », *Notaires de France* [en ligne], Version 2.3, 6 juin 2019, https://www.preuve-electronique.org/ListeRevocations/cgu_fr-1.14.pdf, Accueil > Conditions Générales > Clé REAL.
[1356] JULIENNE (Maxime), art. cit., n° 6.
[1357] Décr. n° 2020-1422, 20 nov. 2020, instaurant la procuration notariée à distance, *JORF* n° 0282, 21 nov. 2020, texte n° 25. – Sur le sujet, v. également, BOISMAIN (Corinne), « Quelques réflexions sur les contrats intelligents (smarts contracts) », *LPA* 1 mars 2021, n° 158q0, p. 6.
[1358] « Nouvelle présidence du CNUE », *Defrénois* 28 janv. 2021, n° 168a4, p. 11.
[1359] « Les Notaires du Grand Paris lancent la "Blockchain Notariale" », *Defrénois* 16 juill. 2020, n° DEF161W1, p. 11. – V. également, « Notariat », *JCl. Roulois*, fasc. 7300, n° 1.

de sécurisation de preuves[1360]. Toute demande visant l'utilisation de la BCN pour le développement d'une application spécifique sera analysée par le comité de gouvernance du dispositif (« Autorité de Confiance de la Blockchain Notariale »), composé des membres signataires de la Politique de confiance, et secondé par un comité stratégique composé de notaires et d'experts. Ces applications seront tenues également de proposer de conserver les documents constituant des preuves, dont la *blockchain* ne peut garder qu'une preuve cryptographique certifiant de leur contenu, de leur origine et de leur date. En pratique, ces documents seront placés dans un coffre-fort électronique dédié, que ces preuves soient destinées à constituer des documentations ou à être transmises à d'autres personnes ou organismes[1361]. La seconde étape du dispositif sera de délivrer des identités numériques et de constituer un registre de preuves de l'identification des clients[1362].

Ce type de système pourrait par la suite se déployer à plus grande échelle et être investie par des services publics, des entreprises, en France, en UE ou même dans le monde entier afin de s'assurer de l'intégrité d'un document reçu ou à l'inverse de la transmission d'un document à d'autres personnes. L'origine et la fiabilité pourront être contrôlées, de manière transparente et instantanée, ce qui créera un environnement de confiance, de sûreté et d'affaires finalement.

179. L'adoption à l'international de la preuve authentique inscrite sur *blockchain* : état des lieux. En remettant en cause l'utilité des tiers de confiance ancestraux, la *blockchain* les a incités à se surpasser et à investir la technologie jusqu'à opérer un redéploiement de leurs fonctions[1363]. Que ce soit en principal avec assistance humaine ou en accessoire, il ne fait aucun doute que la technologie *blockchain* dispose d'importantes capacités en matière de preuves qu'il est nécessaire de s'approprier. Potentiel probatoire que d'autres États comme la Suisse (ville de Zoug), le Honduras, le Ghana, la Géorgie[1364], la Suède et l'Estonie ont, à plus ou moins grande échelle, d'ores et déjà déployé[1365].

[1360] MARRAUD DES GROTTES (Gaëlle), « Stéphane Adler, vice-président de la Chambre des notaires de Paris : "Notre volonté est d'être une autorité de confiance numérique notariale pour la fourniture de services blockchain" », art. cit.
[1361] *Id.*
[1362] « Les Notaires du Grand Paris lancent la "Blockchain Notariale" », art. cit.
[1363] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., *loc. cit.*
[1364] Sur les systèmes décentralisés de « wiki-cadastres » honduriens, ghanéens et géorgiens, *supra* n° 8.
[1365] Rapp. AN n° 1092, rapp. Sénat n° 584, 20 juin 2018, Comprendre les blockchains : fonctionnement et enjeux de ces nouvelles technologies, présenté par Valéria FAURE-MUNTIAN, Claude DE GANAY, et Ronan LE GLEUT, au nom de l'office parlementaire d'évaluation des choix scientifiques et technologiques.

L'Estonie est en effet considérée comme le précurseur en Europe de la technologie *blockchain* en matière de fourniture de services public. Depuis le 1er janvier 2015, *Bitnation* met à disposition des Estoniens et résidents du monde un service d'inscription notarié des titres de propriété et des contrats de mariage sur *blockchain* en vertu du e-*Residency Program*[1366].

Alors que l'Estonie s'interroge actuellement sur l'intérêt de l'utilisation de la technologie pour les transactions immobilières[1367], depuis le début de l'année 2019 le registre national suédois des biens immobiliers, *Lantmäteriet*, utilise officiellement la *blockchain* pour enregistrer des transactions foncières et immobilières[1368]. Il est notamment question d'inscrire des contrats de vente et des hypothèques immobilières, sans qu'il soit nécessaire que les parties soient présentes[1369]. De plus, l'ensemble de ces transactions s'exécute à partir de *smart contracts* vérifiés par la *blockchain*[1370]. Grâce à la technologie de la chaîne de blocs, la Suède espère réduire de plusieurs mois à quelques jours le délai entre la conclusion d'un contrat de vente d'un immeuble et l'enregistrement de sa propriété. Outre la rapidité de traitement de la chaîne, *Lantmäteriet* se fie à ses multiples autres performances pour, d'une part, réduire les frais attachés à ce type de transactions et, d'autre part, simplifier et sécuriser les transferts de titres fournis, de manière inédite, en originaux électroniques[1371]. Chacune des parties concernées par la transaction, c'est-à-dire l'acheteur, le vendeur, l'agent immobilier, la banque de l'acheteur et le registre foncier, détient sa propre identité numérique sur la chaîne par le biais d'identifiants. Par conséquent, une seule application est nécessaire pour visualiser les documents et informations associés, vérifier le cours des étapes du processus, et enfin envoyer et signer en toute sécurité les documents officiels.

[1366] LYON (Nina), « Estonian e-Residency and BitNation launch new Public Notary in "Blockchain Jurisdiction" », *Cointelegraph* [online], 30 Nov. 2015, https://cointelegraph.com/news/estonian-e-residency-and-bitnation-launch-new-public-notary-in-blockchain-jurisdiction. – V. également, SULLIVAN (Clare), BURGER (Éric), « E-residency and blockchain », Elsevier 2017 [en ligne], n° 33, pp. 470-480, http://www.arifsari.net/isma500course/project/19.pdf.

[1367] RASTORGUJEVA (Jelizaveta), « NJORD Estonia: Real estate transaction using blockchain technology », *NJORD Lawfirm* [online], 25 May 2018, https://www.njordlaw.com/njord-estonia-real-estate-transaction-using-block-chain-technology/.

[1368] Lantmäteriet, Landshypotek Bank, SBAB, Telia company, ChromaWay, Kairos Future, « The Land Registry in the blockchain – testbed », Kairos Future [online], Mar. 2017, https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf.

[1369] Young (Josep), « Sweden Officially Started Using Blockchain to Register Land and Properties », *Cointelepgraph* [online], 6 Jul. 2017, https://cointelegraph.com/news/sweden-officially-started-using-blockchain-to-register-land-and-properties.

[1370] Lantmäteriet, Landshypotek Bank, SBAB, Telia company, ChromaWay, Kairos Future, « The Land Registry in the blockchain – testbed », préc., pp. 45-52.

[1371] *Id.*

180. D'une manière générale, comme le soulignent Arnaud Manas et Yoram Bosc-Haddad, « ignorer le foisonnement créatif (ou, pire, le combattre) serait donc prendre le risque de passer à côté du potentiel élevé d'innovation des briques technologiques de la *blockchain* »[1372]. Ce potentiel tient à la fois à l'automatisation des clauses contractuelles et à la certification des données inscrites. Or, quand bien même la force probante de la *blockchain* ne serait pas admise par le monde juridique, cette circonstance n'empêche, en principe, pas les cocontractants qui désireraient l'utiliser – que ce soit pour fixer les modalités d'exécution ou pour constituer une preuve de leurs engagements respectifs – d'insérer dans leur contrat une clause stipulant leur recours à un *smart contract* ou à un registre de preuve de la technologie *blockchain*[1373]. En effet, une telle application demeure attachée au domaine contractuel et à ce que souhaitent mettre en œuvre les parties.

Toutefois, outre la question de l'utilité de la technologie qui peut parfois se poser dans certains domaines[1374] et à laquelle il est nécessaire de répondre en procédant à un calcul coûts/avantages[1375], d'autres éléments viennent entraver l'adoption de la *blockchain* dans les rapports contractuels. Toute technologie, de surcroît émergente, s'appliquant au domaine contractuel et dont le produit est censé matérialiser une « sphère de confiance » dans les relations entre les individus, ne peut se déployer pleinement si les parties n'ont pas la certitude de pouvoir s'y fier. Plus encore, pour passer du déploiement à l'acceptation sociétale et à l'utilisation à grande échelle de la technologie, il appartient à ses concepteurs d'apporter aux utilisateurs une valeur ajoutée par rapport au système déjà existant. Autrement dit, il s'agit de leur fournir une valable raison d'abandonner un système, certes critiquable mais malgré tout efficace, en faveur d'une nouveauté dont l'avenir est incertain. De ce constat s'élève un certain nombre de difficultés qu'il convient d'analyser.

[1372] MANAS (Arnaud), BOSC-HADDAD (Yoram), art. cit., p. 105.
[1373] BARREAU (Catherine), « La régulation des smart contracts et les smart contracts des régulateurs », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 76.
[1374] Tels que pour les élections ou les diplômes universitaires, notamment, en ce sens que des logiciels assurent d'ores et déjà les missions attendues [v., VERBIEST (Thibault), « Blockchain : une révolution juridique ? », *RLDA* 2017/9, n° 129].
[1375] BARREAU (Catherine), art. cit., p. 75.

PARTIE 2

LES SPÉCIFICITÉS DE LA *BLOCKCHAIN* EN TANT QUE POTENTIELS FREINS À L'INSTITUTION D'UNE CONFIANCE ALGORITHMIQUE : DES RÉSISTANCES COMPLIQUANT L'APPLICATION DES EXIGENCES JURIDIQUES ACTUELLES

181. Le plein essor de la *blockchain* se voit assiégé au milieu de difficultés d'adaptation entre le droit positif et les particularismes et limites inhérentes à son propre fonctionnement. Derrière les apparences de facilité, la technologie crée, en substance, d'elle-même ou à travers l'utilisation qui en est faite, d'une part, des contradictions avec un certain nombre de règles de droit (TITRE 1) et, d'autre part, des problèmes de fiabilité (TITRE 2). Dans ces circonstances, et en particulier en l'absence d'une complète adaptation technologique aux exigences juridiques de la société, le risque est de voir s'installer un manque de confiance des potentiels utilisateurs et, progressivement, un sentiment d'insécurité numérique généralisé. Il convient donc d'identifier et d'évaluer précisément l'hétérogénéité de ces deux systèmes pour juger de l'éventualité d'une interférence bénéfique à chacun.

TITRE 1. Incohérences entre *blockchain* et droit : un besoin d'adaptation

182. Bien qu'ils soient intimement liés les uns aux autres, il convient de mettre en évidence deux principaux attributs de la *blockchain*, à savoir, l'immuabilité et la décentralisation. Si les techniques de hachage généralement utilisées par les *blockchains* permettent de rendre techniquement impossible toute modification, suppression, ou ajout d'information au sein du registre de la technologie par l'obtention d'un *hash* inaltérable[1376], c'est l'organisation en Peer-to-Peer (P2P), soit de pair à pair, du protocole qui rend impossible toute intervention tierce et encore moins centrale[1377]. Chacune de ces caractéristiques représente l'essence-même de la technologie, ses capacités, et établit de surcroît la distinction entre elle et les autres produits du numérique. Cependant, leur potentiel se heurte à leurs propres limites qui apparaissent contradictoires avec l'application d'un certain nombre de dispositions du droit actuel. En effet, alors que la première caractéristique de la *blockchain*, qui permet en principe d'empêcher quiconque de prendre le contrôle de la chaîne, s'avère, dans l'état de l'art, tout aussi difficile à maîtriser pour les parties à un contrat inscrit (Chapitre 1), la seconde rend délicate l'intervention pourtant essentielle du juge étatique (Chapitre 2). Or, si aucune contremesure n'est prise, ces circonstances sont vouées à perturber l'intégration de la technologie dans la société contemporaine.

[1376] Pour plus de précisions sur le procédé, *supra* n°s 104-105.
[1377] Pour plus de précisions, *supra* n°s 6, 145.

Chapitre 1. L'immuabilité, une difficile maîtrise des parties

183. Jusqu'à présent le caractère immuable de la *blockchain* s'est toujours révélé être un réel atout, en particulier en matière de sécurité contractuelle. Seulement, comme le souligne Edmond About, « toute médaille a son revers, et il est bien rare qu'une vertu ne soit pas doublée d'un vice »[1378]. Le vice attaché à l'inaltérabilité apparaît dans l'extrême rigidité du système, qui crée alors un mécanisme des plus intransigeants. En effet, d'une part, celui-ci semble rendre éternellement publiques les données, potentiellement personnelles, inscrites sur la chaîne. Or, cette situation n'est pas sans soulever de difficultés vis-à-vis de la conformité à la législation protectrice des droits des personnes physiques à l'égard du traitement de leurs données, en particulier à l'égard du droit des individus à obtenir l'effacement des données les concernant. D'autre part, son caractère « inarrêtable », conduisant le *smart contract* à poursuivre son exécution jusqu'à ce qu'il trouve application conformément à ses stipulations contractuelles, sans modification ou annulation en cours d'exécution[1379], va à l'encontre de certains principes juridiques, notamment ceux gouvernés par la liberté contractuelle. L'art. 1er de la loi Informatique et libertés du 6 janvier 1978 souligne d'ailleurs que « l'informatique doit être au service de chaque citoyen [et] ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques »[1380].

Il convient donc de confronter les principes d'inaltérabilité et d'exécution intégrale des inscriptions, non seulement au Règlement Général sur la Protection des Données (RGPD)[1381] (Section 1), mais également à la pratique des relations contractuelles (Section 2).

[1378] ABOUT (Edmond), *La Grèce contemporaine*, éd. L. Hachette et Cie, 5e édition, 1863, p. 57.
[1379] Sur le principe d'exécution intégrale, *supra* n° 29.
[1380] L. n° 78-17, 6 janv. 1978, relative à l'informatique, aux fichiers et aux libertés, *JORF*, 7 janv. 1978, p. 227, modifiée par L. n° 2018-493, 20 juin 2018, relative à la protection des données personnelles, *JORF* n° 0141, 21 juin 2018, texte n° 1.
[1381] Règl. (UE) n° 2016/679 du Parlement européen et du Conseil, 27 avr. 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (dit « Règlement Général sur la Protection des Données », ou RGPD), *JOUE* L 119/1, 4 mai 2016, pp. 1-88.

Section 1. Le principe d'inaltérabilité des inscriptions face au RGPD

184. D'après le dicton *geek,* « la *blockchain* n'oublie rien ». Cependant, avec le temps, elle est censée oublier certains éléments conformément aux règles en vigueur en matière de responsabilité en ce qui concerne le traitement de données à caractère personnel, et notamment vis-à-vis du nouveau règlement de l'UE. Associée à la problématique de l'identification des utilisateurs sur une *blockchain*[1382], cette nouvelle hypothèse suggère qu'il faille procéder à une analyse élargie quant à la cohérence entre les propriétés et les mécanismes propres à la *blockchain* et la législation en vigueur, en particulier concernant la transparence des blocs de la chaîne qui implique que les données inscrites soient rendues publiques (§ 1). Cependant, il s'agira d'évaluer la portée des contradictions mises en évidence afin de ne pas ériger ce qui pourrait vainement représenter des freins à l'innovation (§ 2).

§ 1. Entre transparence des blocs et transparence des données

185. Partant du postulat que la *blockchain* est avant tout publique, il s'agit de définir la nature des données inscrites et utilisées, d'autant plus que certaines d'entre elles peuvent parfois se révéler être d'une extrême sensibilité. Il convient donc de déterminer quelles données privées sont susceptibles d'être présentes sur la chaîne de blocs (A) et si celles-ci entrent dans le champ d'application de la notion de « données à caractère personnel » du RGPD (B).

A. Étendue des données privées présentes sur la chaîne

186. Protection des données à caractère personnel *versus* traitement de données réputées « anonymes ». Depuis le 20 juin 2018, la législation française s'est alignée sur la réglementation européenne en matière de « traitements automatisés en tout ou partie de données à caractère personnel, ainsi [que de] traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers »[1383]. À l'exception des fichiers ne contenant que des coordonnées d'entreprises et des traitements mis en

[1382] *Supra* n° 121 et s., notamment n° 123.
[1383] Règl. (UE) n° 2016/679, préc.

œuvre pour l'exercice d'activités exclusivement personnelles[1384], domestiques[1385], ou utilisant des données irrémédiablement anonymisées[1386], les dispositions européennes s'inscrivent dans une dynamique visant à renforcer le contrôle des citoyens sur l'exploitation des données les concernant. Pour cela, elles s'articulent autour d'un triptyque fondé sur la responsabilisation des acteurs, la confiance des citoyens et la transparence des traitements.

La *blockchain* a essentiellement été établie, elle aussi, sur des objectifs de transparence et de confiance. La mise en œuvre de la technologie repose sur une intention disruptive pour laquelle la publicité des transactions représente la sécurité du système, si bien qu'elle encourage le recours à l' « anonymat » pour protéger ses utilisateurs[1387]. Le but originel de la *blockchain* n'a donc jamais été de recueillir des informations sur ses utilisateurs. Au contraire, l'écosystème, et en particulier celui de *Bitcoin*, a institué une politique du secret[1388], qui a d'ailleurs été reprise par nombre de protocoles de *blockchains* actuelles. L'avantage recherché dans la technologie était de pouvoir répertorier des faits, et en particulier financiers, à l'instar d'un registre capable de garder automatiquement une trace indélébile des transactions effectuées entre ses utilisateurs, sans jamais demander leurs noms. Autrement dit, sa raison d'être réside dans le service qu'elle est capable de rendre et non dans les données qu'elle est susceptible de collecter, à la différence, par exemple, des *cookies* informatiques[1389]. Étant donné qu'aucune

[1384] L. n° 2018-493, 20 juin 2018, relative à la protection des données personnelles, portant modification de la L. n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JORF*, 21 juin 2018, art. 2, al. 1er.

[1385] Règl. (UE) n° 2016/679, préc., art. 2, § 2, c).

[1386] *Ibid*., considérant n° 26.

[1387] Satoshi Nakamoto avait en effet indiqué que contrairement aux modèles d'organisation traditionnels à l'instar de celui des banques qui « limitent l'accès à l'information aux parties concernées ainsi qu'au tiers de confiance », *Bitcoin* rend chaque transaction accessible au public afin d'en assurer la sécurité et la pérennité. Afin de garantir la confidentialité du système, *Bitcoin* est programmé de sorte à « couper le flux d'information à un autre endroit », c'est-à-dire entre les identités et les transactions, ce qui se matérialise sous la forme de clés publiques anonymes. [« *The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous*. » [notre trad.], NAKAMOTO (Satoshi), « Bitcoin: A Peer-to-Peer Electronic Cash System », [online], Oct. 2008, p. 6, https://bitcoin.org/bitcoin.pdf].

[1388] V. sur le sujet, BLONDEAU (Alison), « Le juge civil face au secret entourant le système de clé privée sur blockchain », *in* NEVEJANS (Nathalie) (dir.), *Données et technologies numériques. Approches juridique, scientifique et éthique*, éd. mare & martin, coll. Droit & Science politique, 2021, pp. 155-164.

[1389] Le « *cookie* » est défini par la CNIL comme constituant « une suite d'informations, généralement de petite taille et identifié par un nom, qui peut être transmis [au] navigateur par un site web sur lequel [l'internaute se connecte]. [Le] navigateur web le conservera pendant une certaine durée, et le renverra au serveur web chaque fois que [l'utilisateur s'y reconnectera]. Les *cookies* ont de multiples usages : ils peuvent servir à mémoriser [un] identifiant client auprès d'un site marchand, le contenu courant [d'un] panier d'achat, un identifiant permettant de tracer [la] navigation pour des finalités statistiques ou publicitaires, etc. » [CNIL [en ligne], v° Cookie, https://www.cnil.fr/fr/definition/cookie]. POILVÉ (Benjamin), « Une petite histoire du cookie », *LINC* [en ligne], 14 janv. 2020, https://linc.cnil.fr/fr/une-petite-histoire-du-cookie : « À l'origine, le *World Wide Web* imaginé par Tim Berners-Lee était "sans état" :

information n'est expressément dévoilée publiquement, *Bitcoin* est souvent présenté comme étant un protocole où « l'anonymat » est garanti[1390]. De plus, l'utilisation d'un système asymétrique permet la génération d'empreintes cryptographiques à sens unique. Il est donc impossible d'en déduire l'information originelle, laquelle détient potentiellement l'identité de l'utilisateur[1391], en admettant que ce dernier en ait de lui-même informé le système, ce qui n'est actuellement pas une exigence préalable à l'inscription sur la chaîne.

Néanmoins, force est de relever des diverses évolutions de la technologie que son déploiement au-delà du secteur financier avec les crypto-monnaies a inévitablement modifié la teneur de ses blocs, si bien que des données à caractère privé sont susceptibles d'y figurer, y compris « en clair », c'est-à-dire publiquement visible[1392].

187. État des lieux du contenu des blocs et des données inscrites en fonction de l'utilisation de la *blockchain*. Une donnée anonyme au sens du règlement suppose que toute identification de la personne concernée soit rendue impossible, et de manière irréversible[1393]. Certaines *blockchains*, en particulier de crypto-monnaies, organisent une confidentialité permanente. *Monero*, par exemple, utilise des données exclusivement anonymisées par le biais d'un système de transactions masquant les adresses publiques d'envoi et de réception, ainsi que les montants transmis[1394]. La réglementation sur les données à caractère personnel n'a donc, en principe, pas vocation à s'appliquer, au contraire de la Réglementation du 14 novembre 2018 établissant un cadre applicable au

chaque requête *via* le protocole http était indépendante, sans possibilité pour le serveur de lier deux requêtes successives venant du même système et donc de garder en mémoire des informations sur un utilisateur. […] Du fait de l'absence d'état, chaque navigation vers une nouvelle page provoque l'oubli de toutes les actions précédentes ». Le cookie propose aujourd'hui « de stocker un "état" dans un nouvel objet, […] "Persistent Client State HTTP Cookies" ou cookie, pour faire court [et permet] au serveur de transmettre un fichier texte au client, celui-ci lui renvoyant ce même fichier à chaque requête subséquente, permettant ainsi d'identifier l'utilisateur et donc, par exemple, de se rappeler du contenu de son panier au niveau du serveur ».

[1390] PAVEL (Ilarion), « La blockchain : Les défis de son implémentation », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 23.

[1391] GUILHAUDIS (Élise), « Comprendre la blockchain à travers l'étude d'un cas pratique : le covoiturage "Blockcar" », *RLDI* 2017/12, nº 143, p. 12.

[1392] POPPE (Morgane), « Quelle relation entre la protection des données à caractère personnel et la blockchain ? », *in* « Dossier : Blockchain, une révolution juridique ? », *RLDA* 2017/9, n° 129. – Sur les informations disponibles en clair concernant chacun de ces éléments, v., notamment, G. (Thomas), « Tutorial : comment lire un explorateur de blockchain Bitcoin ? », *Journal du Coin* [en ligne], 11 mai 2019, https://journalducoin.com/bitcoin/actualites-bitcoin/comment-lire-un-explorateur-de-blockchain/.

[1393] Sur la distinction entre les techniques utilisées pour garantir la confidentialité et l'intégrité des données, à savoir, les techniques réversibles (pseudonymisation et chiffrement) ou irréversibles (anonymisation), v., JOMNI (Adel), « Le RGPD : un atout ou un frein pour la cybersécurité ? », *D. IP/IT* 2019, n° 6, p. 352.

[1394] V., https://web.getmonero.org/get-started/what-is-monero/, Commencer > Qu'est-ce que Monero (XMR) ?

libre flux des données à caractère non personnel dans l'UE[1395]. En revanche, elle s'impose dès lors que les *blockchains* renferment des informations personnelles, notamment sur les utilisateurs. En principe, les quelques éléments inscrits sur une *blockchain* de type *Bitcoin* ne devraient pas permettre cette identification. Mais, les *blockchains* financières ne sont plus les seules versions du protocole utilisées, ce qui suppose que des données inscrites peuvent donc figurer en clair par le biais d'autres utilisations de la technologie des *blockchains*.

188. État des lieux du contenu des blocs et des données inscrites en fonction de l'utilisation de la *blockchain* : *ledger* et données probantes. Il résulte de l'utilisation de fonctions de hachage (ou *hashing*) l'obtention d'une empreinte inaltérable de toute information numérique constituant un condensé du message signé, sous la forme de chiffres et de lettres dont la longueur est fixe[1396]. Figurent sur la *blockchain* les suites de caractères alphanumériques correspondant aux *hashs* des clés publiques identifiant les utilisateurs « participants »[1397] et les mineurs, les *hashs* des blocs de transactions, ainsi que les montants des opérations. Cette empreinte n'est donc en apparence constituée que de suites aléatoires de chiffres et de lettres. Par exemple, sur *Bitcoin*, les données ne sont pas clairement visibles[1398], excepté le pseudonyme du mineur vainqueur, les adresses de l'expéditeur et du destinataire de la transaction, la valeur de la transaction, la valeur du *header*, la version du bloc, l'empreinte du bloc précédent, le *Merkle Root*, la date, la difficulté et enfin le *nonce*[1399]. Il s'agit d'un ensemble d'informations essentiellement cryptées, paraissant, par elles-mêmes, n'avoir aucune signification. Tel que l'a souligné la CNIL, les adresses publiques sont l'essence du protocole et sont par conséquent indispensables au fonctionnement de la plupart des *blockchains*[1400]. Leur apparition en clair sur la chaîne contribue à leur traçabilité au même titre qu'à la sécurité des opérations qu'elles initient et, par extension, à l'intégrité du protocole. D'autre part, peuvent figurer

[1395] Régl. (UE) n° 2018/1807 du Parlement européen et du Conseil, 14 nov. 2018, établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, *JOUE* L 303, 28 nov. 2018, pp. 59-68.
[1396] Sur les *hashs*, *supra* n° 104.
[1397] La CNIL distingue en effet les « participants », qui bénéficient d'un droit d'écriture par le biais de la faculté à inscrire des transactions, des « mineurs », qui vérifient et valident les transactions afin de constituer les blocs de la *blockchain*, et des « accédants », qui bénéficient pour leur part d'un droit de lecture du contenu disponible en clair [v., CNIL, « Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles ? », *CNIL* [en ligne], 24 sept. 2018, https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles].
[1398] GUILHAUDIS (Élise), art. cit., p. 12.
[1399] Sur le contenu des blocs sur *Bitcoin*, *supra* n° 145.
[1400] CNIL, « Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles ? », art. cit.

des données à caractère personnel concernant ses utilisateurs, voire des données relatives à des personnes extérieures à la chaîne. La CNIL distingue ainsi les données essentielles à la chaîne que constituent les identifiants des participants et des mineurs, des données complémentaires (ou « charge utile ») susceptibles d'entrer dans le champ d'application du RGPD[1401]. C'est par exemple le cas lorsque des protocoles ayant vocation à constituer des preuves d'intégrité et d'antériorité des éléments inscrits peuvent atteindre ou laissent apparaître en clair des indications concernant leurs utilisateurs. En règle générale, l'écosystème conseille de ne rien dévoiler sur la *blockchain*[1402], au risque de rendre ces informations publiques. Cependant, les dissimuler n'est pas toujours aisé.

189. État des lieux du contenu des blocs et des données inscrites en fonction de l'utilisation de la *blockchain* : *smart contract* et données contractuelles. Les informations indiquées par les utilisateurs sont le plus souvent essentielles à la réalisation de ce pour quoi ils ont eu recours à la *blockchain*. Par exemple, il peut s'avérer difficile de contracter sans faire apparaître un certain nombre d'éléments concernant le contrat conclu, bien qu'ils puissent ensuite se révéler sensibles ou, du moins, protégés par des règles impératives. Il en va en particulier ainsi en matière de *smart contract*, programmé pour rendre exécutable les écritures inscrites au sein du *ledger* de la *blockchain*. En effet, hormis les cas d'usages n'étant pas mis à disposition des personnes physiques, à l'instar des *smart contracts* utilisés dans les secteurs du commerce, du transport ou de la logistique qui ont trait, pour l'essentiel, à des informations relatives à des produits[1403], l'algorithme mis en œuvre pour, par exemple, automatiser l'exécution d'un contrat *via blockchain* est susceptible de détenir des informations sur au moins l'une des parties. En matière de contrat d'assurance, un auteur souligne qu' « il est indispensable que l'assureur connaisse le risque, au sens de l'événement, mais également au sens du siège du risque (souhaite-t-on garantir un patrimoine ou une personne ?) »[1404], ce qui suppose que dès la formation du contrat, et donc dès la conception du *smart contract*, celui-ci soit capable d'identifier son souscripteur ainsi que tous les éléments le concernant nécessaires

[1401] CNIL, « Blockchain : Premiers éléments d'analyse de la CNIL », CNIL [en ligne], sept. 2018, p. 8, https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf.
[1402] GUILHAUDIS (Élise), art. cit., p. 12. – BERRY (Philippe), « Données, donnez-moi : La blockchain veut sauver nos identités numériques », *20minutes* [en ligne], 21 juin 2018, https://www.20minutes.fr/arts-stars/culture/2292911-20180621-video-donnees-donnez-blockchain-veut-sauver-identites-numeriques.
[1403] À l'image de celles qui proposent de tracer l'acheminement des marchandises et ainsi prouver le respect des normes sanitaires, de réduire les coûts liés à la multiplication des intermédiaires intervenant dans la chaîne logistique, de prévenir les risques de fraude, ou d'éviter les erreurs d'aiguillages de conteneurs, etc. *Supra* n° 8.
[1404] VINGIANO-VIRICEL (Iolande), « Quel usage de la donnée en assurance ? », *RGDA* sept. 2019, n° 116t7, p. 48.

à la garantie. Si « la donnée est au cœur de la relation contractuelle d'assurance », elle sera par conséquent au cœur du *smart contract* l'automatisant[1405]. De plus, certains termes figureront forcément en clair, que ce soit par nécessité protocolaire, contractuelle, ou pour répondre à des exigences légales.

Bien qu'elles ne soient pas forcément de même nature, qu'il s'agisse d'utiliser la *blockchain* pour ses compétences en tant que *ledger* ou en matière d'auto-exécution des dispositions algorithmo-contractuelles, des données personnelles sont forcément collectées. Leur teneur dépendra simplement du service rendu.

190. État des lieux du contenu des blocs et des données inscrites en fonction de l'utilisation de la *blockchain* : dispositifs de fourniture et de contrôle d'identité. Pour contrer la multitude de techniques actuellement en vigueur permettant aux entreprises, sous prétexte qu'elles pourraient personnaliser les annonces publicitaires[1406], de collecter tous types de données *via* fichiers *cookies*, ou permettant aux pirates[1407] de constituer des fichiers datas afin de les marchander dans des enchères secrètes[1408], parfois même clandestines à 12 dollars la carte de crédit[1409], une solution mettant en œuvre une *blockchain* est en projet dans l'univers de l'informatique. L'objectif de ce dispositif est de lutter contre une disposition à la « *datapocalypse* »[1410], résultat d'un phénomène de collecte et de stockage en continu de données[1411], et de mettre fin à ce qui est parfois

---

[1405] *Id.*

[1406] BERRY (Philippe), « Scandale Facebook-Cambridge Analytica : L'audition de Mark Zuckerberg devant le Congrès », *20minutes* [en ligne], 10 avr. 2018, https://www.20minutes.fr/high-tech/2252671-20180410-video-mark-zuckerberg-va-suer-grosses-gouttes-audition-patron-facebook-suivre-direct-20h15.

[1407] ZAFFAGNI (Marc), « Yahoo! reconnaît que 3 milliards de comptes ont été piratés en 2013 », *Futura Tech* [en ligne], 4 oct. 2017, https://www.futura-sciences.com/tech/actualites/securite-yahoo-reconnait-3-milliards-comptes-ont-ete-pirates-2013-64447/.

[1408] *Id.*

[1409] ZICRY (Laure), *Cyber-risques : Le nouvel enjeu du secteur bancaire et financier*, éd. RB, coll. Les essentiels de la banque et de la finance, 2017, p. 31 : « Selon la société CSID, l'une des sociétés les plus connues aux États-Unis dans la gestion des vols de données massifs, les chiffres clés à connaître sont les suivants : 100 adresses e-mail avec mots de passe : entre 2 et 3 dollars ; Compte *PayPal* et compte *eBay* : entre 5 et 10 dollars ; Carte de crédit avec code pin et date d'expiration : 12 dollars ; Numéro de Sécurité sociale avec date de naissance : 17 dollars. »

[1410] BERRY (Philippe), « Données, donnez-moi : La blockchain veut sauver nos identités numériques », préc.

[1411] L'expression « *datapocalypse* » découle d'un roman de science-fiction de Christopher Keast, mettant en scène une IA qui n'a de cesse d'exploiter et de stocker des données (essentiellement de nature photographiques) qu'elle collecte, menant petit à petit le monde à franchir son seuil de limite de stockage (« *Bekenstein Bound* »), constituant un point de non-retour aux conséquences importantes. Nous retiendrons le passage du roman expliquant qu « à l'image d'un sorcier brassant un chaudron de données (*data*) – les algorithmes disposant de bien trop de contrôle, de connaissances, d'autonomie – devenant bien plus puissantes qu'elles ne l'étaient, à tel point d'en être quasi méconnaissables » [« *Like a sorcerer mixing the cauldron of data – algorithms given too much control, too much insight, too much autonomy – vastly becoming more powerful than they were meant to be, nearly to the point of unrecognizability. Thus, it grew, unsuspectingly, except by its original mastermind…* », [notre trad.], KEAST (Christopher), *Datapocalypse*, ed. Goodreads Author, 2020].

considéré comme étant des vols de données. À l'image de la *blockchain uPort*, il s'agit de rendre le contrôle des données personnelles à leurs propriétaires[1412]. L'idée de *Microsoft*, d'IBM et des autres membres de la « *ID2020 Alliance* » est de rassembler l'intégralité des comptes et mots de passe d'un utilisateur en un seul, qui prendrait alors la forme d'une clé privée sur une *blockchain*. Cette clé permettrait à l'utilisateur à la fois de s'authentifier en dehors de la chaîne sur Internet, lui permettant d'accéder à n'importe quel service, tout en sécurisant son « *hub* numérique », lequel contiendrait à la fois les papiers officiels, les identifiants du compte bancaire, et d'autres données sensibles chiffrées par biométrie[1413]. Tel que l'exposait Alex Simons, directeur de la division « Identité » chez *Microsoft*, au cours du Festival américain *FUTUR.E.S*, l'idée est que, pour prouver son âge pour s'inscrire sur *Facebook*, « au lieu de fournir sa date de naissance exacte à l'entreprise, un simple certificat stipulant qu'on a plus de 13 ans [suffise] »[1414]. De plus, chaque utilisateur retrouverait le contrôle de ses données et aurait la possibilité de choisir à qui les céder et à quelles conditions. D'autres acteurs proposent également de permettre aux utilisateurs de monétiser leurs données au lieu de laisser les intermédiaires comme *Facebook* le faire pour eux, en plus de les responsabiliser[1415]. Par ailleurs, les utilisateurs de ces solutions auraient également la possibilité, si ces projets

---

[1412] HARVEY (Campbell R.), MOORMAN (Christine), TOLEDO (Marc), « En quoi la blockchain peut-elle vous aider à construire de meilleures relations avec vos clients ? », *Harvard Business Review* [en ligne], 14 mars 2019, https://www.hbrfrance.fr/magazine/2019/03/24697-en-quoi-la-blockchain-peut-elle-vous-aider-a-construire-de-meilleures-relations-avec-vos-clients/.

[1413] Selon la CNIL, une donnée biométrique recoupe plusieurs éléments identifiable du corps humain, constituée d'une « caractéristique physique ou biologique permettant d'identifier une personne (ADN, contour de la main, empreintes digitales, iris,...) » [CNIL [en ligne], v° Donnée biométrique, https://www.cnil.fr/fr/definition/donnee-biometrique]. – BERRY (Philippe), « Données, donnez-moi : La blockchain veut sauver nos identités numériques », préc. : « On parle ici d'un registre décentralisé extrêmement difficile à falsifier. Dans le cas de *Bitcoin*, la technologie sert à enregistrer des transactions financières en mettant à jour le solde de chaque membre. Pour l'identité, résume Alex Simons, il s'agit "de gérer et de protéger un identifiant unique" qui pourrait permettre de s'authentifier pour faire des achats, de souscrire un prêt, candidater à un job, recevoir des soins ou même voter en ligne. C'est simple sur le papier, mais en pratique, extrêmement compliqué, surtout à l'échelle d'un pays entier. [...] Le système sur lequel travaille *Microsoft* est hybride. Seuls trois éléments sont stockés sur une *blockchain* : un numéro unique passé à la moulinette cryptographique, une clé publique (un peu comme un RIB bancaire) et un pointeur indiquant l'adresse secrète du coffre-fort où sont stockées toutes les informations personnelles sensibles (carte d'identité électronique certifiée par le gouvernement, passeport, permis de conduire, diplôme signé électroniquement par une université, carte vitale, compte bancaire etc.). »

[1414] *Id.*

[1415] ANCIAUX (Arnaud), FARCHY (Joëlle), MÉADEL (Cécile), « L'instauration de droits de propriété sur les données personnelles : une légitimité économique contestable », *Revue d'économie industrielle* 2017/2, n° 158, pp. 26-28, notamment, p. 27 : « Ils proposent un service – de nature ambiguë – entre protection des données personnelles (*data locker*), revente maîtrisée de celles-ci et outils de négociation avec les vendeurs de biens et services (VRM, pour *vendor relationship managament*) [Note sous 23 : « Ainsi des propositions – encore un peu floues – de *Datacoup* ou *YesProfile* par exemple. Pour une liste de nombreux services, voir le wiki du *ProjectVRM* du *Berkman Center for Internet & Society* : http://cyber.law.harvard.edu/projectvrm/VRM_Development_Work. Pour un certain nombre d'offres, marché de la confiance et marché de la monétisation se rejoignent dans les mêmes entreprises. Les propositions de ces dernières regroupent mise en ligne protégée des données personnelles (proche du *cloud computing*) et monétisation envers des tiers. Mélange des genres particuliers qui pourrait évoquer une agence bancaire faisant de son coffre-fort une place de marché… »]. »

venaient à se concrétiser, de se servir de leur *hub* numérique pour prouver leur identité auprès des autres services proposés par les *blockchains* et nécessitant une identification certaine à l'instar des dispositifs de signature électronique[1416]. Seulement, un amas de données sensibles constitutives d'une identité numérique serait alors localisé directement sur la chaîne, comprenant des données telles que le RIB, voire les propriétés de l'ADN ou de l'iris de la personne concernée. Alors que les auteurs s'opposent actuellement sur la question de savoir si les données personnelles sont effectivement des biens considérés dans le commerce ou si elles ne sont que les attributs de la personnalité[1417], cette solution n'invite-t-elle pas à contourner temporairement le problème en le déplaçant ?

191. Le cas particulier des données des *wallets*. En parallèle de la *blockchain*, il s'avère qu'en vertu d'un certain nombre d'exigences légales en matière fiscale, mais également dans le cadre du processus « *Know Your Customer* » (KYC) issu d'obligations de mise en conformité aidant les professionnels à se prémunir contre des activités illégales[1418], les plateformes d'échange de crypto-monnaies et les systèmes de gestion de *wallets* collectent, pour leur part, automatiquement un certain nombre de données à caractère personnel, notamment les nom, prénom, adresse IP[1419]. Elles ont de plus accès

[1416] Sur les préludes d'un système autonome d'identification, *supra* n°s 132 et s.

[1417] Pour plus de précisions sur cette opposition, v., MOURON (Philippe), « Pour ou contre la patrimonialité des données personnelles », *Revue européenne des médias et du numérique* [en ligne], IREC, 2018, pp. 90-96, https://hal.archives-ouvertes.fr/hal-01823901/document ; CHERIF (Anaïs), « Être propriétaire de ses données personnelles, une dangereuse illusion », *La Tribune* [en ligne], 29 mars 2018, https://www.latribune.fr/technos-medias/internet/etre-proprietaire-de-ses-donnees-personnelles-une dangereuse-illusion-773398.html ; BOYER (Kim), « Nos données de santé n'appartiennent à personne », *Slate.fr* [en ligne], 9 févr. 2018, http://www.slate.fr/story/157492/big-data-propriete-donnees-personnelles-sante ; CREQUY (Perrine), « Bientôt tous rentiers grâce à nos données personnelles ? », *L'Observatoire* [en ligne], 11 mai 2018, https://www.mesdatasetmoi-observatoire.fr/article/bientot-tous-rentiers-grace-a-nos-donnees-personnelles.

[1418] World Economic Forum, Deloitte (collab.), « Blueprint for Digital Identity », Industry Project of the Financial Services Community [online], Future of Financial Services Series, Aug. 2016, http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf.

[1419] V. par exemple concernant les obligations KYC, PHILIPPS ERB (Kelly), « IRS Tries Again To Make Coinbase Turn Over Customer Account Data », *Forbes* [online], 20 Mar. 2017, https://www.forbes.com/sites/kellyphillipserb/2017/03/20/irs-tries-again-to-make-coinbase-turn-over-customeraccount-data/#1841d9e5175e. – Pour une définition du processus KYC, *supra* n°s 8, 132 – De nombreuses institutions financières s'engagent dans des procédures KYC en collectant des données et des informations basiques sur leurs clients et en utilisant idéalement la vérification d'identité électronique, à l'image d'un « programme d'identification du client ». Des informations telles que les noms, les numéros de sécurité sociale, les anniversaires et les adresses peuvent être très utiles pour déterminer si une personne est impliquée ou non dans un crime financier. Une fois ces données de base collectées, les banques le comparent généralement à des listes de personnes connues pour leur corruption, sur une liste de sanctions, soupçonnées d'être impliquées dans un crime ou à haut risque de corruption ou de blanchiment d'argent. Les institutions financières consultent également des listes de personnes politiquement exposées (listes PPE). Dès lors, l'établissement bancaire quantifie le degré de risque que son client présente et la probabilité qu'elle soit impliquée dans une activité corrompue ou illégale. Une fois ce calcul effectué, la banque peut donner un aperçu théorique de ce à quoi le compte de ce client devrait ressembler dans un avenir proche. Une fois que la trajectoire attendue du compte est en place, la banque peut alors surveiller en permanence l'activité du compte du client et s'assurer que rien ne semble être déplacé ou suspect. – V. également, ACPR, « Identification et connaissance de la clientèle (KYC) », *ACPR-Banque de France* [en ligne], 12 juin 2018,

aux clés privées des comptes de leurs clients, ce qui, par conséquent, les rend en mesure de croiser ces données et d'identifier les personnes physiques concernées. Plusieurs plateformes de *trading* de crypto-monnaies telles que *Coinbase*[1420], *Bit Bay*[1421] ou encore *Binance*[1422] requièrent une identification plus ou moins importante lors de l'inscription et de la création d'un compte[1423], de sorte qu'elles sont susceptibles de détenir des données à caractère personnel, voire de tenir un registre des bi-clés associés aux identités des clients au sens de l'art. 2 du RGPD[1424].

192. D'une manière générale, la situation n'est pas sans soulever de difficultés, tant au regard du respect de la vie privée et de la protection des données personnelles, que des principes plus spécifiques de secret des affaires, d'espionnage industriel et de protection des données d'entreprise face à la concurrence[1425]. Sans se conformer aux règles en vigueur, le système pourrait finir par agir en contradiction avec les intérêts de son utilisateur[1426]. Cette situation est d'ailleurs assez paradoxale car, d'une part, sur le plan probatoire la pseudonymisation s'oppose souvent aux exigences d'identification[1427] et, d'autre part, cette identification se révèle dangereuse pour la protection de la vie privée.

B. Étendue de la notion de « données personnelles »

193. Anonymat *versus* pseudonymat : l'importance du potentiel identifiant des données. La version communautaire de la notion de « données à caractère personnel » comporte une définition plus précise que celle de l'art. 2 de la loi de 1978 puisqu'elle indique qu'il s'agit de « toute information se rapportant à […] une personne physique identifiée ou qui peut être identifiée, directement ou indirectement », précisant qu'elle peut prendre la forme « notamment » d'une « référence à un numéro d'identification tel,

https://acpr.banque-france.fr/autoriser/fintech-et-innovation/nos-dossiers-thematiques/identification-et-connaissance-de-la-clientele-kyc.

[1420] V.., https://help.coinbase.com/, Products > Coinbase Help Center > Getting started > ID document verification.

[1421] V., https://bitbay.net/, Registre > Bitcoin & digital currencies > Beginner > Do I need to verify my account?

[1422] V., https://www.binance.com/, Home > Binance Terms of Use (II – General Provisions > 3. Binance Account Registration and Requirements > c. User Identity Verification).

[1423] Sur la recherche et l'existence de solutions permettant l'identification sécurisée des utilisateurs de *blockchain*, *supra* n°s 132 et s., notamment n°s 134-135.

[1424] « Un fichier est un traitement de données qui s'organise dans un ensemble stable et structuré de données. Les données d'un fichier sont accessibles selon des critères déterminés. » [CNIL [en ligne], v° Fichier, https://www.cnil.fr/fr/definition/fichier].

[1425] BEAUDEMOULIN (Nathalie) *et al.*, « Les enjeux de la Blockchain pour la Banque de France et l'Autorité de Contrôle prudentiel et de Résolution (ACPR) », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 31.

[1426] GUILHAUDIS (Élise), art. cit., p. 12.

[1427] *Supra* n°s 109, 110 et s.

qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale »[1428]. La CNIL ajoute à la définition légale que l'identification indirecte peut découler d'un numéro client, d'un numéro de téléphone, de la voix ou de l'image de la personne concernée[1429]. Elle précise également que cette identification peut être opérée tant par le biais d'une seule donnée, telle que le numéro de sécurité sociale ou l'ADN d'un utilisateur, qu'à partir du croisement de plusieurs données visibles sur le réseau qui, même anonymes, permettent de réidentifier la personne[1430]. Par exemple, la position actuelle d'un internaute est calculée par le moteur de recherche *Google Chrome* à partir de différentes sources telles que la position de l'appareil, les adresses avec libellé, l'historique des positions, l'activité précédente dans l'ensemble des produits *Google*, l'adresse IP de la connexion Internet, qui est obligatoire pour naviguer en ligne[1431].

Une donnée anonyme, insusceptible d'emporter l'application des dispositions du règlement, suppose que toute identification d'une personne déterminée soit impossible[1432]. En principe, les quelques éléments inscrits sur une *blockchain* comme *Bitcoin* ne devraient pas permettre cette identification. Toutefois, au-delà de s'apercevoir qu'une personne est *identifiée*[1433], pour savoir si une personne est effectivement *identifiable* – ce qui revient à analyser le « potentiel identifiant » d'une donnée[1434] – il convient selon le règlement de prendre en compte tant l'ensemble des moyens technologiques disponibles, que le coût à mettre en œuvre afin de réussir à identifier la

[1428] Règl. (UE) n° 2016/679, préc., art. 4, § 1.
[1429] CNIL, « RGPD : de quoi parle-t-on ? », CNIL [en ligne], https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on, Accueil > Comprendre le RGPD > De quoi parle-t-on ?
[1430] La CNIL explique, par exemple, qu' « une base marketing contenant de nombreuses informations précises sur la localisation, l'âge, les goûts et les comportements d'achats de consommateurs, y-compris si leur nom n'est pas stocké, est considérée comme un traitement de données personnelles, dès lors qu'il est possible de remonter à une personne physique déterminée en se basant sur ces informations » [*id.*]. – V. également, CNIL, « Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data », *CNIL* [online], 6 Nov. 2018, https://www.cnil.fr/en/blockchain-and-gdpr-solutionsresponsible-use-blockchain-context-personal-data ; BERBERICH (Mattthias), STEINER (Malgorzata), « Blockchain technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers? », *European Data Protection Law Review*, Vol. 2, Issue 3, 21 Mar. 2016, p. 422 ; Report of the European Blockchain Observatory and Forum, « Blockchain and the GDPR », EU Blockchain Forum [online], 16 Oct. 2018, https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf.
[1431] https://support.google.com/, Centre d'aide, Comprendre et gérer vos données de localisation lorsque vous effectuez une recherche sur Google > Comment Google détermine votre position lorsque vous effectuez une recherche.
[1432] Sur la distinction entre les techniques utilisées pour garantir la confidentialité et l'intégrité des données, à savoir, les techniques réversibles (pseudonymisation et chiffrement) ou irréversibles (anonymisation), V., JOMNI (Adel), « Le RGPD : un atout ou un frein pour la cybersécurité ? », *D. IP/IT* 2019, n° 6, p. 352.
[1433] GUILHAUDIS (Élise), art. cit., p. 13.
[1434] VERBIEST (Thibault), « Blockchain : une révolution juridique ? », art. cit., *loc. cit.*

personne[1435]. La liste d'exemples de données à caractère personnel identifiantes ou permettant d'identifier une personne fournie par l'art. 4 § 1 du règlement se prétend non limitative de manière à pouvoir étendre la notion de donnée personnelle à toute donnée nécessitant une protection[1436]. Le règlement s'applique ainsi à toute information à caractère personnel, même couverte par un pseudonyme, dès lors qu'il est possible de « réidentifier la personne physique concernée »[1437], c'est-à-dire de remonter jusqu'à elle, en se servant aussi bien d'autres données que de moyens techniques divers pour y parvenir[1438]. Or, il semble qu'en matière de *blockchain*, cela soit possible.

194. Des données pas si anonymes. Dans le protocole *Bitcoin*, l'historique complet des transactions est accessible au public, simplement, celui-ci est anonymisé de sorte à assurer la confidentialité des utilisateurs en plus de sécuriser leurs opérations. Chacun peut donc prendre connaissance de la façon dont les *bitcoins* voyagent d'une adresse – ou d'un pseudonyme – à une autre, et éventuellement relier différentes adresses afin d'identifier un même utilisateur[1439]. Il s'avère en effet que, dès la mise en œuvre du protocole, l'article original de *Bitcoin* mentionnait déjà cette « inévitable » circonstance comme une exception à la « *privacy* » mise en place[1440]. Par la suite, alors que plusieurs auteurs ont confirmé qu'en analysant les chaînes de transactions il est possible de regrouper les adresses et donc les pseudonymes des utilisateurs[1441], d'autres ont démontré que les adresses peuvent parfois être croisées avec les identités de personnes physiques

[1435] L. n° 2018-493, préc., art. 2, al. 2 : « Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. »
[1436] ZICRY (Laure), *op. cit*., p. 23.
[1437] MEKKI (Mustapha), « Le smart contract, objet du droit (Partie 2) », *D. IP/IT* 2019, n° 1, p. 27.
[1438] Le règlement précise en effet que « les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable » [Règl. (UE) n° 2016/679, préc., considérant n° 26].
[1439] BIRYUKOV (Alex), KHOVRATOVICH (Dmitry), PUSTOGAROV (Ivan), « Deanonymisation of Clients in Bitcoin P2P Network », *arXiv.org* [online], 5 Jul. 2014, https://arxiv.org/abs/1405.7418.
[1440] Satoshi Nakamoto avait en effet indiqué que « certains regroupements sont toujours inévitables avec les multiples entrées de transactions, car elles révèlent nécessairement que leurs entrées appartenaient au même propriétaire. Le risque est que si l'identité du propriétaire d'une clé est révélée, le regroupement pourrait révéler d'autres adresses appartenant à ce même propriétaire » [« *Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner*. » [notre trad.], NAKAMOTO (Satoshi), « Bitcoin: A Peer-to-Peer Electronic Cash System », préc.].
[1441] MEIKLEJOHN (Sarah), POMAROLE (Marjori), JORDAN (Grant), LEVCHENKO (Kirill) *et al.*, « A fistful of bitcoins: Characterizing payments among men with no names », *in* LUCKIE (Matthew J.), BEVERLY (Robert), BRINKMEYER (William), CLAFFY (Kc Claire), *IMC '13: Proceedings of the 2013 Conference on Internet Measurement Conference*, ed. ACM, 2013, pp. 127-140 ; RON (Dorit), SHAMIR (Adi), « *Quantitative analysis of the full bitcoin transaction graph* », *in* BÖHME (Rainer), BRENNER (Michael), MOORE (Tyler), SMITH (Matthew), *Financial Cryptography and Data Security*, ed. Springer, 2014, pp. 6-24.

lorsqu'elles sont combinées avec d'autres données, y compris de sources différentes telles que les messages sur les forums dédiés, lesquels sont en pratique souvent signés par le même pseudonyme que celui utilisé sur la chaîne[1442]. Cependant, comme le relève Satoshi Nakamoto en ce qui concerne *Bitcoin*, s'il advient qu'un tiers, ou même l'utilisateur lui-même par inadvertance ou à la suite d'un problème de sécurité, divulgue l'identité de la personne physique liée à une adresse, toutes les données de transactions liées à celle-ci seraient immédiatement révélées publiquement[1443]. Ainsi serait-il ensuite aisé de reconstituer la chaîne des transactions.

Il est également possible en théorie de parvenir à identifier un utilisateur *via* le croisement avec des informations collectées par des objets communicants ou par des *cookies*, telles que des identifiants de connexion, des identifiants permettant de tracer la navigation pour des finalités statistiques ou publicitaires, etc.[1444], à condition que l'utilisateur en question ait utilisé ses identifiants sur un site Internet ayant capté ses données[1445]. Il est probable également que l'identité d'un utilisateur soit découverte dans le cas où son *wallet* serait hébergé *via* un site opérant à partir d'un établissement centralisé, tel qu'une banque[1446], ou qu'elle soit indirectement fournie par l'algorithme d'un *smart contract*[1447]. Ne constituent toutefois pas des données à caractère personnel les données composant les documents inscrits à titre de preuve sous la forme d'un *hash* et qui sont par conséquent à la fois inaccessibles, en clair et au protocole.

Ces méthodes ne sont toutefois pas génériques[1448]. L'écosystème des *blockchains* veille toujours, en principe, à mettre à jour la chaîne pour éviter tout problème de confidentialité. Cependant, ces divers exemples suggèrent que, parfois, les attaques tentées fonctionnent et sont susceptibles de révéler l'identité des utilisateurs. Partant de là, il n'est pas déraisonnable d'estimer que l'adresse ou la clé publique utilisée *via* les technologies *blockchains* ne peut emporter la qualification d'une donnée « anonyme »

[1442] REID (Fergal), HARRIGAN (Martin), « An analysis of anonymity in the bitcoin system », *in* ALTSHULER (Yaniv), ELOVICI (Yuval), CREMERS (Armin B.), AHARONY (Nadav) *et al., Security and Privacy in Social Networks*, ed. Springer, 2013, pp. 197-223 ; MEIKLEJOHN (Sarah), POMAROLE (Marjori), JORDAN (Grant), LEVCHENKO (Kirill) *et al.*, *op. cit.*, *loc. cit.*

[1443] NAKAMOTO (Satoshi), « Bitcoin: A Peer-to-Peer Electronic Cash System », préc.

[1444] V. https://www.journal-officiel.gouv.fr, Accueil > Gestion des cookies > A propos des cookies, 1. Qu'est-ce qu'un "cookie" ?

[1445] Sur l'aléa de l'identification en matière de *blockchain*, *infra* n°s 114-115 ; DEVILLIER (Nathalie), « Jouer dans le "bac à sable réglementaire" pour réguler l'innovation disruptive : le cas de la technologie de la chaîne de bloc », *RTD com.* 2017, p. 1037.

[1446] *Id.*

[1447] Sur les données contractuelles pouvant figurer au sein d'un *smart contract*, *supra* n° 189.

[1448] BIRYUKOV (Alex), KHOVRATOVICH (Dmitry), Pustogarov (Ivan), « Deanonymisation of clients in Bitcoin P2P network », *arXiv* [online], 28 May 2014, p. 1, https://arxiv.org/pdf/1405.7418v1.pdf.

puisqu'elle ne peut pas « ne pas être [associée] directement ou indirectement à une personne physique »[1449].

195. Une qualification perméabilisée par l'interprétation protectrice de la jurisprudence : l'exemple de la réidentification par l'intermédiaire de l'adresse IP. Force est de reconnaître que des moyens techniques permettent actuellement l'identification de certains utilisateurs d'une *blockchain*[1450]. En parallèle, la jurisprudence européenne mais aussi française a eu tendance ces dernières années à étendre progressivement le spectre des données à caractère personnel et *a fortiori* le champ d'application des règles en la matière[1451]. Par exemple, l'adresse IP a été assimilée à une donnée à caractère personnel par la CJUE dans l'affaire « *Google Spain SL Google Inc c/Agencia Espanola de Proteccion de Datos* » en 2014[1452]. Ensuite, après avoir insisté sur l'importance de l'utilisation du terme « indirectement » dans la définition donnée par le règlement, la CJUE a étendu la qualification de donnée personnelle à l'adresse IP dynamique[1453]. En France, les tribunaux ont adopté un raisonnement similaire[1454] afin de casser le jugement qui considérait qu'une adresse IP ne se résumait qu'à une suite de « chiffres se rapportant à un ordinateur et non à un utilisateur »[1455]. Par conséquent, l'adresse IP, même dynamique, est désormais considérée comme une information personnelle dont la collecte constitue un traitement de donnée à caractère personnel.

En matière de *blockchains*, si un tiers réussit à obtenir l'adresse IP d'un utilisateur, il pourrait *ipso facto* retracer l'intégralité de son activité[1456], mais également identifier le fournisseur d'accès à Internet (FAI) de l'adresse et donc obtenir l'identité de la personne

---

[1449] HAAS (Gérard), « Bilan après neuf mois d'application du RGPD », *D. IP/IT* 2019, n° 6, p. 357.
[1450] Règl. (UE) n° 2016/679, préc., considérant n° 26. – *Supra* n°s 119 et s. – V. également, VERBIEST (Thibault), « Blockchain : une révolution juridique ? », art. cit., *loc. cit.*
[1451] GUILHAUDIS (Élise), art. cit., p. 13.
[1452] CJUE, 13 mai 2014, n° C-131/12, *Google Spain SL Google Inc c/ Agencia Espanola de Proteccion de Datos.*
[1453] CJUE, 19 oct. 2016, n° C-582/14, *Breyer c/ Bundesrepublik Deutschland*, JurisData n° 2016-030407. – D'après le site Définitions-marketting.com [https://www.definitions-marketing.com/definition/adresse-ip-dynamique/] : « Lorsque l'accès Internet d'un abonné n'est pas dégroupé, son fournisseur d'accès lui attribue à chaque établissement d'une connexion (par le modem) une adresse IP différente dite adresse IP dynamique. Une adresse IP dynamique est donc dans le temps utilisée par plusieurs utilisateurs. L'adresse IP dynamique ne permet donc pas l'identification d'une machine d'une session à l'autre et encore moins celle d'un utilisateur. Elle permet cependant la géolocalisation plus ou moins précise du point d'accès. »
[1454] Cass. Civ. 1ère, 3 nov. 2016, nº 15-22.595 (« Les adresses IP, qui permettent d'identifier indirectement une personne physique, sont des données à caractère personnel, au sens de l'article 2 de la L. n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, de sorte que leur collecte constitue un traitement de données à caractère personnel et doit faire l'objet d'une déclaration préalable auprès de la Commission nationale de l'informatique et des libertés. »).
[1455] VERBIEST (Thibault), « Blockchain : une révolution juridique ? », art. cit., *loc. cit.*
[1456] GUILHAUDIS (Élise), art. cit., *loc. cit*.

physique concernée. Or, dans la pratique, si l'adresse IP n'est pas une donnée accessible en clair, deux méthodes peuvent malgré tout conduire un individu à l'obtenir.

D'une part, l'individu peut pirater un tiers ayant un accès direct à ce type de données, à l'image des plateformes de *trading* de crypto-monnaies et les systèmes de gestion de portefeuilles de *bitcoins*[1457].

D'autre part, il peut employer des moyens techniques, parfois sous forme d'attaques informatiques, pour déduire d'un croisement d'informations un numéro d'identification correspondant à une adresse IP unique sur le réseau Internet. Volontairement transparente, la *blockchain* laisse en effet apparaître en clair les informations concernant les opérations effectuées. Cela suppose qu'en analysant les transactions, soit émises, soit reçues, ou les deux, ou même en utilisant la topologie du réseau pour croiser une adresse d'un protocole d'une *blockchain* avec une localisation et/ou une adresse IP, ces informations peuvent être connues. Plusieurs techniques ont aujourd'hui été mises en lumière par les chercheurs. Andreas M. Antonopoulos constate, par exemple, qu'il est possible, lors de la première « prise de contact initial » entre un nouveau nœud et les pairs du réseau *Bitcoin*, d'analyser et de croiser les données inscrites sur la chaîne et les adresses IP automatiquement enregistrées et instantanément visibles sur le réseau[1458]. Une étude publiée en 2014 par trois chercheurs de l'Université du Luxembourg décèle une autre forme de « désanonymisation des clients du réseau P2P *Bitcoin* »[1459]. Les auteurs remarquent qu'à chaque fois qu'un client *Bitcoin*, qui est un logiciel de fourniture de *wallets* (*software wallets*), se connecte au réseau *Bitcoin* pour son utilisateur, il établit en pratique huit connexions avec les serveurs[1460]. Au cours de ces multiples connexions, le client *Bitcoin* s'identifie sur le réseau grâce à un octet de connexions qui lui sert d'identifiant unique pendant toute la durée d'une session

[1457] Les utilisateurs peuvent transférer des *bitcoins* sur le réseau et les utiliser de la même manière que des pièces de monnaie ou des fonds déposés sur un compte bancaire pour acheter ou vendre des biens et services, envoyer de l'argent, demander un crédit ou un change, etc., utilisent des portefeuilles numériques pour *bitcoin*, des *wallets*. Pour plus de précisions sur le fonctionnement, *supra* n° 6.

[1458] En pratique, il apparaît que les adresses IP des nœuds sont stockées sur la chaîne de blocs *via* des DNS. Explications d'après le mécanisme de prise de contact initial entre les pairs du réseau [v., ANTONOPOULOS (Andreas M.), *Mastering Bitcoin*, ed. O'Reilly, 2nd edition, 2017, p. 152, (trad., préc.)] : « Comment un nouveau nœud trouve des pairs ? La [...] méthode consiste à interroger un DNS en utilisant un certain nombre de graines DNS (*DNS seeds*), des serveurs DNS qui fournissent une liste 8 d'adresses IP de nœuds *bitcoin*. Certaines de ces graines DNS fournissent une liste statique des adresses IP des nœuds *bitcoin* stable en écoute. D'autres sont des implémentations personnalisées de BIND (*Berkeley Internet Name Daemon*) qui renvoient un sous-ensemble aléatoire d'adresses à partir d'une liste d'adresses de nœuds *bitcoin* recueillies par un robot ou d'un nœud *bitcoin* en activité depuis longtemps. Le client *Bitcoin Core* contient les noms de cinq graines DNS différentes. [...] » – Pour plus de précisions, v. également, Bitcoin Project, « Protéger votre confidentialité », *Bitcoin.org* [en ligne], https://bitcoin.org/fr/proteger-votre-vie-privee.

[1459] BIRYUKOV (Alex), KHOVRATOVICH (Dmitry), Pustogarov (Ivan), art. cit.

[1460] *Id.*

utilisateur[1461]. Cet octet de connexions correspond à une liste des huit nœuds d'entrée connectés. Tout assaillant peut alors créer une série d'attaques au cours desquelles il va prendre connaissance de l'octet de connexions du client *Bitcoin* et, en analysant l'activité du réseau, relier le *hash* d'une transaction émise par les nœuds du client *Bitcoin* avec l'adresse IP de son expéditeur, qui est un utilisateur du *software wallet* figurant sur le réseau. Le coût d'une telle attaque ne dépasserait pas, selon les auteurs, l'équivalent de 1 500 euros[1462].

196. En dehors des données personnelles et pseudonymes, par essence, les chaînes de blocs comportent systématiquement au moins une donnée qualifiée de personnelle, à savoir l'adresse IP de l'utilisateur. La *blockchain* n'est donc pas un « OVNI technologique » et, par-delà ses spécificités, il est désormais impossible de soutenir l'inapplication des règles protectrices en matière de données à caractère personnel. Il convient alors de s'assurer de leur compatibilité.

§ 2. Entre contradictions et freins à l'innovation

197. Tout traitement de données doit répondre à certains impératifs qui peuvent se classer en deux catégories, à savoir, les exigences avant collecte et les exigences après collecte. Appliquées à la *blockchain*, il en ressort que, de la collecte au traitement, si la technologie se révèle relativement neutre vis-à-vis des données inscrites, force est de constater que leur mise en œuvre pose pourtant parfois problème. Il en va ainsi non seulement à raison de l'impossibilité de pourvoir la technologie d'un responsable (A), mais plus encore de l'absence de limitation protocolaire quant à l'étendue du traitement des données effectué (B). Toutefois, comme le rappelle la Commission de réflexion sur l'Éthique de la Recherche en sciences et technologies du Numérique d'Allistene (CERNA) concernant les systèmes numériques en général et robotiques en particulier, il convient de ne pas brider les capacités d'innovation numérique d'une technologie, si bien que, lorsqu'il apparaît difficile de la rendre compatible, il est au moins essentiel de « veiller à ce que le système […] facilite le contrôle de l'usage des données »[1463].

[1461] *Id.*
[1462] *Id.*
[1463] « Éthique de la recherche en robotique. Rapport n° 1 de la CERNA, Commission de réflexion sur l'Éthique de la Recherche en sciences et technologies du Numérique d'Allistene », *CERNA* [en ligne], nov. 2014, p. 16, 31, https://hal.inria.fr/ALLISTENE-CERNA/hal-01086579v1(concernant les préconisations générales [GEN-5] applicables à tout système numérique).

198. La nécessité d'un paramétrage dès la conception du système. Le RGPD, et *a fortiori* les lois françaises sur la protection des données personnelles, sont fondés à s'appliquer dès lors que la mise en œuvre d'un projet entraîne un traitement de données à caractère personnel. Quel que soit le type de données personnelles collecté, le responsable de traitement est chargé de prendre en compte en amont, autrement dit dès la conception (*by design*), l'ensemble des questions relatives à leur protection, tant d'un point de vue technique qu'organisationnel, de manière à les intégrer à l'algorithme du protocole (*by default*)[1464]. Ce concept repose sur le principe du *Privacy by design*, imposé par l'art. 25 du RGPD, et de son corollaire, le principe du *Privacy by default*[1465], qui impliquent que le transfert et le stockage des données se réalisent de manière à impacter le moins possible les droits et les libertés des personnes concernées[1466]. L'objectif est avant tout préventif et permet de limiter les risques de dommages résultant d'une non-conformité[1467]. Tel que le relève un auteur, il semble donc « préférable que la gouvernance d'un système basé sur la technologie passe par la technologie elle-même », de sorte qu'il est nécessaire d'intégrer les exigences du RGPD au code dès sa conception[1468]. Les plateformes de *trading* de cryptomonnaies et autres systèmes de gestion de portefeuilles procédant au traitement des données personnelles des utilisateurs qui recourent à leurs services ne peuvent évidemment pas se prévaloir de telles difficultés étant donné que leur organisation ne repose pas sur les règles particulières de fonctionnement de la *blockchain*.

199. De la nécessité des données inscrites par et pour les utilisateurs aux paramètres indispensables au respect de l'obligation de minimisation. S'agissant d'abord de l'obligation de minimisation de la collecte conduisant le responsable de traitement à ne collecter et traiter que les données nécessaires au traitement, ce principe

[1464] Règl. (UE) n° 2016/679, préc., art. 25, notamment : « le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, […] qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, […] de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée ».
[1465] ANCIAUX (Arnaud), FARCHY (Joëlle), MÉADEL (Cécile), « L'instauration de droits de propriété sur les données personnelles : une légitimité économique contestable », art. cit., p. 29.
[1466] GODEFROY (Lêmy), « La gouvernementalité des blockchains publiques », *D. IP/IT* 2019, n° 9, p. 497.
[1467] DE MONZA (Romain), « "Privacy by design/by default" – Assurer des mesures préventives », *Solutions Numériques* [en ligne], 13 mars 2018, https://www.solutions-numeriques.com/articles/privacy-by-designby-default-assurer-des-mesures-preventives/.
[1468] *Id.*

est, pour certains auteurs, inappliqué car inapplicable[1469]. En effet, selon eux la chaîne étant inarrêtable, personne ne peut contrôler tant la masse de données personnelles inscrite dans chaque bloc, que la vitesse à laquelle les blocs sont validés et enchaînés à la suite des derniers blocs de la *blockchain*[1470]. Il leur semble par conséquent impossible de maîtriser les données qui sont stockées sur la chaîne.

Aussi ne s'agit-il pas tant de savoir si le responsable de traitement peut agir sur la chaîne et la contrôler directement, mais plutôt de s'assurer que la masse d'informations vouées à être inscrites respectent des règles en termes de quantité et de qualité. Or, il importe de rappeler, d'une part, le fondement sur lequel s'appuie le principe de minimisation, à savoir que les données collectées doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées »[1471] et, d'autre part, que la *blockchain* est constituée des inscriptions générées par ses utilisateurs. Cela permet en effet de soulever la notion de pertinence par défaut de la collecte au même titre que la relative indifférence du protocole vis-à-vis des données collectées en tant qu'elles suffisent à son fonctionnement, ce qui justifie ainsi de nuancer le propos. La masse de données inscrite dans les blocs l'est par les utilisateurs eux-mêmes selon leurs besoins, lesquels correspondent en règle générale aux nécessités contractuelles et aux exigences posées par la loi en fonction du service qui leur est rendu par la *blockchain*. Ces informations sont en principe limitées à ce qu'ils décident d'inscrire et ne résultent donc que d'une transcription de leur volonté. Elles ont, pour l'essentiel, trait à l'identité et éventuellement, dans le cas d'un *smart contract*, aux coordonnées de la personne physique concernée, et sont en pratique essentielles à l'exécution du contrat. Par ailleurs, tout document inscrit notamment à titre de preuve ne fait l'objet d'un stockage sur la *blockchain* que sous la forme d'un *hash* à sens unique, rendant impossible la reconstitution du document initial auquel même le protocole de la *blockchain* n'a pas accès. Finalement, les informations seraient donc à la fois pertinentes et nécessaires pour les parties ainsi que pour la bonne exécution du protocole, ce qui permet à la technologie de remplir la double condition de proportionnalité et de finalité du traitement.

Cependant, et tel que le constate également la CNIL, le protocole étant par nature public, les données complémentaires inscrites par ses utilisateurs, c'est-à-dire autres que les identifiants consistant en des bi-clés cryptographiques, sont, pour la plupart, publiquement accessibles elles aussi[1472]. Les utilisateurs sont en principe conscients de

[1469] CREQUY (Perrine), art. cit.
[1470] VERBIEST (Thibault), « Blockchain : une révolution juridique ? », art. cit., *loc. cit.*
[1471] Règl. (UE) n° 2016/679, préc., art. 5, § 1, c).
[1472] CNIL, « Blockchain : Premiers éléments d'analyse de la CNIL », préc., p. 8.

cette particularité des *blockchains* mais, comme pour les fournisseurs de services de réseaux sociaux, le RGPD s'applique quand bien même les données sont rendues publiques par la personne elle-même, ce qui les oblige à en assurer la confidentialité. Parmi les solutions de minimisation couramment utilisées, figure la sécurisation des données *via* des techniques de chiffrement des communications[1473]. La CNIL préconise donc le recours aux techniques de cryptographie[1474] et déclare que « si cela n'est pas possible, un enregistrement sous la forme d'une empreinte obtenue avec une fonction de hachage à clé est possible ou, *a minima*, d'un chiffré, permettant d'assurer un haut niveau de confidentialité »[1475]. L'objectif est finalement double. D'une part, il est question de limiter le nombre de personnes ayant un accès direct aux données à caractère personnel présentes sur les chaînes. D'autre part, il s'agit de laisser la possibilité à chacun de vérifier l'existence et la véracité d'une donnée en contrôlant l'intégrité de l' « information prouvant l'existence de la donnée » stockée seule et en clair sur la *blockchain* sous la forme, par exemple, d'un engagement cryptographique ou d'une empreinte issue d'une fonction de hachage à clé[1476]. La CNIL indique que « le principe commun à certaines de ces solutions est que la donnée en clair est stockée ailleurs que sur la *blockchain* » et propose pour cela de l'enregistrer sur le système d'information du responsable de traitement[1477].

200. La flexibilité du paramétrage au service de la conformité aux obligations d'information et de consentement. La réglementation protectrice des données personnelles contraint également le responsable de traitement à une obligation d'information[1478]. La *blockchain* doit donc, dès sa conception[1479], prévoir de garantir et de satisfaire le droit de chaque utilisateur à une information à la fois claire et complète[1480], assortie d'un certain nombre d'éléments, tels que l'identité et les coordonnées du responsable de traitement et, le cas échéant, celles de son représentant, les finalités poursuivies par le traitement auquel les données sont destinées, ou encore la mention du

---

[1473] FÉRAL-SCHUHL (Christiane), *CyberDroit : Le droit à l'épreuve de l'Internet*, éd. Dalloz, coll. Praxis Dalloz, 8e édition, 2020, pp. 119-120.
[1474] Elle précise d'ailleurs qu'il doit s'agir d'un « engagement cryptographique », c'est-à-dire « un mécanisme qui permet de figer une donnée de telle sorte qu'il soit possible, avec des éléments supplémentaires, de prouver ce qui a été figé, et à la fois impossible de la retrouver ou de la reconnaître à partir de cette seule version "engagée" » [CNIL, « Blockchain : Premiers éléments d'analyse de la CNIL », préc., *loc. cit.*].
[1475] *Id.*
[1476] *Id.*
[1477] *Id.*
[1478] Règl. (UE) n° 2016/679, préc., art. 13.
[1479] *Ibid.*, art. 25.
[1480] L. n° 78-17, préc., art. 70-1 (nouveau), modifié par la L. n° 2018-493, préc., art. 30.

droit d'introduire une réclamation auprès de la CNIL. La mise en œuvre de cette obligation doit permettre de recueillir un consentement à la fois libre, spécifique, éclairé et univoque de l'utilisateur d'une *blockchain*[1481], manifesté par le biais d'un acte positif clair et explicite[1482]. Pour cela, l'information doit être délivrée au moment du recueil du consentement[1483] en des termes « clairs et compréhensibles en utilisant des mots simples du langage courant »[1484].

En pratique, toute première participation à une *blockchain* – qu'il s'agisse d'inscrire une transaction ou de miner – doit donc être précédée d'une étape au cours de laquelle l'utilisateur quel qu'il soit est dûment informé de l'étendue et de la finalité du traitement opéré par la *blockchain* pour ensuite manifester son accord. Force est de constater que la technologie conduit par elle-même à respecter ces exigences et à en faciliter la preuve puisqu'il en va de son fonctionnement de requérir une validation pour chaque information avant de l'inscrire de façon immuable sur la chaîne[1485]. Comme le constate un auteur, aucune difficulté ne devrait apparaître car « le consentement […] est au cœur du fonctionnement d'une *blockchain* »[1486]. Il sera simplement nécessaire, avant même qu'elle ne fournisse un service quelconque, que le consentement soit recueilli en vertu de l'art. 7 du RGPD et, au préalable, que l'information soit délivrée. Bien que la CNIL paraisse relativement partagée quant à la capacité de la technologie à se conformer à de telles exigences[1487], il semble que les algorithmes soient, dans cette hypothèse, suffisamment flexibles pour s'y adapter. Un auteur souligne qu'il est effectivement primordial que des précautions soient prises, mais elles le pourront « sinon hors de tout support numérique, du moins en mettant en place un process attirant l'attention de l'auteur sur l'objet, la nature et l'étendue de son consentement »[1488]. Lors d'une délibération en date du 4 juillet 2019 concernant les opérations de lecture ou écriture dans le terminal d'un utilisateur, en particulier les *cookies* et autres traceurs, la CNIL a précisé que le consentement valide d'un individu résultait obligatoirement d'une démarche active, en ce sens que l'accord implicite déduit à partir du comportement de la personne concernée de

[1481] Règl. (UE) n° 2016/679, préc., art. 7 ; FÉRAL-SCHUHL (Christiane), *CyberDroit : Le droit à l'épreuve de l'Internet*, *op. cit.*, p. 35.
[1482] Règl. (UE) n° 2016/679, préc., art. 4, § 11 ; Lignes directrices n° 17/FR WP259 rév.01 du Groupe de travail « Article 29 », 28 nov. 2017, sur le consentement au sens du règlement 2016/679.
[1483] Délib. n° 2019-093, 4 juill. 2019, portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janv. 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs), *JORF* n° 0166, 19 juill. 2019, texte n° 92.
[1484] *Id.*, comm. LEBEAU-MARIANNA (Denise), CAULIER (Tiphaine), « Délibération de la CNIL du 4 juillet 2019 sur les cookies : quelles conséquences pratiques pour les entreprises ? », D. IP/IT 2019, n° 12, p. 703.
[1485] MEKKI (Mustapha), « Le smart contract, objet du droit (Partie 2) », art. cit.
[1486] *Id.* – V. également, WEINBAUM (Noémie), « La preuve du consentement à l'ère du RGPD et de la blockchain », *JCP E* 2018, n° 10, pp. 28-32.
[1487] CNIL, « Blockchain : Premiers éléments d'analyse de la CNIL », préc., p. 7.
[1488] MEKKI (Mustapha), « Le smart contract, objet du droit (Partie 2) », art. cit.

continuer sa navigation sans répondre explicitement à la demande de consentement n'était plus guère valable[1489]. À l'instar de l'acte positif, libre et obligatoirement explicite requis en matière de *cookies*, le protocole de la *blockchain* pourrait permettre à ses utilisateurs d'accepter le traitement, par exemple, par le biais d' « un clic d'acceptation », de « l'activation d'un bouton »[1490] ou d'une touche spécifique, après avoir été informés sur l'existence et les potentielles finalités du traitement effectué par la *blockchain*.

Ces obligations de mise en conformité incombent au responsable de traitement. Mais faut-il, pour cela, désigner préalablement à toute collecte cet acteur[1491].

201. La nécessité d'un responsable. Bien que la technologie semble être en mesure de s'adapter par le biais de la programmation à la plupart des exigences posées, la détermination d'un responsable génère quelques difficultés. Il est toutefois primordial de connaître les acteurs d'un traitement[1492], ne serait-ce parce que ce sont eux qui ont à charge de fixer puis d'informer les utilisateurs de la finalité du traitement de données à caractère personnel les concernant, mais également de leur possibilité de s'y opposer[1493], d'assurer une sécurité suffisante des données collectées, « et, notamment, [d']empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès »[1494]. Le rôle du responsable de traitement est d'autant plus important qu'il est tenu de rendre des comptes aux utilisateurs en cas de violation de leurs données personnelles, à l'occasion, par exemple, d'une faille de sécurité[1495], définie comme étant une action accidentelle ou illicite ayant entraîné « la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques »[1496]. Finalement, tel que le constate un auteur, le rôle affecté au responsable de traitement témoigne de l'importance, encore aujourd'hui, de ce tiers[1497]. Si tant est que la *blockchain* soit naturellement protégée de toute intrusion par attaque informatique ayant pour objectif de modifier, d'endommager, ou de subtiliser et d'utiliser les informations qu'elle renferme, l'exécution de ces impératifs apparaît malgré tout entravée par le caractère distribué, lequel garantit l'immuabilité du système[1498]. En effet,

[1489] Délib. n° 2019-093, préc.
[1490] *Id.*, comm. LEBEAU-MARIANNA (Denise), CAULIER (Tiphaine), art. cit.
[1491] L. n° 78-17, préc., art. 81-83, modifié par la L. n° 2018-493, préc., art. 32-37.
[1492] GUILHAUDIS (Élise), art. cit., p. 13.
[1493] L. n° 78-17, préc., art. 82, respectivement 1° et 2°, modifié par la L. n° 2018-493, préc., art. 32, II.
[1494] L. n° 78-17, préc., art. 121, modifié par la L. n° 2018-493 préc., art. 34, al. 2.
[1495] *Infra* n°s 273 et s., concernant les failles de sécurité potentielles en matière de *blockchain*.
[1496] L. n° 78-17, préc., art. 83, I, al. 2, modifié par la L. n° 2018-493, préc., art. 34 (bis), I.
[1497] MEKKI (Mustapha), « Le smart contract, objet du droit (Partie 2) », art. cit.
[1498] CREQUY (Perrine), art. cit.

en plus de permettre la pseudonymisation des informations inscrites, les *blockchains* ont pour principe la mise en place d'un réseau P2P où aucun mineur n'est supérieur à un autre. Cette caractéristique s'est souvent révélée être un atout majeur mais, comment, dans ce contexte, désigner un responsable de traitement ?

202. Aucun responsable à bord de la chaîne ? État des lieux des acteurs et pistes de réflexion. Des auteurs ont proposé de considérer le développeur de l'application, du *smart contract* ou plus largement de la *blockchain* concernée, comme étant le responsable de traitement[1499]. Si une telle solution semble difficile à appliquer concernant les *blockchains* existantes à raison du libre accès à leurs protocoles, de sa modification souvent collaborative et de l'intervention sous pseudonymes de leurs initiateurs comme de leurs utilisateurs[1500] – on pense notamment à *Bitcoin* et son ou ses créateurs dont l'identité demeure, encore aujourd'hui, un secret –, elle pourrait en revanche être une hypothèse à envisager pour les futures *blockchains*. Dès lors que l'identité du développeur serait connue, celui-ci en assumerait *ipso facto* la responsabilité juridique[1501].

Néanmoins, dans l'incertitude d'une identification efficace de ces divers acteurs, il est essentiel de parvenir à désigner un responsable. L'idée est apparue de confier cette tâche de manière ponctuelle et partagée, respectivement à chaque mineur dont le nœud a validé un bloc. D'ailleurs, le règlement lui-même évoque la possibilité de mettre en place une responsabilité conjointe[1502]. Cependant, une telle approche semble *a priori* non seulement imparfaite, car identifier un responsable après que la collecte a été effectuée – laquelle intervient avant l'intégration de l'opération dans un bloc par le mineur – ne permettrait de régler que partiellement le problème puisque, par exemple, cela suggère que la nature, la portée, le contexte et les finalités de la collecte effectuée par le responsable n'ont pas été fixés avant que ladite collecte ait effectivement eu lieu. Mais elle apparaît également contraire aux intérêts du réseau, d'abord parce que l'idéologie *blockchain* bannit toute forme de hiérarchie, et ensuite parce que son fonctionnement serait fragilisé par l'inutile complication qu'elle engendrerait. Notamment, il convient de se demander si les mineurs seraient aussi nombreux s'ils devaient accepter de s'engager dans une telle fonction à responsabilités, si ce n'est peut-être pour une rémunération supérieure. Cette hypothèse n'est donc pas sans soulever quelques difficultés.

[1499] VERBIEST (Thibault), « Blockchain : une révolution juridique ? », art. cit., *loc. cit.*
[1500] MEKKI (Mustapha), « Le smart contract, objet du droit (Partie 2) », art. cit.
[1501] *Id.* L'auteur mentionne notamment l'hypothèse d'une *blockchain* privée.
[1502] Règl. (UE) n° 2016/679, préc., art. 27.

Un parallèle peut être tracé avec la distinction opérée par la doctrine entre les éditeurs et les hébergeurs de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)[1503] en rapport avec leurs équivalents au sens de la loi n° 78-17 du 6 janvier 1978, à savoir les responsables et les sous-traitants de traitement de données à caractère personnel[1504]. La teneur de la responsabilité civile en matière d'activités ou d'informations stockées à la demande d'un destinataire de ces services diffère en effet selon que l'acteur ait un statut d'éditeur ou d'hébergeur. Ce constat conduit à reconsidérer la responsabilité endossée par les mineurs dans le traitement des données personnelles collectées par le protocole sous le prisme de la sous-traitance, plutôt que sur le fondement de la responsabilité du responsable de traitement. Selon la LCEN, l'hébergeur d'un site Internet est la personne physique ou morale qui assure « le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature »[1505], alors que l'éditeur est la personne dont « l'activité est d'offrir un accès à des services de communication au public en ligne » dont il choisit et organise le contenu[1506]. Un arrêt commenté par la doctrine en conclut qu'il est donc « difficile, voire impensable, de demander à un hébergeur de vérifier la conformité des traitements de données de ses clients », ce qui par conséquent ne peut engager sa responsabilité à raison du traitement de données personnelles en tant que responsable de ce traitement[1507]. Au sein d'un système de *blockchain*, un mineur fait partie intégrante du dispositif de distributivité, et contribue pour cela à garder une version à jour de la chaîne en la stockant dans sa machine, tel un hébergeur. À l'instar du régime de responsabilité applicable aux activités ou informations stockées à la demande d'un destinataire de services de communication en ligne, les mineurs ne font que vérifier, par le biais de leurs machines – les nœuds –, la validité des transactions d'un point de vue technique (voire protocolaire) et non qualitatif. D'ailleurs, ils n'offrent pas non plus un accès à des services au public en ligne. Ils ne devraient donc pas engager leur responsabilité à raison du traitement de données personnelles en tant que responsable de ce traitement. La CNIL souligne d'ailleurs qu'ils « se limitent à la validation des transactions que leur soumettent les participants et n'interviennent pas sur l'objet de ces transactions », ils ne déterminent par conséquent ni

[1503] L. n° 2004-575, 21 juin 2004 pour la confiance dans l'économie numérique, *JORF* n° 0143, 22 juin 2004, p. 11168, texte n° 2.
[1504] GALICHET (Charlotte), « Hébergeurs de sites internet : la loi pour la confiance dans l'économie numérique se superpose-t-elle à la loi Informatique et libertés ? », *D. IP/IT* 2019, n° 6, p. 404.
[1505] L. n° 2004-575, préc., art. 6, I, 2.
[1506] *Ibid.*, art. 6, I, 1.
[1507] CA Paris, Pôle 1, 8e Ch., 1er mars 2019, n° 18/15084, comm. Charlotte Galichet, *D. IP/IT* 2019, n° 6, p. 404.

les finalités, ni les moyens à mettre en œuvre[1508]. Plus encore, le mineur héberge la version de la chaîne sans avoir accès aux données y figurant ou, du moins, pas directement, puisque seul le nœud, son ordinateur, les traite pour pouvoir effectuer les calculs nécessaires à la vérification et à la validation des blocs. Il ne les exploite donc pas pour son propre compte, à l'image de l'hébergeur qui « en tout état de cause n'a accès aux données que très rarement, et uniquement pour des interventions techniques »[1509]. Par la suite, seul l'algorithme du protocole continue, en principe, à pouvoir y accéder en cas de besoin pour de futures transactions. En réalité, force est de constater que contrairement aux mineurs, ce sont finalement les utilisateurs qui, presqu'indirectement, choisissent et organisent le contenu des blocs de la chaîne au fil de leurs inscriptions. C'est pourquoi, tout comme une société de services d'hébergement de site(s) web, le mineur d'une *blockchain* devrait être « considéré comme un sous-traitant [qui] ne traite les données qu'il héberge que sur instructions et pour le compte du responsable de traitement », son client, et il ne devrait pas lui incomber de « fournir aux personnes concernées les informations visées par la loi Informatique et libertés (identité du responsable de traitement, finalité du traitement, destinataires, droits des personnes, etc.) »[1510].

Mais il n'en demeure pas moins nécessaire de trouver un responsable. Faut-il alors attacher également une grande importance à la question de savoir *qui*, du mineur ou de l'utilisateur, a la maîtrise des données inscrites sur la chaîne, de sorte à en déduire une plus forte similarité entre éditeurs de site Internet et utilisateurs – plutôt qu'un autre acteur d'une *blockchain* – et ainsi considérer ces derniers comme des responsables de traitement ? L'hypothèse apparaît envisageable, ou, du moins, il semble possible de la soutenir. En effet, il s'agit d'un système fondamentalement autonome car les utilisateurs se gèrent entre eux à travers l'exécution du protocole, ils fixent leurs propres règles à chaque nouvelle transaction – ce qui est d'autant plus vrai en matière de *smart contract* – et finalement mettent en œuvre leur propre vision de la société à l'image de la « démocratie liquide » qu'envisage Vitalik Buterin[1511]. Bien que cette vision soit dépourvue de tiers de confiance, la *blockchain* ne peut garantir seule la protection des données personnelles de chacun sans un représentant qui va « mettre en place et mettre en œuvre un process conformément aux principes de la *compliance* que véhicule la *Privacy by design* », ce qui confirme, selon un auteur, « que le tiers de confiance n'a pas

[1508] CNIL, « Blockchain : Premiers éléments d'analyse de la CNIL », préc., p. 2.
[1509] *Id.*
[1510] GALICHET (Charlotte), « Hébergeurs de sites internet : la loi pour la confiance dans l'économie numérique se superpose-t-elle à la loi Informatique et libertés ? », art. cit., p. 404.
[1511] BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », *github* [liens de publication originaux supprimés] [online], Nov. 2013, https://github.com/ethereum/wiki/wiki/White-Paper.

disparu » en la matière[1512]. De plus, il est inimaginable qu'un quelconque système, sous prétexte que la question de la responsabilité ne fait pas partie des règles initiales, aboutisse à instaurer une irresponsabilité de principe. Étant donné que les données potentiellement personnelles déposées puis traitées par le protocole sont le plus souvent essentielles à la réalisation de l'objectif poursuivi par l'utilisateur ayant recours à la *blockchain*[1513], et que le fonctionnement de cette dernière résulte la plupart du temps d'une volonté et d'un travail de codage effectué par ses utilisateurs et pour ses utilisateurs, il serait simplement question pour eux, de prévoir de modifier le protocole. Si cela n'a pas été fait dès la création par le développeur, ils pourraient en effet se concerter pour inclure une étape d'information et de recueil du consentement des utilisateurs avant toute utilisation, en particulier de ceux qui se manifestent après la mise en réseau du protocole. De cette manière, il appartiendrait à chacun de prendre conscience des droits et obligations qui lui seraient attachés lors de l'utilisation d'une *blockchain* déterminée et d'en accepter le fonctionnement avant d'y accéder. Cela suggèrerait qu'en parallèle, en tant que sous-traitant les mineurs devraient seconder les utilisateurs lorsque l'un d'eux soumet une réclamation visant à exercer ses droits en vertu de la législation sur la protection de leurs données[1514] et ils devront les assister dans le respect des obligations qui incombent au responsable de traitement, notamment pour ce qui est de la sécurité[1515], « par des mesures techniques et organisationnelles appropriées »[1516]. Concernant, par exemple, l'obligation du sous-traitant d' « effacer ou [de] retourner les données au responsable de traitement au terme du contrat »[1517], il apparaît qu'en principe, dès lors qu'un mineur décide de ne plus miner, sa machine se déconnecte automatiquement du réseau et ne reçoit donc plus les mises à jour de la chaîne de blocs.

203. Aucun responsable à bord de la chaîne ? Analyse des propositions formulées par la CNIL. L'idée est d'assurer que les diverses obligations de protection exigées par le règlement puissent être mises en œuvre, tout en veillant à respecter autant que faire se peut les fondements de la technologie. Cela suggère d'organiser une sorte de responsabilité partagée entre tous les acteurs de la *blockchain*, attribuée en fonction du statut et des capacités de chacun. En effet, un utilisateur – autrement dit, un participant avec droit d'écriture au sens de la CNIL – ne peut, par exemple, pas assurer les obligations

[1512] MEKKI (Mustapha), « Le smart contract, objet du droit (Partie 2) », art. cit.
[1513] *Supra* n° 193.
[1514] Règl. (UE) n° 2016/679, préc., art. 28, § 3, f ; art. 32-36.
[1515] Sur l'obligation de sécurité des données, *infra* n° 207.
[1516] HAAS (Gérard), art. cit.
[1517] *Id.*

à la charge du responsable de traitement consistant à modifier des données inscrites. Cette hypothèse serait susceptible toutefois d'entraîner une confusion entre l'utilisateur, considéré en principe comme une « personne protégée », et le « responsable de traitement », bien que cela permettrait de réaliser l'objectif de responsabilisation de la chaîne des acteurs du traitement (*accountability*) initialement fixé par le règlement[1518]. Pour qu'aucun flou ne subsiste, la CNIL évoque elle-même la possibilité de faire endosser aux participants « qui ont un droit d'écriture sur la chaîne et qui décident de soumettre une donnée à la validation des mineurs » la responsabilité du traitement opéré. Elle opère cependant une restriction du champ d'application de cette solution par le biais d'une distinction fondée sur la nature des participants, c'est-à-dire selon qu'ils soient des personnes morales, des personnes physiques exerçant une activité professionnelle ou commerciale, ou non[1519]. Le plus souvent, la personne à l'origine de l'inscription est une entité, telle qu'une *start-up*, une compagnie d'assurances, ou encore un office notarial. Elle prend l'initiative d'organiser l'inscription au sein de la chaîne, par le biais, par exemple, d'une plateforme ou d'une application mise à disposition des clients, ce qui, en principe, devrait engager sa responsabilité vis-à-vis des données à caractère personnel exploitées. Il peut en ce sens s'agir d'un courtier en assurance ayant mis en œuvre un *smart contract* garantissant automatiquement les risques de retards d'avion[1520] ou d'un notaire déposant l'empreinte cryptographique d'un titre de propriété sur la chaîne[1521]. La CNIL insiste donc sur l'impossibilité de considérer une personne physique ayant inscrit des données sur la chaîne en dehors d'une activité professionnelle ou commerciale comme responsable de traitement, en échos au principe d'exception domestique de l'art. 2, § 2, c), du RGPD[1522]. Or, au-delà de l'hypothèse de l'inscription de l'empreinte d'un contrat conclu entre deux personnes privées ou de sa mise à exécution sous la forme d'un *smart contract*, il est fréquent que des individus prennent personnellement et individuellement part à une *blockchain* eu égard au service qu'elle propose et pour lequel elle a été programmée. Dans ce cas, autrement dit selon la CNIL lorsque plusieurs

[1518] CNIL, « Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles ? », art. cit.
[1519] CNIL, « Blockchain : Premiers éléments d'analyse de la CNIL », préc., p. 3. – La CNIL précise d'ailleurs que « les personnes physiques qui inscrivent des données à caractère personnel dans la Blockchain, en dehors d'une activité professionnelle ou commerciale, ne sont pas responsables de traitement (en application du principe d'exception domestique prévu à l'article 2 du RGPD). Par exemple, une personne physique qui procède à la vente ou à l'achat de Bitcoin pour son propre compte n'est pas responsable de traitement. Elle peut en revanche être considérée comme responsable de traitement si elle procède à ces transactions dans le cadre d'une activité professionnelle ou commerciale, pour le compte d'autres personnes physiques. »
[1520] ALLOUCH (Benjamin), « Blockchain et RGPD : une cohabitation en question », *Cryptoast* [en ligne], 11 juill. 2020, https://cryptoast.fr/blockchain-et-rgpd-une-cohabitation-en-question/.
[1521] CNIL, « Blockchain : Premiers éléments d'analyse de la CNIL », préc., *loc. cit.*
[1522] *Id.*

participants décident, de manière conjointe, de mettre en œuvre un traitement ayant une même finalité, à l'instar des assurances P2P[1523] et des *smart grids*[1524], les participants doivent, tels un regroupement de développeurs, s'organiser entre eux pour répondre aux missions incombant au responsable de traitement. Le principe veut qu'ils désignent l'un d'eux comme étant le responsable de traitement mais, à défaut, la CNIL précise qu'ils seront tous « considérés comme ayant une responsabilité conjointe, conformément à l'art. 26 du RGPD et devront donc définir, de manière transparente, les obligations de chacun aux fins d'assurer le respect de la règlementation »[1525].

204. En définitive, il apparaît que la conformité au RGPD ne constitue pas un but inatteignable, simplement elle nécessite une certaine adaptation conjointe de la technologie et des règles en vigueur. Il n'est pas question de brider l'innovation ni l'autonomie de ses utilisateurs, mais plutôt de l'accompagner dans son développement tout en veillant à ce qu'elle évolue en respectant les principes de transparence, de sécurité juridique et de protection assignés à la protection des individus et à la surveillance cohérente du traitement des données à caractère personnel[1526]. La CNIL souligne d'ailleurs que « le RGPD n'a pas pour objectif de réguler des technologies, mais les usages qui en sont faits par les acteurs dans un contexte impliquant des données personnelles »[1527]. Ses encouragements à recourir à des « solutions innovantes », notamment en ce qui concerne la responsabilité des mineurs sous-traitants, dès lors qu'elles permettent aux acteurs de garantir l'application du règlement, suggèrent qu'elle a conscience des difficultés à innover de manière *compliant*, tout en garantissant la conformité *by design*[1528].

B. Un traitement des données neutre mais non limité

205. Licéité et loyauté. La licéité et la loyauté du traitement[1529], premiers principes généraux relatifs à la protection des données inchangé depuis la loi du 6 janvier 1978[1530] et impliquant que le responsable de traitement ait procédé à une collecte, d'une part, conformément aux règles applicables et, d'autre part, sans user de moyens frauduleux,

[1523] Sur les assurances P2P, *supra* n° 50.
[1524] Sur les *smart grids*, *supra* n° 86.
[1525] CNIL, « Blockchain : Premiers éléments d'analyse de la CNIL », préc., p. 3.
[1526] Règl. (UE) n° 2016/679, préc., considérant n° 13.
[1527] CNIL, « Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles ? », art. cit.
[1528] CNIL, « Blockchain : Premiers éléments d'analyse de la CNIL », préc., p. 4.
[1529] *Ibid.*, art. 5, repris par le Règl. (UE) n° 2016/679, art. 5, § 1, a).
[1530] L. n° 78-17, préc., art. 4, 1°.

déloyaux ou illicites, semblent dans le cas de la *blockchain* pouvoir être garantis. En effet, l'utilisateur peut avoir donné son accord au traitement de ses données à caractère personnel « pour une ou plusieurs finalités spécifiques »[1531], ou être partie à un contrat – exécuté sur la chaîne *via smart contract* ou simplement signé et conservé – dont le traitement des données se révèle nécessaire à son exécution[1532]. Quant aux plateformes de *trading* de cryptomonnaies et autres dispositifs de gestion de portefeuilles, il semble qu'il leur soit possible de se prévaloir de leurs obligations légales en matière fiscale[1533] et de KYC[1534] pour arguer la licéité du traitement des données des utilisateurs[1535].

La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique érige le principe d'autodétermination informationnelle[1536] en promouvant les notions de consentement, de transparence, d'information, d'effacement, d'opposition, de rectification, de limitation et de portabilité, énoncées dans le RGPD comme constituant des moyens pour restaurer la confiance de l'usager[1537]. Cependant, l'immuabilité et la pérennité permises par le « dogme du consensus » établi au sein de la *blockchain*[1538] s'avèrent être en conflit avec un certain nombre d'entre elles. Cependant, force sera de constater que la conformité de la technologie des blocs n'en sera toutefois pas forcément si irrémédiablement impactée. Tel que l'a souligné le rapport de Laure De La Raudière et de Jean-Michel Mis à l'Assemblée Nationale, « il n'existe pas d'incompatibilité irrémédiable entre les principes du RGPD – qui présenterait une certaine "plasticité" – et la technologie des *blockchains* »[1539]. C'est dans cette optique que seront évoquées certaines solutions proposées par la doctrine, la CNIL et l'European Parliamentary Research Service (EPRS).

[1531] L. n° 78-17, préc., art. 5, 1° ; Règl. (UE) n° 2016/679, art. 6, § 1, a). – Sur le consentement en matière de *blockchain*, *supra* n° 200.
[1532] L. n° 78-17, préc., art. 5, 2°. – Règl. (UE) n° 2016/679, art. 6, § 1, b).
[1533] Amendement n° II-2523, 13 nov. 2018, au projet de loi de finance n° 1255 pour 2019 (pour les comptes ouverts auprès de plateformes établies à l'étranger) ; CGI, art. 1649 bis C (concernant spécifiquement les *bitcoins* – obligation d'en mentionner le montant sur la déclaration annuelle d'ISF (BOI-PAT-ISF-30-20-10, n° 80)).
[1534] En principe, depuis le 1er janvier 2019, les détenteurs de wallets sont censés déclarer leurs comptes. – World Economic Forum, Deloitte (collab.), « Blueprint for Digital Identity », Industry Project of the Financial Services Community [online], Future of Financial Services Series, Aug. 2016, http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf. – Sur la politique KYC et la lutte contre les activités illégales (blanchiment de capitaux, financement du terrorisme, etc.), *supra* n° 132.
[1535] L. n° 78-17, préc., art. 5, 3°. – Règl. (UE) n° 2016/679, art. 6, § 1, c).
[1536] BARBIER-CHASSAING (Françoise), « Garantir la sécurité des données et mieux prendre en compte la cybercriminalité dans une logique de responsabilisation pour les entreprises », *D. IP/IT* 2019, n° 4, p. 217.
[1537] L. n° 2016-1321 du 7 octobre 2016 pour une République numérique, *JORF* n° 0235, 8 oct. 2016, texte n° 1, art. 1er.
[1538] GODEFROY (Lêmy), « La gouvernementalité des blockchains publiques », art. cit.
[1539] Rapp. AN n° 1501, 12 déc. 2018, de Laure DE LA RAUDIÈRE et Jean-Michel MIS sur les chaînes de blocs (*blockchains*).

206. Portée du droit à l'oubli et à la rectification : l'obligation de modifier la chaîne à l'épreuve du principe d'immuabilité. Prétorien[1540] avant d'être reconnu au niveau réglementaire[1541] puis législatif[1542], le nouveau « droit à l'oubli »[1543] correspond au droit d'obtenir l'effacement de ses données, la cessation de leur diffusion, jusqu'à l'effacement de « tout lien vers [ses] données à caractère personnel, ou de toute copie ou reproduction de celles-ci »[1544], à certaines conditions limitativement énumérées[1545]. L'objectif est de donner à l'utilisateur le pouvoir de retirer son consentement, aussi simplement qu'il l'a donné, à n'importe quel moment, mais également de le protéger d'un traitement illicite de ses données, *a fortiori* s'il s'agit de données jugées sensibles[1546]. Forme de droit à l'oubli[1547], ce droit à l'effacement consacré par le RGPD est plus large que l'inflexible droit au déréférencement consacré par l'arrêt *Google Spain* du 13 mai 2014.

En parallèle, la loi prévoit que les données ne doivent être conservées que pour « une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées »[1548]. Plus encore, le principe est élargi et entraîne un effacement de droit pour toute donnée dès lors qu'elle est accessible au public et aux utilisateurs de la chaîne. Cela implique qu'en principe, après l'exécution puis la finalisation d'un *smart contract*, par exemple, la *blockchain* est censée ne plus pouvoir exploiter les données à caractère personnel correspondantes. Cette durée doit donc être définie en amont du traitement et au moment de la collecte. Le RGPD admet toutefois de déroger à cette règle dès lors que le traitement est nécessaire à l'exercice de la liberté d'expression, au respect d'une obligation légale, et, en particulier, à la constatation, à l'exercice ou à la défense de droits en justice[1549]. Selon certains auteurs, cette exception pourrait également être trouvée au sein de l'art. 23 du RGPD qui envisage la possibilité pour les autorités publiques étatiques de limiter la portée des droits de la personne concernée au nom de « l'intérêt supérieur de

---

[1540] CJUE, 13 mai 2014, n° C-131/12, *Google Spain SL Google Inc c/ Agencia Espanola de Proteccion de Datos, Mario Costeja González.*
[1541] Règl. (UE) n° 2016/679, préc., art. 17.
[1542] L. n° 2018-493, préc., art. 40.
[1543] Il existait, sous l'égide de la L. n° 78-17, 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, un droit à l'effacement. Le Règl. (UE) n° 2016/679 du Parlement européen et du Conseil, 27 avr. 2016, a élargi ce droit préexistant en prenant en compte la jurisprudence *Google Spain* et les débats actuels. – Pour plus de précisions, v., FÉRAL-SCHUHL (Christiane), *CyberDroit : Le droit à l'épreuve de l'Internet*, *op. cit.*, pp. 54-65.
[1544] L. n° 78-17, préc., art. 51, II, modifié par la L. n° 2018-493, préc., art. 1er et 40, II, al. 1er.
[1545] Règl. (UE) n° 2016/679, préc., art. 17, § 1 et 2.
[1546] *Ibid.*, art. 17, § 1, b).
[1547] Il ne s'agit en effet pas du droit à l'oubli à proprement parlé et tel que les partisans de son instauration le requièrent. À ce sujet, v. notamment, KAYSER (Pierre), *La protection de la vie privée*, 3e édition, PUAM, 1995 ; FÉRAL-SCHUHL (Christiane), *CyberDroit : Le droit à l'épreuve de l'Internet*, *op. cit.*, pp. 55-56.
[1548] L. n° 78-17, préc., art. 4, 5°, modifié par la L. n° 2018-493, préc., art. 1er.
[1549] Règl. (UE) n° 2016/679, préc., art. 17, § 3, a) et c).

tiers, y compris de l'initiateur de la *blockchain* »[1550]. Mais encore faut-il que cette exception puisse être légalement admise dans le cas d'une *blockchain*, ou que les délais de prescription ne soient pas dépassés, ce qui rendrait la conservation des données inutiles et donc requerrait leur effacement immédiat[1551].

Dès lors, comment assurer une durée de conservation limitée alors même que la chaîne de blocs est censée être ineffaçable ? La *blockchain* est un système « *append-only* »[1552], ce qui signifie que les données s'ajoutent, mais ne s'effacent pas[1553]. D'autant plus si un seul nœud est identifié comme étant le responsable, à lui seul il n'aurait pas assez de puissance de calcul pour revenir en arrière, c'est-à-dire avant la création du bloc et donc la fixation définitive des données sur la chaîne. Lêmy Godefroy nomme cette spécificité de la *blockchain* « le dogme du consensus », en ce sens qu'il est impossible, sauf consensus de la majorité des mineurs, d'inscrire ou de « désinscrire » une information[1554]. Plus encore, quand bien même seraient-ils plusieurs nœuds à tenter cette opération, une telle configuration semble bien trop aléatoire pour fournir une protection efficace et assurée dans le temps. En effet, poursuivis ou simplement alertés par un des utilisateurs-victime d'une violation de ses données, ils ne semblent pas être en mesure de parvenir au but escompté. La vitesse imposée par le mécanisme de validation des blocs fait d'elle une technologie quasi « *unstoppable* ». D'autant plus que la chaîne se cristallise dans la durée, il serait alors rapidement « trop tard ». Alors que des blocs feraient l'objet d'une modification, des nouveaux s'ajouteraient en continuant de prendre en compte les anciennes versions du bloc en cours de modification, rendant cette hypothèse techniquement non viable. Bien que l'une des spécificités de la technologie implique que les inscriptions, potentiellement détentrices de données à caractère personnel, deviennent moins accessibles à mesure que les blocs s'enchaînent à la chaîne, il semble que cela ne soit pas suffisant pour garantir le droit des personnes physiques à l'effacement de leurs données à caractère personnel.

[1550] POULLET (Yves), JACQUEMIN (Hervé), art. cit., p. 809.

[1551] Finalement, comme le soulignent des auteurs, « *so, as with many issues that arise in data protection law, the appropriate answer to the question of whether a blockchain may be used to process personal data is not binary but rather "it depends"* » [KUNER (Christopher), CATE (Fred H.), LYNSKEY (Orla), MILLARD (Christopher), NI LOIDEAIN (Nora), « Blockchain versus data protection », *International Data Privacy Law*, Vol. 8, No. 2, 2 Jul. 2018, p. 104].

[1552] European Parliamentary Research Service, « Blockchain and the General Data Protection Regulation Can distributed ledgers be squared with European data protection law? », European Parliament [online], Panel for the Future of Science and Technology, Jul. 2019, p. I, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

[1553] CERTES (Nicolas), « Le RGPD, un frein à la blockchain ? », *Le Monde Informatique* [en ligne], 3 août 2018, https://www.lemondeinformatique.fr/actualites/lire-le-rgpd-un-frein-a-la-blockchain-72500.html.

[1554] GODEFROY (Lêmy), « La gouvernementalité des blockchains publiques », art. cit.

Outre la fausse solution consistant à considérer le droit à l'oubli comme un droit subjectif auquel son propriétaire peut librement renoncer[1555], pour contourner ce problème technique, il convient de se demander s'il existerait un moyen de programmer le protocole, ou d'inscrire une nouvelle inscription de type *ledger* ou *smart contract*, qui interdirait à la *blockchain* elle-même d'afficher les données en clair passé un certain délai. L'idée serait de rompre algorithmiquement le lien vers les données contenues dans des anciens blocs, par exemple à partir du $x^{ème}$ bloc à compter du dernier validé, hormis pour effectuer les vérifications nécessaires à la validation des futures transactions, telles que concernant la balance des paiements ou encore la solvabilité des adresses de l'émetteur[1556]. Reste qu'un tel dispositif demeure soumis à sa faisabilité, et au-delà, ne fait que rendre difficile l'accès à l'information sans l'effacer. Mais, « rendre difficile l'accès à l'information », ne s'agit-il pas justement d'une forme d'effacement et, au mieux, de *déréférencement*, à l'image de ce qui est opéré dans le domaine des sites Internet et des moteurs de recherche[1557] ? Bien qu'il ne semble pas exister de consensus au sein de l'UE sur ce point, les autorités de protection des données de certains États membres à l'instar de l'Autriche et, anciennement, du Royaume-Uni, se sont révélés plus flexibles dans leur appréciation des moyens techniques choisis pour procéder à un effacement en acceptant que l'anonymisation[1558] et la « mise hors d'usage » (dérivé de « *put beyond use* »[1559]) soient suffisantes[1560]. Une auteure propose ainsi de paramétrer le protocole pour qu'il anonymise automatiquement les données au bout d'un temps prédéfini[1561]. Il s'agirait de rendre toute identification impossible à partir des informations contenues dans les blocs enchaînés depuis *x* jours, tout en laissant le protocole accéder

[1555] V., Rapport Groupe Fintech, « Les impacts des réseaux distribués et de la technologie blockchain dans les activités de marché », Paris EUROPLACE [en ligne], 23 oct. 2017, p. 83, https://www.paris-europlace.com/sites/default/files/public/paris_europlace_-_livre_blanc_blockchain_-_26_octobre_2017.pdf (promeut cette solution) ; MEKKI (Mustapha), « Le smart contract, objet du droit (Partie 2) », art. cit. (rejette cette hypothèse, considérant que, « même si la qualification de droit subjectif l'emporte, ces clauses de renonciation ne vont-elles pas être jugées excessives en ce qu'elles portent une atteinte substantielle à ce droit et constituent en ce sens une atteinte disproportionnée ? »).

[1556] Sur l'étape de vérification consistant à s'assurer de l'absence de « double dépense », *supra* n° 143.

[1557] Il s'agit notamment de l'arrêt Google Spain du 13 mai 2014, qui consacre le droit au déréférencement [CJUE, 13 mai 2014, n° C-131/12, *Google Spain SL Google Inc c/ Agencia Espanola de Proteccion de Datos, Mario Costeja González*].

[1558] Datenschutzbehörde, DSB-D123.270/0009-DSB/2018, 5 Dez. 2018, https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00.html.

[1559] Information Commissioner's Office, « Right to erasure », *ico*. [online], https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/.

[1560] V. également sur le sujet, FINCK (Michèle), « Blockchain and the General Data Protection Regulation Can distributed ledgers be squared with European data protection law? » *in* Panel for the Future of Science and Technology (STOA), European Parliament Research Service (EPRS) [online], Jul. 2019, pp. 75-76, http://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2019)634445.

[1561] GUILHAUDIS (Élise), art. cit., p. 13.

aux données nécessaires à son fonctionnement. De la même manière, la CNIL suggère de se *rapprocher* d'une conformité au RGPD en rendant la donnée « quasi inaccessible » lorsque celle-ci provient d'un procédé cryptographique[1562]. Étant donné que les mineurs ne peuvent effectivement pas satisfaire l'obligation d'effacement directement, il s'agirait pour le responsable de traitement de supprimer les éléments permettant tant la preuve que la vérification de l'intégrité d'une donnée cryptée, à l'instar de la clé privée d'une fonction de hachage[1563]. Sans toutefois mettre les différents protocoles sur le même plan, nous pensons que les applications en matière d'identification par *blockchain*[1564] pourraient s'inspirer des protocoles à la base d'Internet. À l'instar du protocole *OAuth* de délégation d'autorisation pour le web[1565], celui de la *blockchain* pourrait plus particulièrement intégrer des solutions permettant de réguler l'accès direct à certaines données contenues dans les blocs de transactions. Par le biais de *tokens* d'accès dont il contrôlerait la distribution, le protocole délivrerait des autorisations non seulement ponctuelles mais également temporaires. À ces *tokens* pourraient en effet être attachées des conditions à la fois de temps, comme une date de péremption prédéfinie – date après laquelle le *token* n'est plus valable et son accès est automatiquement refusé –, et de consentement, pour laisser la possibilité à l'utilisateur de révoquer le *token* à tout moment. Il convient toutefois de veiller à ce que le protocole de la *blockchain* puisse de son côté continuer à avoir accès aux données dont il a besoin pour fonctionner, en particulier les éléments nécessaires à la vérification de la chaîne de transactions. Pour garantir toutefois l'inaccessibilité de ces dernières données, notamment au bout d'un temps prédéfini, le protocole pourrait éventuellement utiliser une méthode de chiffrement qui lui permettrait de procéder aux calculs nécessaires sans qu'il ait besoin de déchiffrer les données. Il conviendrait alors de se rapprocher des techniques de chiffrement homomorphe, qui constituent d'ailleurs un domaine de recherche actif[1566]. Sinon, le protocole devrait prévoir de rendre les données simplement illisibles, à condition qu'il puisse toujours y accéder. Cette exigence conduit donc à effectuer une distinction entre les données pouvant faire l'objet d'une sécurisation *via* autorisation d'accès, et les données nécessaires au fonctionnement de la chaîne ne pouvant pas être complètement anonymisées ou

[1562] CNIL, « Blockchain : Premiers éléments d'analyse de la CNIL », préc., p. 8.
[1563] *Ibid.*, pp. 8-9.
[1564] *Supra* n°s 132 et s.
[1565] Pour plus de précisions sur le protocole *OAuth*, v. notamment, GABILLON (Alban), GALLIER (Romane), BRUNO (Emmanuel), « Access Controls for IoT Networks », *SN Computer Science* 2020 [online], n° 24, Sept. 2019, p. 11, https://doi.org/10.1007/s42979-019-0022-z ; Hardt (Dick), « The OAuth 2.0 authorization framework », *tools.ietf.org* [online], Oct. 2012, https://tools.ietf.org/html/rfc6749.html #section-1.4.
[1566] DELAHAYE (Jean-Paul), « Déléguer un calcul sans divulguer ses données », *Pour la Science*, n° 456, oct. 2015.

obstruées. Finalement, sans toutefois constituer un effacement au sens strict, enrayer l'accès aux données permet, à tout le moins, de reproduire ses effets, et *a fortiori*, tel que le constate la CNIL, « de se rapprocher de l'exercice effectif de son droit à l'effacement pour la personne concernée »[1567]. La CNIL souligne par ailleurs que le meilleur moyen d'assurer ce droit à l'effacement est simplement de s'abstenir d'inscrire une donnée à caractère personnel lorsque celle-ci apparaîtra en clair sur la chaîne, à moins de la crypter[1568].

La question s'est donc posée de savoir si le même raisonnement pouvait être appliqué au droit dont dispose l'utilisateur[1569], ou les ayants-droit de celui-ci[1570], de rectifier et de mettre à jour ses données[1571]. Corollaire du principe d'exactitude de l'art. 5, d, du RGPD, l'exigence d'actualisation des données à caractère personnel inexactes requiert, soit un effacement, soit une rectification. Toutefois, la rectification est, en principe, aussi impossible d'un point de vue technique que l'effacement. Le risque est effectivement de faire face à des problématiques similaires. Cependant, les deux ne sont pas tout à fait identiques et l'adaptation de la pratique de l'avenant à la *blockchain* semble pouvoir dans ce cas être envisagée comme une solution à l'immuabilité de la chaîne. C'est en tous cas l'idée développée par la CNIL et qui consiste, selon elle, à « annuler » les informations périmées[1572]. La rectification par avenant n'interviendrait toutefois sur la chaîne que d'un point de vue temporel puisqu'il serait question d'intervenir, non sur des blocs d'ores et déjà validés, mais au niveau de la mise à jour de la chaîne, en créant un nouveau bloc rectificatif. Les informations initiales y demeureraient donc inscrites et visibles mais ne seraient plus exploitées par le protocole[1573], puisque le traitement s'effectuerait à partir des informations rectifiées, autrement dit en accord avec le principe d'exactitude du RGPD.

Finalement, bien que la technologie semble souvent difficilement conciliable sur ces points, elle est relayée par l'apparente flexibilité du RGPD qui laisse envisager la possibilité de prendre en compte des « difficultés techniques », pour autant que la protection des données soit pleinement assurée[1574].

[1567] CNIL, « Blockchain : Premiers éléments d'analyse de la CNIL », préc., p. 9.
[1568] *Ibid*., p. 10.
[1569] L. n° 2018-493, préc., art. 40.
[1570] Décr. n° 2007-451, 25 mars 2007, modifiant le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la Loi n° 2004-801 du 6 août 2004, *JORF* n° 74, 28 mars 2007, texte n° 30, art. 100.
[1571] CREQUY (Perrine), art. cit.
[1572] CNIL, « Blockchain : Premiers éléments d'analyse de la CNIL », préc., p. 10.
[1573] *Id.*
[1574] Règl. (UE) n° 2016/679, préc., art. 17, § 2. – V. également, VERBIEST (Thibault), « Blockchain : une révolution juridique ? », art. cit., *loc. cit.*

207. Accessibilité des données au sein de l'UE et en dehors de l'UE : analyse des conséquences sur la sécurité des données. Selon la réglementation protectrice des données à caractère personnel, il est exclu que des données apparaissent ou soient transférées à destination d'États qui n'assurent pas un niveau de protection *a minima* équivalent à celui du droit de l'UE[1575]. Le caractère international de la *blockchain* ne fait pas exception puisque le champ d'application territorial du RGPD s'étend expressément à tous responsables de traitement et sous-traitants établis au sein de l'UE ou hors des frontières de l'UE, traitant des données de résidents européens[1576]. À défaut donc pour les États tiers dans lesquels les informations contenues sur la *blockchain* sont susceptibles d'être transférées, notamment lors des mises à jour de la chaîne, de pouvoir bénéficier des exceptions limitativement énumérées, la question de la conformité de la *blockchain* se posera. Il s'agit notamment des cas où l'État possède une décision d'adéquation de la Commission reconnaissant un niveau de protection des données répondant aux exigences européennes[1577], ou lorsque la technologie prévoit dès sa conception[1578] des « garanties appropriées » et « à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives »[1579], ou, pour finir, lorsque le transfert de données correspond à une des exceptions au principe d'interdiction du transfert, telle que le recueil du consentement express de la personne concernée ou la nécessité du transfert pour l'exécution d'un contrat[1580]. Or, quel que soit le responsable de traitement et quelle

[1575] GUILHAUDIS (Élise), art. cit., p. 13.
[1576] Règl. (UE) n° 2016/679, préc., art. 3.
[1577] *Ibid.*, art. 45. – À ce sujet, la Commission publie au Journal officiel de l'Union européenne (JOUE) la liste des États bénéficiant de cette décision d'adéquation. Jusqu'ici, la Commission européenne a reconnu les États suivants : Andorre, Argentine, Canada (organisations commerciales), Îles Féroé, Guernesey, Israël, Île de Man, Japon, Jersey, Nouvelle-Zélande, Suisse, Uruguay et États-Unis d'Amérique, comme assurant une protection adéquate. Liste et décisions disponibles en ligne : https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
[1578] Règl. (UE) n° 2016/679, préc., art. 25.
[1579] Il s'agit de celles fournies « sans que cela ne nécessite une autorisation particulière d'une autorité de contrôle », par : « - (a) un instrument juridiquement contraignant et exécutoire entre les autorités ou organismes publics, - (b) des règles d'entreprise contraignantes, - (c) des clauses types de protection des données adoptées par la Commission, ou - (d) adoptées par une autorité de contrôle et approuvées par la Commission, - (e) un code de conduite approuvé, - (f) un mécanisme de certification approuvé » [*Ibid.*, art. 46, § 2]. V. également *Ibid.*, art. 42, notamment § 1 : « Les États membres, les autorités de contrôle, le comité et la Commission encouragent, en particulier au niveau de l'Union, la mise en place de mécanismes de certification en matière de protection des données ainsi que de labels et de marques en la matière, aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le présent règlement. » – Pour plus de précisions sur le sujet, v. FÉRAL-SCHUHL (Christiane), *CyberDroit : Le droit à l'épreuve de l'Internet*, *op. cit.*, pp. 166 et s.
[1580] *Ibid.*, art. 49, § 1 : « a) la personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées ; b) le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée ; c) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale ; d) le transfert est nécessaire pour des motifs importants d'intérêt public ; e) le transfert est nécessaire à la constatation, à l'exercice ou à la défense de

que soit la *blockchain*, réguler la destination des transactions comme celle des mises-à-jour n'est pas possible. Partant du constat que le responsable de traitement peut, en effet, « difficilement exercer un contrôle sur la localisation des mineurs », la CNIL en déduit qu'il sera plus difficile de mettre en œuvre des solutions contractuelles telles que des clauses contractuelles types, des règles d'entreprises contraignantes, des codes de conduite ou encore des mécanismes de certification, et d'adapter la technologie aux exigences en matière de transferts hors UE[1581].

Cependant, il est nécessaire de constater deux choses. D'une part, la technologie repose sur des principes et des dispositifs majoritairement axés sur la sécurité. Tel que le souligne Mustapha Mekki, « la transparence, le pseudonymat et les technologies de signature et d'horodatage numériques permettent de protéger les données personnelles », ce qui fait de la *blockchain* « un atout et non un danger pour ces données »[1582]. D'autre part, eu égard à l'application obligatoire du règlement et des exigences en matière de sécurité, si les données seront peut-être visibles aussi bien en UE qu'en dehors de l'UE, il n'en demeure pas moins que les règles de fonctionnement du protocole resteront elles aussi identiques, à la fois en UE et en dehors de l'UE. En toute logique, à partir du moment où les exigences sont remplies et jugées adéquates au sein de l'UE, elles le demeureront hors UE. En revanche, la difficulté pourrait émaner de l'impératif selon lequel toute *blockchain* accessible aux ressortissants de l'UE doit respecter les principes du RGPD, autrement dit, y compris dans le cas où son protocole serait développé hors UE.

Par ailleurs, l'une des recommandations générales en matière de sécurité formulée par la CNIL consiste à mettre en place « des procédures techniques et organisationnelles […] permettant de modifier les algorithmes lorsqu'une vulnérabilité est identifiée », notamment sous la forme d'un plan d'urgence[1583]. Il semble pourtant que ce système de mise à jour de protocole face aux nouvelles menaces fait parties des règles de principes au sein des écosystèmes des *blockchains*. En règle générale, dès lors qu'un utilisateur

droits en justice ; f) le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ; g) le transfert a lieu au départ d'un registre qui, conformément au droit de l'Union ou au droit d'un État membre, est destiné à fournir des 'informations au public et est ouvert à la consultation du public en général ou de toute personne justifiant d'un intérêt légitime, mais uniquement dans la mesure où les conditions prévues pour la consultation dans le droit de l'Union ou le droit de l'État membre sont remplies dans le cas d'espèce. »

[1581] CNIL, « Blockchain : Premiers éléments d'analyse de la CNIL », préc., p. 6.

[1582] MEKKI (Mustapha), « Le smart contract, objet du droit (Partie 2) », art. cit. L'auteur précise d'ailleurs que « la transparence et la traçabilité qu'offre la *blockchain* permettent de vérifier qui a utilisé les données et comment [Sur ce point, v. J. Deroulez, Blockchain et données personnelles. Quelle protection de la vie privée ?, *JCP* n° 38, 18 sept. 2017. 973] et de limiter l'accès aux données sécurisées aux seules personnes concernées [Sur ce point, G. Zyskind, O. Nathan et A. Pentland, White paper. Decentralizing Privacy: using blockchain to protect personal data, www.enigma.co/ZNP15.pdf] ».

[1583] CNIL, « Blockchain : Premiers éléments d'analyse de la CNIL », préc., p. 11.

identifie une faille dans le système potentiellement exploitable par un *hacker*, les dispositifs annexes des *blockchains*, le plus souvent des plateformes libres à l'instar de *GitHub* pour *Bitcoin*, permettent aux membres de l'écosystème de donner l'alerte et d'accéder aux codes sources hébergés pour corriger les vulnérabilités, après un vote selon les principes du consensus.

208. La nécessité d'éclaircir les contradictions subsistantes dans l'intérêt double de l'innovation et de la protection des individus. Avant 2019, certains auteurs et même l'Observatoire européen en matière de *blockchain*, annonçaient que si la Commission et le Parlement européen ne se décidaient pas rapidement à s'intéresser à la technologie et aux modalités de son utilisation, « les tests et développement de produits et services basés sur *blockchain* pourraient être avortés »[1584]. Face à une redoutable concurrence provenant à la fois de Chine et des États-Unis, cette décision semble être d'une importance fondamentale pour l'essor de la technologie[1585]. De plus, contrairement à certains tiers de confiance actuels qui n'ont pas toujours fait preuve d'*accountability* dans leurs traitements de données à caractère personnel[1586], si la *blockchain* s'avère en non-conformité avec certaines exigences du règlement, eu égard à son statut de technologie encore émergeante, la société ne sera pas aussi conciliante. Les dommages en termes de réputation et de confiance pourraient être inéluctables. L'idée est d'instaurer la confiance dans la *blockchain* et de restaurer celle vis-à-vis des acteurs économiques tout en les responsabilisant, par le biais d'un renforcement des droits des individus vis-à-vis de leurs données. Concernant les innovations d'une manière générale, il ne s'agit pas, tel que le souligne des auteurs, d'être « contre-productif »[1587], de constituer un frein[1588], ou bien encore « de protéger [uniquement] les personnes contre les risques des technologies ou de rendre celles-ci plus "acceptables" socialement » au risque de renoncer à leurs propres particularismes et leur capacité à faire évoluer les pratiques des secteurs dans lesquels elles s'implantent[1589]. Mais, il s'agit « d'éviter que des atteintes volontaires ou

[1584] CERTES (Nicolas), « Le RGPD, un frein à la blockchain ? », préc. – V. également, CREQUY (Perrine), art. cit.
[1585] The European Union Blockchain Observatory & Forum, « Blockchain innovation in Europe », European Commission [online], 27 Jul. 2018, https://www.eublockchainforum.eu/sites/default/files/reports/20180727_report_innovation_in_europe_light.pdf.
[1586] V. les affaires mettant en cause *Facebook*, *Yahoo*, *Google* [*supra*, n° 1] et notamment *Firefox* [OSBORNE (Charlie), « Une extension Firefox collecte les données de navigation de 200 000 utilisateurs », *ZDNet* [en ligne], 16 août 2018, https://www.zdnet.fr/actualites/une-extension-firefox-collecte-les-donnees-de-navigation-de-200000-utilisateurs-39872453.htm].
[1587] ROTILY (Cassandra), ARCHAMBAULT (Laurent), « Drones civils professionnels et RGPD : enjeux liés à la collecte des données personnelles et au respect de la vie privée », *D. IP/IT* 2019, n° 6, p. 376.
[1588] MEKKI (Mustapha), « Le smart contract, objet du droit (Partie 2) », art. cit.
[1589] Mustapha Mekki souligne d'ailleurs que l'encadrement juridique « ne doit pas être un frein au développement d'une technologie pleine de promesses sur le plan économique » [*id.*].

involontaires aux droits des personnes se multiplient à l'avenir »[1590]. La CNIL indique d'ailleurs que la mise en place des diverses solutions permettant d'adapter et/ou de s'adapter à la technologie nécessiteront une évaluation approfondie[1591]. Également questionné à ce sujet, le Parlement européen, sous la plume de son service de recherche, a mis en exergue la particularité et la multiplicité des *blockchains* pour soulever lui aussi, tout au long de son rapport, l'importance de l'analyse au cas par cas de la nécessité ainsi que de la compatibilité de chaque solution envisagée – qu'il s'agisse de déterminer si les données traitées donnent lieu à l'application du règlement ou encore de distinguer les responsables des sous-traitants, par exemple[1592]. Instrument d'une « conciliation subtile entre principe d'innovation et principe de précaution »[1593], la réalisation d'une étude d'impact relative à la protection des données (AIPD) avant la mise en œuvre du traitement pourra permettre de vérifier et, le cas échéant, de démontrer la conformité opérationnelle du dispositif.

209. Bien qu'il soit possible de s'adapter, l'immuabilité de la chaîne de blocs s'avère problématique au-delà des questions de droit à l'oubli et de responsabilité des traitements de données à caractère personnel, en particulier en ce qui concerne la pratique des relations contractuelles.

Section 2. Le principe d'exécution intégrale face à la pratique des relations contractuelles

210. Le code d'une *blockchain* est « *unstoppable* », ce qui signifie qu'il s'exécute jusqu'à avoir intégralement achevé l'ensemble des tâches – ou opérations – qui lui ont été confiées par le codeur. Née de l'immuabilité de la chaîne[1594], cette caractéristique apparaît tout à fait cohérente. De cette manière, un drone piloté par son propre algorithme qui emprunterait la trajectoire définie par son code ne devrait donc, *a priori*, s'arrêter que lorsque son programmeur en a pré-décidé ainsi. Seulement, lorsqu'un drone, actionné par un *smart contract* exécuté sur la *blockchain Ethereum*, s'est élevé dans le ciel russe le 6

[1590] CNIL, « Drones et vie privée : un cadre à inventer, Rapport annuel d'activité », *CNIL* [en ligne], 2014, p. 27, https://bit.ly/2KlvLCy.
[1591] CNIL, « Blockchain : Premiers éléments d'analyse de la CNIL », préc., p. 10.
[1592] European Parliamentary Research Service, « Blockchain and the General Data Protection Regulation Can distributed ledgers be squared with European data protection law? », *European Parliament* [online], Panel for the Future of Science and Technology, Jul. 2019, p. I.
[1593] MEKKI (Mustapha), « Le smart contract, objet du droit (Partie 2) », art. cit.
[1594] Sur les systèmes permettant l'immuabilité de la *blockchain*, *infra* n°s 147 et s.

mars 2016 et a échappé au contrôle des opérateurs, cela n'a pas été sans soulever de difficultés. En effet, volontairement dépourvu d'intermédiaire disposant de commandes annexes de pilotage[1595], les opérateurs ont été contraints d'opérer manuellement sa mise hors tension, laquelle était la seule façon de reprendre le contrôle de l'engin. Personne n'a réussi et n'aurait réussi à dévier informatiquement sa direction[1596]. Cependant, *quid* de la personne pouvant se trouver sur la trajectoire du drone si l'algorithme de ce dernier ne l'a pas prévu ? Une prise en compte anticipée de ce type de difficultés aurait sûrement pu éviter les risques encourus d'incidents. Finalement, au-delà de la question d'en imputer ou non la responsabilité à la technologie, force est de constater la rigidité du système. Un code sur *blockchain* est écrit puis s'exécute, il est « *unstoppable* ». Il est donc essentiel de parvenir à identifier les conséquences du caractère « inarrêtable » de la technologie, tant vis-à-vis d'elle-même que vis-à-vis de ses utilisateurs, pour ensuite évaluer les solutions et adapter les comportements.

Même si en règle générale il ne s'agit pas, pour les parties à un contrat « blockchaîné », de coder un contrat pour donner vie à un drone, une telle indifférence technologique suggère qu'il faille cibler ses effets au sein de la relation contractuelle afin de prendre conscience de l'ampleur de la rigidité de la chaîne de transactions utilisée (§ 1). Pour tenter de dissiper ses conséquences, il semble qu'il faille renouer avec les pratiques relationnelles humaines, ce qui commencera par reconnaître l'importance du rôle joué par l'Homme dans ces hypothèses (§ 2).

§ 1. La rigidité de la chaîne de transactions

211. En matière contractuelle, cette rigidité algorithmique se manifeste sous la forme d'une immobilisation des termes du contrat, empêchant les parties de revenir sur les modalités d'exécution ou sur l'existence et la portée de leurs engagements. Présente à deux niveaux, cette rigidité rend donc, d'une manière générale, à la fois impossible non seulement la modification du contrat (A) mais également son annulation (B).

[1595] LEVICH (Andrew), « "Drone employee" at Blockchain & Bitcoin Conference Russia 2016 », *CoinFox* [online], 14 Apr. 2016, http://www.coinfox.info/news/5302-drone-employee-at-blockchain-bitcoin-conference-moscow.

[1596] DE FILIPPI (Primavera), WRIGHT (Aaron), « The Blockchain of Things », *Slate* [online], 19 Jun. 2018, https://slate.com/technology/2018/06/blockchain-is-likely-to-advance-the-internet-of-things-and-robot rights.html.

212. Une technologie plus ferme que la position de la Cour de cassation concernant la théorie de l'imprévision[1597]. La technologie offre au contrat un moyen de renforcer la force obligatoire de ses dispositions dont la qualité repose sur son caractère intangible. Selon Alfred Fouillé, « qui dit contractuel dit juste »[1598], seulement, comme un effet secondaire logique de l'immuabilité, la chaîne de blocs ne conçoit en principe ni les retards, ni les changements, ni même les rectifications et ce, quel qu'en soit le motif, y compris s'il est légitime.

En effet, il s'avère que la *blockchain* éprouve des difficultés protocolaires à prendre en compte et à faire face aux événements imprévisibles[1599]. À défaut d'être préalablement indiquée dans le protocole ou dans le code du *smart contract*, en règle générale, dès lors qu'une situation est inconnue pour l'algorithme, elle le demeurera et la *blockchain* ne pourra réagir d'aucune manière. Qu'il s'agisse d'un « évènement échappant au contrôle du débiteur » (C. civ., art. 1218) ou d'un « changement de circonstances imprévisible » intervenu postérieurement à l'inscription de la transaction sur la *blockchain* ou à celle du *smart contract* (C. civ., art. 1195), en principe la chaîne ne peut pas s'y adapter. Il semble alors que les parties seraient condamnées à supporter un risque qu'elles n'avaient pas accepté d'assumer, allant à rebours du principe de fidélité au contrat tel qu'institué par la doctrine, et du « "maintien de la proportion voulue" (à l'origine) »[1600].

Jusqu'à ces dernières années, cette modalité aurait pu satisfaire la jurisprudence, relativement hostile, de la Cour de cassation en matière d'imprévision[1601]. Cependant, le droit a évolué et le « canot de sauvetage à trois étages » du dispositif de l'ordonnance de 2016, par ailleurs confirmé[1602] après avoir éprouvé nombre de difficultés pour

---

[1597] René Demogue indiquait dans son Traité [DEMOGUE (René), *Traité des obligations en général*, t. 6, 1931, ed. A. Rousseau, n° 634 bis] que, « depuis longtemps », la jurisprudence de la Cour de cassation « refuse d'une façon très ferme d'adopter la théorie de l'imprévision ».

[1598] Citation d'Alfred Fouillé, v. notamment, ROLLAND (Louise), *« Qui dit contractuel, dit juste.» (Fouillée) ... en trois petits bonds, à reculons*, éd. R.D. McGill, 2006.

[1599] MEKKI (Mustapha), « Les mystères de la blockchain », *D.* 2017, n° 37, pp. 2160 et s., n° 28.

[1600] TRIGEAUD (Jean-Marc), *Justice et fidélité dans les contrats*, coll. Arch. Phil. dr., vol. 28, éd. Sirey, 1983, p. 20, cité par LE TOURNEAU (Philippe), POUMARÈDE (Matthieu), « La bonne foi dans l'exécution du contrat », *Rép. civ. Dalloz*, v° Bonne foi, 2019, n° 81. V. également, *ibid.*, n°s 77-82.

[1601] Sur le refus de la Cour de cassation de reconnaître la théorie de l'imprévision, v. notamment, ANCEL (Pascal), « Imprévision – Approche historique et comparative », *Rép. civ. Dalloz*, v° Imprévision, 2018, n°s 14 et s. ; PICOD (Yves), « CONTRAT. – Force obligatoire du contrat. – Bonne foi », *JCl. Civil Code*, Art. 1103 et 1104, fasc. Unique, n°s 53-55.

[1602] Ord. n° 2016-131, 10 février 2016, portant réforme du droit des contrats, du régime général et de la preuve des obligations, *JORF* n° 0035, 11 févr. 2016. Confirmé par la L. n° 2018-287, 20 avr. 2018, ratifiant l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, *JORF* n° 0093, 21 avr. 2018.

s'imposer[1603], ne semble pas être en mesure de s'appliquer aussi naturellement que le voudrait la loi[1604]. Par ailleurs, en estimant que le juge intervienne, qu'adviendrait-il de sa décision au sein de la chaîne de blocs ? Disposerait-elle d'une force exécutoire équivalente[1605] ?

213. Une impossibilité de modification favorisant les hypothèses de déséquilibre contractuel. Ayant, par le passé, déjà été confronté aux conséquences négatives de l'intangibilité du contrat, le législateur de 2016 a également montré la volonté de prendre en considération les hypothèses de déséquilibre *ab initio*. S'inspirant du régime éminemment protecteur du droit de la consommation en matière de lutte contre les clauses abusives (C. consom., art. L. 212-1 et s.), l'ordonnance a élargi cette protection à tous les contrats d'adhésion, quelle que soit la qualité des parties (C. civ., art. 1171). Or, la pratique révèle que dans ce type de rapports contractuels, l'un des contractants est malgré tout systématiquement empêché de négocier les termes de ses propres engagements. Par conséquent, la loi impose qu'en parallèle, jouissant des avantages de la forme du contrat, son cocontractant doive stipuler un certain nombre de mentions protectrices (C. civ., art. 1110)[1606]. Par ailleurs, outre le déséquilibre qui serait dû à un défaut d'équivalence (C. civ., art. 1168) ou à une erreur sur la valeur qui n'est, en soi, pas une cause de nullité[1607], qu'en serait-il si un contrat inscrit s'avérait en réalité lésionnaire (C. civ., art. 1148, 1149, 1674, 889, 131-5) ? Dans ces différentes situations, avant d'évoquer les facteurs de nullité, un correctif pourrait être appliqué. Bien qu'en principe les parties puissent corriger leur oubli, il semble que l'immuabilité caractéristique de la *blockchain* contribuerait néanmoins à faire obstacle à toute rectification. Toutefois, si un tel correctif pourrait éventuellement être mis en œuvre sous la forme d'un avenant sur la *blockchain*, il reste qu'il exige l'accord des deux parties puisque les clés privées des deux utilisateurs sont nécessaires pour finaliser un contrat sur la chaîne de blocs. Encore faut-il pour cela que le créancier accepte d'agir spontanément pour rééquilibrer la réciprocité et/ou la proportionnalité du contrat conclu[1608] notamment en ce qui concerne les droits et obligations des parties, ainsi que le prix excessivement réduit par rapport à la prestation

[1603] ANCEL (Pascal), *op. cit.*, n°s 22 et s.
[1604] BENABENT (Alain), *Droit des obligations*, éd. LGDJ, 18e édition, coll. Précis Domat, Privé, 2019, p. 250.
[1605] LEGEAIS (Dominique), « Blockchain », *JCl. Sociétés Traité*, fasc. 2160, n° 55. – Sur ces questions, *infra* n°s 229 et s.
[1606] Sur la question des contrats d'adhésion, *infra* n° 213.
[1607] GUERLIN (Gaëtan), « Considérations sur les smart contracts », *D. IP/IT* 2017, n° 10, p. 512. – Cass. Civ. 3e, 12 juin 2014, n° 13-18.446, dite « Affaire Poussin ».
[1608] CHANTEPIE (Gaël), SAUPHANOR-BROUILLAUD (Natacha), « Déséquilibre significatif », *Rép. com. Dalloz*, v° Déséquilibre significatif, 2019, n° 139.

fournie en retour. L'immuabilité de la chaîne empêchant par principe de revenir sur ses engagements œuvrerait ainsi sans le vouloir pour le renforcement du déséquilibre contractuel potentiellement existant, et risquerait finalement d'entraîner une recrudescence de la « loi du plus fort ».

214. L'effectivité d'un accord synallagmatique portant sur la rectification du contrat. Si une erreur matérielle se glisse dans le *smart contract* et que celle-ci ne peut être rectifiée, tel un assuré qui renseigne incorrectement les formulaires qui lui sont présentés, les parties peuvent être privées de certaines garanties ou clauses spécifiques. D'une manière générale, la force du contrat implique que les conventions « ne peuvent être modifié[e]s ou révoqué[e]s que du consentement mutuel des parties, ou pour les causes que la loi autorise » (C. civ., art. 1103). Or, en utilisant la *blockchain*, même une modification synallagmatique des termes du contrat par les deux parties, conjointement, ne pourrait être véritablement effective. En effet, même s'il advient que les parties décident de conclure une forme d'avenant sur la *blockchain*, celui-ci n'aurait que pour effet de rendre exécutoire de nouveaux termes, tout en laissant les anciens, inefficaces et donc inexécutables. En d'autres termes, l'assuré ne pourrait, en principe, pas récupérer ce qu'il a perdu du fait de son erreur.

B. Impossibilité d'annuler le contrat

215. Un retour au *statu quo ante* inconcevable. L'une des qualités techniques de la *blockchain* est probablement sa première limite du point de vue du droit. L'enjeu réside dans le couple formé par la décentralisation et l'immuabilité, autrement dit dans l'impossibilité de supprimer les transactions inscrites, quand bien même elles se révèleraient entièrement illicites ou illégales[1609]. Peut ainsi prêter à discussion, par exemple, l'affaire « *Augur* », du nom de la plateforme de prédictions qui permet de s'engager dans de multiples paris proposés par les utilisateurs, et qui a notamment permis que 1 500 dollars soient mis en jeu sur la probabilité que Donald Trump soit assassiné dans le courant de l'année 2018[1610]. Un autre projet de *blockchain* ayant vraisemblablement été soutenu depuis la Californie (États-Unis), proposait pour sa part de « défendre les libertés individuelles » en mettant en œuvre un « marché décentralisé

[1609] BERBAIN (Côme), « La blockchain : concept, technologies, acteurs et usages », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 3.
[1610] Pour plus de précisions sur le sujet, v., WILMOTH (Josiah), « First Assassination Markets Appear on Prediction Platform Augur », *CCN* [online], 24 Jul. 2018, https://www.ccn.com/first-assassinationmarkets appear-on-gambling-platform-augur/.

du sexe ». L'application était présentée sous la forme d'un catalogue de travailleuses du sexe stocké sur un réseau de réseaux intraçables[1611], qui proposait de communiquer une proposition dématérialisée à la partenaire sélectionnée, valant demande de consentement[1612]. Il est évident qu'une telle plateforme aurait, en France, été qualifiée d'activité illégale en vertu de la loi n° 2016-444 du 13 avril 2016 visant à renforcer la lutte contre le système prostitutionnel et à accompagner les personnes prostituées, interdisant tout achat d'un acte sexuel[1613]. Cependant, et bien que le projet se soit visiblement avéré être un moyen de capitalisation frauduleux permettant d'escroquer ses investisseurs[1614], il n'a pas moins réussi à récolter l'équivalent de 19 millions de dollars[1615]. Finalement l'ancien principe « *quod nullum est nullum producit effectum* »[1616] selon lequel le contrat nul est réputé n'avoir jamais existé[1617] est entièrement remis en cause avec la *blockchain*. Une transaction émise ultérieurement pourrait éventuellement en modifier les effets, à l'instar de ce que produirait un avenant mais, dans les faits, cela ne ferait que donner le sentiment de solutionner le problème de l'illégalité ou de l'illicéité originelle alors que l'empreinte de celle-ci demeurerait perpétuellement inscrite au sein de la chaîne. En définitive, non seulement le retour au *statu quo* tel que l'exigerait une nullité classique (C. civ., art. 1178, 1184) est purement et simplement impensable[1618], mais les éventuelles restitutions des art. 1352 à 1352-9 du C. civ. semblent également inenvisageables.

216. La portée de la théorie de la responsabilité : vers une indemnisation des conséquences de l'immuabilité ? Les conséquences éventuellement inextricables de la situation nous invitent à explorer d'autres approches que celle de l'avenant. Il est question notamment de ne plus réfléchir en termes de rétroactivité qui, d'ailleurs, est une notion

[1611] Sur le choix des termes, v., COMTE (Jacqueline), « Stigmatisation du travail du sexe et identité des travailleurs et travailleuses du sexe », *Déviance et Société*, 2010/3 (vol. 34), pp. 425-446.
[1612] Selon les porteurs du projet, celui-ci aurait dû être installé sur le réseau *ZeroNet*, le même qu'utilise le *DarkNet*. V. notamment, « Imminent ICO of Uber-like decentralized "SilkRoad of Sex" from Eros », *Coin Idol* [online], 5 Jul. 2017, https://coinidol.com/imminent-ico-of-silkroad-of-sex/ ; Samama (Pascal), « Le pari gonflé de la start-up Eros pour révolutionner la prostitution », *BFM Business* [en ligne], 21 juill. 2017, https://bfmbusiness.bfmtv.com/hightech/le-pari-gonfle-de-la-start-up-eros-pour-revolutionner-la-prostitution-1220868.html.
[1613] L. n° 2016-444, 13 avr. 2016, visant à renforcer la lutte contre le système prostitutionnel et à accompagner les personnes prostituées, *JORF* n° 0088, 14 avr. 2016, texte n° 1. Les faits de proxénétisme sont notamment punis par les art. 225-5 à 225-12 du C. pén.
[1614] FINES SCHLUMBERGER (Jacques-André), « Les blockchains : une invention qui n'a pas dix ans », *La revue européenne des médias et du numérique* [en ligne], Automne 2017, n° 44, https://la-rem.eu/2018/01/blockchains-invention-na-dix-ans/.
[1615] FINES SCHLUMBERGER (Jacques-André), art. cit.
[1616] Latin, « Ce qui est nul ne doit produire aucun effet. »
[1617] BENABENT (Alain), *op. cit.*, p. 194.
[1618] BARREAU (Catherine), « La régulation des smart contracts et les smart contracts des régulateurs », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 75.

qui essuie de nombreuses critiques eu égard à sa difficile application[1619], mais comme le propose notamment Alain Bénabent, de régler le passé en termes de responsabilité[1620]. Il s'agirait de prévoir l'exécution automatique d'une clause d'un *smart contract* instituant une indemnisation, afin de compenser, s'il y a lieu, la nullité de la transaction et l'impossibilité d'exécuter le contrat. Cette théorie permettrait donc, à l'image du mécanisme de l'*efficient breach* anglo-saxon[1621], de garantir les parties d'une impossibilité d'exécution du fait de la technologie. Cela pourrait probablement diminuer les effets négatifs de la chaîne de blocs en la matière.

Cette approche aurait pu être envisagée, cependant, deux éléments font opposition à son application. D'une part, la notion de responsabilité remplaçant celle de la rétroactivité et de ses effets est certes attrayante, mais elle demeure, pour le moment, infondée en droit[1622]. D'autre part, la pérennité de l'inscription d'opérations illégales ou illicites reste en soi problématique. D'autant plus que la *blockchain* n'est, en règle générale et en termes de contenu, soumise à aucun contrôle de la part des acteurs, lesquels laissent souvent les utilisateurs gérer le suivi de leurs propres transactions, jusqu'à ce que, dans les faits, les autorités s'y intéressent, spontanément ou après avoir été saisies, et décident si elles doivent être tenues pour nulles.

217. Impossibilité d'annuler le contrat ou ses effets, même en cas d'invalidité. Le contrôle opéré par les acteurs de la *blockchain*, et en particulier par les mineurs lors de la validation et de l'inscription de la transaction, ne porte, à l'évidence, pas sur des questions juridiques de légalité[1623]. Mais il ne concerne également pas la validité des conventions, à savoir si les exigences de consentement, de capacité et de licéité du contenu sont réunies[1624]. L'âge, par exemple, n'est, en l'état de l'art, pas une information qui est requise lors de l'inscription à une *blockchain*, ce qui peut être source de difficultés dans l'hypothèse où l'utilisateur est mineur (C. civ., art. 1124), en particulier si l'acte irrégulier lui porte préjudice (C. civ., art. 1305). Il en va également ainsi concernant les clauses

[1619] BENABENT (Alain), *op. cit.*, *loc. cit.*
[1620] *Ibid.*, pp. 194-195.
[1621] Sur la théorie de l'*efficient breach*, V. notamment, BIRMINGHAM (Robert L.), « Breach of Contract, Damage Measures, and Economic Efficiency », *Rutgers Law Review*, No. 24, 1970, p. 284 ; GOETZ (Charles J.), SCOTT (Robert E.), « Liquidated Damages, Penalties, and the Just Compensation Principle: A Theory of Efficient Breach », *Columbia Law Review*, Vol. 77, No. 4, May 1977, pp. 554-594 ; MARIQUE (Enguerrand), « Les smart contracts en Belgique : une destruction utopique du besoin de confiance », *D. IP/IT* 2019, n° 1, p. 22. – Le Black's Law Dictionary [Black's Law Dictionary, v° efficient breach] définit l'*efficient breach* comme la théorie selon laquelle « une partie devrait être autorisée à rompre un contrat et à payer des dommages et intérêts si cela serait plus efficace économiquement que d'exécuter le contrat ».
[1622] BARREAU (Catherine), art. cit., p. 76.
[1623] V. notamment sur le sujet, GUILHAUDIS (Élise), art. cit., p. 5.
[1624] C. civ., art. 1128 : « Sont nécessaires à la validité d'un contrat : 1° Le consentement des parties ; 2° Leur capacité de contracter ; 3° Un contenu licite et certain. »

abusives (C. consom., art. L. 241-1 ; C. civ. 1171) et les clauses dépourvues de cause telles que celles conférant à un contractant un avantage dépourvu de contrepartie (C. civ., art. 1162 et 1169). Réputées non-écrites, elles ne devraient, en principe, pas être exécutées[1625]. Un consentement vicié (C. civ., art. 1130 et s.) serait aussi susceptible d'entacher la validité d'un *smart contract* après avoir été conclu (C. civ., art. 1171)[1626]. En définitive, seules les adresses des utilisateurs, la demande de transaction, la solvabilité de l'émetteur et l'intégrité de la demande de paiement font partie du processus de vérification établi par les nœuds lors de l'étape de validation des blocs[1627]. Par conséquent, en cas d'irrégularité, de vice, ou encore de clause réputée non-écrite au sein d'un *smart contract*, l'immuabilité de la chaîne entraînera indubitablement une exécution intégrale, à l'image du drone russe[1628].

Par ailleurs, il n'existe pas non plus de mécanisme de révocation[1629]. En effet, hormis la possibilité de changer d'avis avant la durée de verrouillage de la transaction (« *nLockTime* »)[1630], ce qui supposerait l'émission d'une transaction d'annulation[1631], la chaîne manœuvre sur l'instantané. Étant donné que, selon le protocole utilisé, ce temps est plus ou moins long, à savoir dix minutes pour *Bitcoin* et cinq secondes pour *Ethereum*[1632], l'action en annulation est plus ou moins envisageable. Passé ce laps de temps, l'inscription devient irrémédiable par l'action des mineurs, et même si un déséquilibre ou une erreur entache la relation contractuelle, les parties pourraient difficilement révoquer leur engagement sans, au moins dans un premier temps, encourir les sanctions automatiques éventuellement prévues.

218. Une philosophie parfois difficile à concilier avec les volontés des parties elles-mêmes. Un certain scepticisme subsiste concernant les réels effets de la programmation, dans le code d'une *blockchain,* des sanctions contractuelles ayant pour objectif de tenir compte de la nullité des rapports synallagmatiques, à savoir de la résolution unilatérale de l'art. 1227 du C. civ. et de l'exception d'inexécution préventive consacrée par l'art. 1220 du C. civ. Bien que les solutions n'attendent plus qu'à être développées et intégrées

[1625] BARREAU (Catherine), art. cit., pp. 75-76.
[1626] GUILHAUDIS (Élise), art. cit., p. 5.
[1627] *Supra* n° 132.
[1628] Sur l'affaire du drone russe piloté par un *smart contract*, *supra* n° 210.
[1629] LEGEAIS (Dominique), *op. cit., loc. cit*.
[1630] Il s'agit de la période durant laquelle la transaction est mise en attente avant d'être vérifiée puis intégrée à un bloc [v., ANTONOPOULOS (Andreas M.), *op. cit.*, p. 117].
[1631] Une telle transaction en réalité se concrétise par l'émission d'une transaction inverse reprenant les mêmes « *input* » et en se les retournant.
[1632] RODRIGUEZ (Philippe), *La révolution blockchain : Algorithmes ou institutions, à qui donnerez-vous votre confiance ?*, éd. Dunod, 2017, p. 144.

aux *smart contracts*, les doutes formulés ont pour conséquence de freiner l'intégration confiante de la technologie. Les instructions des contractants sont appliquées de manière automatique et absolue. Volontairement décentralisée, la *blockchain* évolue pourtant parfois en contradiction avec les droits contractuels des parties, leur intérêt ou la législation en vigueur, y compris les principes fondamentaux du droit des contrats. Pourtant, bien que « les algorithmes [puissent] conduire au pire ou au meilleur », tel que le rappellent Serge Abiteboul et Gilles Dowek, « nous ne devons jamais oublier qu'ils n'ont, en eux-mêmes, aucune intention. Ils ont été conçus par des êtres humains. Ils sont ce que nous avons voulu qu'ils soient »[1633]. Néanmoins, comme le souligne Boris Barraud, la technologie est malgré tout, dès l'origine, « imprégnée d'une idéologie libérale que le droit français des contrats, traditionnellement, n'accepte guère »[1634].

§ 2. L'importance du rôle joué par l'Homme

219. Contrairement au code, le droit n'est pas une suite de « 0 » et de « 1 », de « Oui » et de « Non », mais un fascicule d'exceptions et de subtilités censées protéger les contractants en toute situation. En l'état actuel, la programmation de la *blockchain* ne prend pas encore en compte ni ces finesses, qui pourraient en outre être traduites par des « 0,7 » ou des « Oui, mais pas tout à fait », ni les valeurs du « savoir-contracter ». Or, ce sont ces particularités humaines qui font toute la différence dans l'univers juridique (A) et qui obligent finalement ce dernier à réintervenir pour colmater les difficultés éprouvées par les algorithmes en la matière (B).

A. Face à la brutalité des rapports sur blockchain : les spécificités des règles humaines

220. La mise à exécution brutale de la sanction programmée. Deux exemples concrets mettent en lumière cette « brutalité »[1635] parfois inadaptée des algorithmes d'une *blockchain*.

221. La mise à exécution brutale de la sanction programmée : la problématique du locataire enfermé ou privé d'accès au bien loué. La première situation est celle de

[1633] ABITEBOUL (Serge), DOWEK (Gilles), *Le temps des algorithmes*, éd. Le Pommier, 2017, pp. 8 et s.
[1634] BARRAUD (Boris), « Le droit en datas : comment l'intelligence artificielle redessine le monde juridique (PARTIE II : Les nouvelles technologies juridiques ou l'intelligence artificielle au service du droit) », *RLDI* 2019/12, n° 165.
[1635] RODA (Jean-Christophe), « Smart contracts, dumb contracts ? », *D. IP/IT* 2018, n° 2, p. 397, n° 11.

l'utilisateur preneur d'un bien qui, n'ayant pas versé le loyer dans le délai qui lui était imparti (C. civ., art. 1728, al. 2), est immédiatement privé de l'accès à ce bien et donc de son usage par le biais de son verrouillage à distance (C. civ., art. 1729)[1636]. Il peut s'agir, par exemple, de la location saisonnière d'une maison ou d'un appartement (C. tourisme, art. L. 324-1 et s., C. com., art. L. 145-5, al. 1er, 5, 6)[1637], ou de la location d'un véhicule automobile (C. civ., art. 1713 s.)[1638]. Si le bien est verrouillé, le contrat peut avoir prévu qu'il se déverrouillera dès lors que le locataire aura respecté son engagement, c'est-à-dire après règlement du solde du prix de la location, en plus de tout acompte ou arrhes déjà versés. Mais, l'accord entre le loueur et son preneur peut également prévoir que le paiement du solde du prix par ce dernier puisse intervenir dans un délai de *x* jours à compter de son entrée dans les lieux. De cette manière, le locataire qui ne paierait pas le prix de la location dans le délai imparti par l'échéancier manquerait à son obligation contractuelle, ce qui serait susceptible d'entraîner la résiliation du contrat et, le cas échéant, le verrouillage automatique du bien, non temporaire, mais définitif[1639]. Ce type de sanction, certes envisagé par la loi, paraît néanmoins brusque pour le débiteur qui a jusqu'ici toujours été l'objet d'une attention particulièrement protectrice du droit[1640]. En plus de respecter en principe tant les exigences des art. 1219 et 1225 du C. civ., et notamment celle d'une « inexécution suffisamment grave »[1641], que le principe de bonne foi, la sanction contractuelle devrait, selon le cas, mobiliser le droit du surendettement des particuliers (C. consom., art. L. 711-1, L.712-2-L. 743-2 et R. 711-1-R. 761-1). En effet, ne laisser au consommateur aucune possibilité de présenter ses arguments ou de demander un délai d'exécution témoigne d'une contradiction avec la philosophie du droit en la matière[1642]. Un auteur constate d'ailleurs que « le droit des contrats est protecteur des débiteurs, des locataires, tandis que le *smart contract*, au contraire, est protecteur des créanciers, des bailleurs » [1643]. De la même manière, la question se pose de savoir si le locataire du véhicule utilisé dans le cadre de son travail, par exemple s'agissant d'un

[1636] *Id.*
[1637] DEROME (Emma), « Location, achat : quand la blockchain réinvente l'immobilier », *WE Demain* [en ligne], 29 juin 2018, https://www.wedemain.fr/Location-achat-quand-la-blockchain-reinvente-l-immobilier_a3416.html.
[1638] Blockchain France, « Les applications prometteuses des smart contracts », *Blockchain France* [en ligne], 28 janv. 2016, https://blockchainfrance.net/2016/01/28/applications-smart-contracts/.
[1639] GUERLIN (Gaëtan), art. cit., *loc. cit*.
[1640] RODA (Jean-Christophe), art. cit., *loc. cit*.
[1641] BENABENT (Alain), *op. cit.*, p. 291.
[1642] *Id.*
[1643] BARRAUD (Boris), « Le droit en datas : comment l'intelligence artificielle redessine le monde juridique (PARTIE II : Les nouvelles technologies juridiques ou l'intelligence artificielle au service du droit) », art. cit.

chauffeur de taxi, pourrait encore, dans une situation similaire, invoquer l'art. L. 442-8, I, 5°, du C. com. pour rupture brutale des relations commerciales établies[1644].

222. La mise à exécution brutale de la sanction programmée : la spécificité du droit des procédures collectives. N'est pas non plus sans soulever de difficultés l'hypothèse de l'entreprise qui, accumulant les difficultés financières et multipliant tout autant les pénalités pour retard de paiement, serait expulsée de ses locaux par l'application des dispositions d'un *smart contract*[1645]. En effet, dans l'automaticité et le respect des instructions programmées par les parties elles-mêmes, le contrat, auto-exécuté, déclenche les pénalités à la seconde où les délais sont dépassés, et verrouille s'il y a lieu les biens loués non-payés, tels que les locaux, les véhicules, les machines. Il convient donc de se demander si dans ce cas l'utilisation de la technologie ne constituerait finalement pas un « facteur d'accélération des difficultés »[1646], rendant par conséquent difficile son articulation avec le droit des procédures collectives. En effet, sa mise en œuvre pose également un problème de conformité vis-à-vis des règles applicables en matière de cessation des paiements et de suspension et d'interdiction des poursuites individuelles telles qu'elles sont consacrées par les art. 3 et 47 de la loi du 25 janvier 1985[1647] (C. com., art. L. 622-7 et L. 622-22), et en particulier dans l'hypothèse d'un *smart contract*, lequel serait programmé pour poursuivre l'exécution des obligations contractuelles. Bien qu'*a priori* il résulte de ces dispositions la possibilité pour le juge d'annuler[1648], *a posteriori* et « à la demande de tout intéressé ou du ministère public dans un délai de trois ans à compter de la conclusion de l'acte ou du paiement de la créance », tout acte ou tout paiement passé en violation de celles-ci (C. com., art. 622-7, III), ces illustrations suffisent pour mettre à jour les quelques obstacles techniques qui se lèvent face à la *blockchain*[1649].

223. Les effets contractuels de l'indulgence humaine. Alors que le système *blockchain* est réputé pour « ne jamais rien oublier », beaucoup d'auteurs comparent cette faculté à celle de la nature humaine qui elle, peut décider de pardonner ou, à tout le moins,

[1644] GUERLIN (Gaëtan), art. cit., *loc. cit*.
[1645] Dans les conditions de l'art. L. 622-14 du C. com., en ce que la continuation du contrat de bail commercial connaît un sort spécifique.
[1646] RODA (Jean-Christophe), art. cit., *loc. cit*.
[1647] L. n° 85-98, 25 janvier 1985, relative au redressement et à la liquidation judiciaires des entreprises, *JORF*, 26 janv. 1985.
[1648] Pour une analyse sur les pouvoirs du juge étatique au sein de l'écosystème des *blockchains*, *infra* n°s 229 et s.
[1649] Pour plus de précisions, v. également, DAVERAT (Xavier), « Saisie : protection du débiteur – Difficultés économiques du débiteur », *Rép. pr. civ. Dalloz*, v° Difficultés économiques du débiteur, 2019, n°s 123-144.

de tenir compte des difficultés économiques rencontrées par le débiteur. En particulier, il s'agit d'évoquer deux aspects des pratiques contractuelles et relationnelles de la vie en société, à savoir, d'une part, les dispositifs et délais juridiquement accordés pour retard d'exécution, et d'autre part, plus spécifiquement la faculté pour certains professionnels de se montrer indulgents et d'accorder une sorte de seconde chance à des clients qui, par le passé, ont été imprudents, maladroits et/ou malchanceux[1650].

En effet, dans un premier temps, bien que le créancier soit en principe en droit d'exiger le paiement intégral de la dette à l'échéance stipulée (C. civ., art. 1244)[1651], le juge ou même le créancier, tolérant et patient[1652], peut accorder au débiteur qui tarde à remplir ses obligations un rééchelonnement de ses paiements ou un délai supplémentaire pour qu'il s'exécute. Comme le souligne un auteur, « toute personne peut être victime de difficultés économiques. Des mesures de réaménagement des dettes suffisent parfois à débloquer une situation »[1653], de sorte que le législateur s'est souvent soucié des conséquences que pouvaient engendrer des difficultés économiques rencontrées par le débiteur[1654]. D'ailleurs, l'art. 1343-5 du C. civ. indique non seulement que le juge dispose d'un pouvoir souverain d'apprécier l'opportunité d'accorder des délais de grâce, mais également qu'il s'agit d'une disposition d'ordre publique de sorte qu'aucune clause ne peut en écarter l'application. Ainsi, « toute stipulation contraire est réputée non écrite » (C. civ., art. 1343-5, al. 5). En règle générale, « l'octroi du délai doit être motivé » (C. pr. civ., art. 510, al. 4), mais le juge peut tenir compte de l'ensemble des éléments relatifs à la situation du débiteur et des besoins du créancier, afin de « reporter ou échelonner, dans la limite de deux années, le paiement des sommes dues » (C. civ., art. 1343-5, al. 1er). Il peut également, en vertu de l'al. 2 de l'art. 1343-5 du C. civ., moduler les taux d'intérêt et, en vertu de l'al. 3 du même art., offrir des garanties du paiement de la dette au créanciers[1655]. En parallèle, il existe des dispositifs spéciaux, que le législateur a développés au fil du temps afin de répondre à un surendettement chronique[1656]. De la loi n° 89-1010 du 31 décembre 1989, dite « loi Neiertz », relative à la prévention et au

[1650] PAVEL (Ilarion), art. cit., p. 23.
[1651] V. également, CHOLET (Didier), « Exécution des jugements et des actes », *Rép. pr. civ. Dalloz*, v° Délais judiciaires, 2015 (actualisation : 2020), n°s 110 et s. ; TESTU (François Xavier), *Contrats d'affaires*, éd. Dalloz, coll. Dalloz Référence, 2010-2011, pp. 463-466.
[1652] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., n° 29.
[1653] DAVERAT (Xavier), *op. cit.*, n° 78.
[1654] *Ibid.*, n° 79.
[1655] Dans un arrêt en date du 19 février 1993, les juges ont accordé à l'intéressé un délai de grâce sous réserve que la demande soit « assortie d'un effort financier sérieux et immédiat » [TGI Saint-Dié, JEX, 19 fév. 1993, *D.* 1994. 35, note Prévault J.].
[1656] AVENA-ROBARDET (Valérie), « Prochaine réforme du surendettement », *AJ fam*. 2012, p. 363.

règlement des difficultés liées au surendettement des particuliers et des familles[1657], à la loi du 18 novembre 2016 de modernisation de la justice du XXIe siècle[1658], les réformes ont conduit à créer un véritable arsenal juridique au sein du Code de la consommation. Un auteur explique que les procédures initiales, lesquelles avaient pour objectif de rechercher quelques possibilités de rééchelonnement des dettes, ont laissé place à un dispositif complet, proposant « d'appréhender la situation de la personne surendettée et de suspendre des mesures prises à son encontre avant [qu'une] commission ne prévoie, si c'est possible, le traitement de la situation de surendettement, ou ne recommande un rétablissement personnel »[1659]. Dès lors qu'un particulier, personne physique, surendetté, est de bonne foi confronté à « l'impossibilité manifeste […] de faire face à l'ensemble de ses dettes non professionnelles », il peut demander à bénéficier des mesures de traitement des situations de surendettement (C. consom., art. L. 711-1) et ainsi saisir la commission départementale d'examen des situations de surendettement des particuliers (C. consom., art. L. 712-1, L. 721-1). Cette entité spécialisée dresse l'état du passif du débiteur afin de lui proposer des solutions viables. Cette procédure peut ainsi conduire à reporter ou à rééchelonner le paiement d'une dette, mais également à procéder à la régularisation d'un incident de paiement (C. consom., art. L. 733-17), à la réduction, voire à l'effacement de la dette dans son ensemble (C. consom., art. L. 743-1), et à programmer, « si la situation du débiteur l'exige », une mesure d'aide ou d'action sociale (C. consom., art. L. 712-9) qui peut consister en un plan d'éducation budgétaire (dispositif des Points Conseil Budget (PCB)[1660]). Ces solutions témoignent d'autant plus de la bienveillance des règles humaines qu'elles sont proposées et mises en place dans un objectif de conciliation et donc en accord avec les besoins du créancier. Comme le constate un auteur, « désormais, le législateur prescrit de tenir compte également de la situation du créancier qui pourrait également se trouver en grande difficulté s'il n'était pas payé à temps »[1661]. D'ailleurs, des garanties en faveur de ce dernier peuvent aussi être imposées au débiteur (C. consom., art. L. 732-2). La bonne foi du débiteur constitue une condition essentielle de la mise en application de ces procédures. Par conséquent, le juge attache une grande importance à

[1657] L. n° 89-1010, 31 déc. 1989, relative à la prévention et au règlement des difficultés liées au surendettement des particuliers et des familles, *JORF* n° 1, 2 janv. 1990. – DAVERAT (Xavier), *op. cit.*, n° 80.
[1658] L. n° 2016-1547, 18 nov. 2016, de modernisation de la justice du XXIe siècle, *JORF* n° 269, 19 nov. 2016, texte n° 1.
[1659] DAVERAT (Xavier), *op. cit.*, n° 81.
[1660] Le dispositif des PCB a été mis en place par l'instruction du 31 décembre 2015 dans le cadre du plan pluriannuel de lutte contre la pauvreté et pour l'inclusion sociale.
[1661] CHOLET (Didier), *op. cit.*, n° 113.

sa caractérisation et vérifie, pour cela, que l'absence déclarée de ressources ou de biens saisissables est réelle[1662].

Ces procédures n'empêchent pas la pratique, plus informelle et autonome, voulant qu'un professionnel puisse octroyer par lui-même un délai supplémentaire à son débiteur pour qu'il s'exécute, ou qu'il puisse accorder une seconde chance à un ancien client imprudent, maladroit et/ou malchanceux. Il en va ainsi des banques, par exemple, qui ont subi les aléas financiers de clients retardataires ou mauvais payeurs et qui, malgré tout, décident quelques années plus tard de conclure à nouveau un prêt avec les anciens défaillants[1663].

Il convient de se demander si dans des cas similaires à ceux évoqués, l'exécution intégrale automatique de la technologie ne constituerait pas, à nouveau, un « facteur d'accélération des difficultés »[1664], rendant par conséquent difficile son articulation avec le droit du surendettement des particuliers et, d'une manière générale, les règles mais également les coutumes, usages et pratiques contractuelles. Dans le cadre spécifique des *smart contracts*, au contraire de l'être humain, la patience n'est pas innée et elle ne peut être acquise que par le biais d'une programmation. Les utilisateurs sont libres de fixer leurs propres règles, le revers étant qu'ils devront appliquer celles-ci rigoureusement. Le moindre écart ne pourra être permis par l'algorithme puisqu'à l'évidence celui-ci ne bénéficie pas des mêmes dispositions à la fois légales et morales qui fondent la société. Bien que cette caractéristique ait pour effet direct de renforcer tant la technologie que son application dont les instructions ne peuvent être ni omises ni contournées indépendamment de la volonté de toutes les parties[1665], elle n'est pas sans soulever de difficultés. Il est clair qu'éliminer des algorithmes contractuels les risques de falsification, d'inexécution ou de violation ne peut suffire à justifier leur utilisation telle que proposée si cela conduit les parties à devoir renoncer à l'usage de leurs droits, même informels. De la même manière comment, par exemple, introduire l'obligation d'exécution ou de négociation de bonne foi (C. civ., art. 1104) dans une ligne de code[1666] ? Peut-il seulement y avoir bonne ou mauvaise foi dans l'exécution d'un programme informatique, ou peut-être s'agit-il davantage d'apprécier la bonne foi de l'informaticien codeur ? Selon un auteur, l'automaticité notamment de la sanction ou de l'extinction du contrat a pour conséquence d'inhiber cette notion directrice du droit des contrats[1667]. Ce constat laisse

[1662] *Id.* ; DAVERAT (Xavier), *op. cit.*, n° 81.
[1663] PAVEL (Ilarion), art. cit., p. 24.
[1664] RODA (Jean-Christophe), art. cit., *loc. cit*.
[1665] *Id.*
[1666] GUERLIN (Gaëtan), art. cit., *loc. cit*.
[1667] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., *loc. cit*.

de surcroît entière la question du bien-fondé de l'exigence de loyauté dans un système de *blockchain*[1668], laquelle constitue un autre principe fondamental du droit contractuel contemporain[1669].

224. Dominés par la rigidité et l'absence d'adaptation de la technologie, seules les règles juridiques et les coutumes, usages et pratiques contractuelles semblent en mesure de transformer ces rapports brutaux en relations contractuelles stables. Cela suppose toutefois qu'une programmation active et anticipée soit mise en place.

B. Face à l'extrême nécessité d'anticiper : le retour du juriste-codeur

225. La solution du paramétrage. En principe, annuler ou modifier *a posteriori* de leur inscription les termes d'un contrat, quand bien même cette circonstance permettrait de les conformer aux règles dictées par la pratique des relations contractuelles, est techniquement impossible puisque cela suggère d'opérer des manipulations sur la *blockchain*. Au-delà, de tels évènements contraires aux principes admis au sein de l'écosystème pourraient, s'ils étaient tentés, non seulement déstabiliser le bon fonctionnement de la chaîne, mais également risquer de nuire à son organisation, à l'instar de l'incident « *TheDAO* »[1670]. La seule solution serait donc d'intégrer, au sein du *smart contract* ou, selon la situation, de la chaîne, l'ensemble de ces subtilités contractuelles afin que la technologie soit capable de les mettre en œuvre.

En effet, le *smart contract* a naturellement l'avantage de procurer une forte sécurité en même temps que d'assurer une exécution en tous points conforme aux instructions des parties. Mais il présente l'inconvénient majeur d'immobiliser les conditions prédéfinies, donc paradoxalement d'empêcher la bonne exécution d'un contrat. Tel que le souligne un auteur, « le *smart contract* comme tout protocole est limité par le principe d' "exécution intégrale" : tout le programme mais rien que le

[1668] GUERLIN (Gaëtan), art. cit. *loc. cit.*

[1669] À titre d'exemple il est possible de les retrouver avec l'exigence de bonne foi dans : CPC, art. 14-15 concernant le principe du contradictoire ; C. com., art. L. 420-1 en matière commerciale ; C. consom., art. L. 211-4, L. 221-1 concernant l'obligation de conformité et de sécurité du vendeur ; C. trav., L. 1221-6, L. 1222-1, L. 5331-3, L. 6321-1 (pour la bonne foi et la loyauté de l'employeur) et L. 1222-2 (pour celles du salarié) ; Cass. Crim., 27 févr. 1996, n° 95-81.366 concernant le principe de la loyauté de la preuve en matière pénale ; CE, Assemblée, 28 déc. 2009, n° 304802, arrêt « Ville de Béziers » en matière administrative, Publié au recueil Lebon.

[1670] Pour une analyse des conséquences de la prise de contrôle de la Fondation Ethereum sur la chaîne lors de l'incident « *TheDAO* », *infra* n°ˢ 270 et s.

programme »[1671]. Par conséquent, chaque hypothèse doit être prévue[1672], la technologie ne peut combler les vides laissés par les parties. Il est alors nécessaire d'anticiper. L'intégralité des sanctions, des issues, des conséquences à *x* ou *y* conditions remplies/non-remplies doit être spécifié. Le principe même d'une sanction, d'une issue ou d'une conséquence doit être fixé de manière explicite[1673], sans quoi le programme ne le reconnaîtra pas. « Bête et méchant », « incapable d'adaptabilité »[1674] ou simplement respectueux des dispositions prédéfinies par les parties, la technologie impose aux parties un encadrement rigoureux si elles attendent de lui l'application de notions complexes telles que « diligences utiles », « meilleurs efforts », « délai raisonnable »[1675]. Ainsi, selon Boris Barraud, « l'avenir est-il entièrement écrit dès le départ et l'aléa et l'imprévisibilité n'ont-ils pas de place dans un *smart contract* »[1676]. Finalement, la rigidité de la technologie dépend de celui qui la conçoit.

226. L'importance du paramétrage *by design* : le rôle du juriste. Finalement, la *blockchain* n'est pas une zone de non-droit, elle est simplement à l'intersection de plusieurs disciplines et nécessite avant tout l'anticipation des parties dès sa conception[1677]. L'enjeu de son développement réside dans l'intégration *by design* des règles de droit et de la pratique des relations contractuelles. L'étape de formation du *smart contract*, qui consiste à programmer l'algorithme qui aura la charge de contraindre les parties à respecter leurs engagements éventuellement respectifs et à pérenniser la relation établie, est par conséquent la clé. Praticien du droit par définition, le juriste pourrait, en collaboration avec un informaticien, investir ce champ d'action afin d'intervenir *ex ante* auprès des parties en tant que conseil[1678]. L'objectif ne serait pas de minimiser le rôle de la technologie, mais au contraire de lui permettre de dévoiler et de décupler son potentiel en la matière.

[1671] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., n° 22.
[1672] *Id.*
[1673] BARRAUD (Boris), « Les blockchains et le droit », *RLDI* 2018/4, nº 147, p. 13.
[1674] BARRAUD (Boris), « Le droit en datas : comment l'intelligence artificielle redessine le monde juridique. PARTIE II : Les nouvelles technologies juridiques ou l'intelligence artificielle au service du droit », art. cit.
[1675] COIFFARD (Didier), « Entretien du mois : La Blockchain a un sens pour répartir une partie de la confiance en rendant une information infalsifiable mais cette confiance est très en deçà de celle conférée par le notaire », *RLDC* 2017/4, n° 147 ; CHRISTODOULOU (Hélène), « Intelligence artificielle – Les nouvelles technologies à l'origine de l'évolution contractuelle », *Comm. com. électr*. 2020, étude 20, 11 nov. 2020, n° 4.
[1676] BARRAUD (Boris), « Le droit en datas : comment l'intelligence artificielle redessine le monde juridique. PARTIE II : Les nouvelles technologies juridiques ou l'intelligence artificielle au service du droit », art. cit.
[1677] GUERLIN (Gaëtan), art. cit., *loc. cit*.
[1678] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., *loc. cit*.

Le juriste pourrait alors aider les contractants à comprendre le langage informatique[1679], pour notamment prévenir tout risque d'aléa dans le respect à la fois de leurs volontés[1680] et des exigences légales. Par le biais de « clauses informatiques », lesquelles consisteraient en des formules conditionnelles prenant la forme « *If ... ; Then ...* », il s'agirait d'inclure, *via* le mécanisme du consensualisme, l'ensemble des règles de droit et des règles à caractère privé pouvant se révéler utiles lors de l'exécution du contrat entre les parties. Hormis les « délai raisonnable » et « diligences utiles », elles ont trait pour l'essentiel aux clauses de force majeure, par ailleurs précitées[1681], permettant d'anticiper au sein du code informatique la survenance d'événements fortuits conformément à l'art. 1218 du C. civ.[1682]. Afin d'assurer l'efficacité du dispositif, il sera nécessaire de lister ces hypothèses en veillant à ne pas interférer avec le droit des consommateurs[1683]. Il en irait ainsi, par exemple, d'une indisponibilité du réseau[1684], d'une cyber-attaque[1685]. Les règles de droit et les règles à caractère privé pourraient également comprendre la clause de *hardship* et la clause d'indexation, couramment utilisées dans le monde des affaires. D'ailleurs, ces clauses visaient déjà, avant la réforme du 10 février 2016, à compenser les vides résultants du refus du législateur d'envisager de réviser le contrat en cas de changement imprévisible de circonstances venant bouleverser son équilibre[1686]. Concernant la clause de *hardship*, les parties ont plusieurs possibilités. D'une part, elles peuvent choisir de reprendre les principes UNIDROIT[1687]. D'autre part, elles peuvent composer leur clause de sauvegarde elles-mêmes. Elles devront dans ce cas veiller à fixer quatre éléments indispensables à la validité de la clause, à savoir, le seuil de déclenchement de la clause (la nature des circonstances, les effets exigés et les conditions de forme), le mécanisme de révision choisi (l'objet de l'adaptation, l'intervention d'un tiers et les délais), la situation du contrat au cours de l'adaptation (autrement dit, s'il y a continuation ou suspension), le dénouement

[1679] GODEFROY (Lêmy), « Le code algorithmique au service du droit », *D.* 2018, pp. 734 et s.
[1680] GUILHAUDIS (Élise), art. cit., p. 11.
[1681] Sur la programmation des clauses de force majeure, *supra* n° 212.
[1682] Pour plus de détails sur le sujet, v., BENABENT (Alain), *op. cit.*, pp. 279-287.
[1683] V. en ce sens, Cass. Civ. 1ère, 10 févr. 1998, *D.* 1998.539, note Mazeaud D. ; BENABENT (Alain), *op. cit.*, p. 283.
[1684] V. en ce sens, CA Versailles, 4 févr. 2004, n° 03/07368 (« Qu'en sa qualité de prestataire des services Orange est tenu à une obligation de résultat envers l'abonné ; Qu'elle est présumée responsable de tout dysfonctionnement sauf à elle à rapporter la preuve d'une cause étrangère. »).
[1685] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., *loc. cit.*
[1686] BENABENT (Alain), *op. cit.*, p. 249.
[1687] Principes UNIDROIT, art. 6. 2. 3 : « 1) En cas de *hardship*, la partie lésée peut demander l'ouverture de renégociations. La demande doit être faite sans retard indu et être motivée. 2) La demande ne donne pas par elle-même à la partie lésée le droit de suspendre l'exécution de ses obligations. 3) Faute d'accord entre les parties dans un délai raisonnable, l'une ou l'autre peut saisir le tribunal. 4) Le tribunal qui conclut à l'existence d'un cas de *hardship* peut, s'il l'estime raisonnable : a) mettre fin au contrat à la date et aux conditions qu'il fixe ; ou b) adapter le contrat en vue de rétablir l'équilibre des prestations. »

(processus de mise à jour du *smart contract* et effets)[1688]. La clause d'indexation, ou clause d'échelle mobile, permet quant à elle de contourner la rigueur du principe de nominalisme monétaire auquel conduit l'intangibilité, laquelle avait déjà été constatée en ce qui concerne les relations d'affaires traditionnelles mais s'avère inévitable en matière de *smart contract*[1689]. Les parties doivent pour cela choisir un indice de référence présentant un lien direct avec l'objet du *smart contract* ou avec l'activité d'une des parties (CMF, art. L. 112-2). La rigidité et le caractère automatique de l'exécution du *smart contract* pourraient également être compensés par l'intégration dans l'algorithme de clauses de conciliation ou de médiation préalable obligatoire[1690]. De la même manière, la pratique des contrats d'affaires traditionnels indique que pourraient également être « blockchaînées » des clauses d'obligations alternatives (C. civ., art. 1307 et s.), de client le plus favorisé (C. com., art. L. 420-1)[1691], limitatives de responsabilité[1692] et de répartition des risques[1693], entre autres[1694].

Force est de constater que, finalement, étant donné, d'une part, l'état du développement de la technologie et, d'autre part, les subtilités du droit positif des contrats, l'exercice n'est pas simple pour les parties qui, le plus souvent, sont inexpérimentées au moins dans le domaine algorithmique, sinon dans la matière juridique. En effet, au-delà des *blockchains* et des *smart contracts*, le rôle du juriste consiste à « critiquer et [à] proposer »[1695], à identifier en amont d'une décision toute conséquence problématique, à la qualifier, l'explorer et l'analyser afin d'éviter ou, à défaut de le pouvoir, contourner ses propres conséquences. En définitive, l'intervention d'un juriste *ex ante* se révèle nécessaire, voire inévitable. Comme le souligne Mustapha Mekki, « le juriste fait souvent office d'empêcheur de tourner en rond, de trublion qui ne voit que des difficultés là où les informaticiens voient des opportunités. Pourtant, tel est son rôle : comprendre pour mieux accompagner, interroger pour mieux sécuriser, questionner pour mieux anticiper »[1696].

[1688] LACROIX (Guillaume), *L'adaptation du contrat aux changements de circonstances*, Reims : Université de Reims, 2015, non publié [en ligne], pp. 19-23, https://dumas.ccsd.cnrs.fr/dumas-01317150/document.
[1689] BENABENT (Alain), *op. cit.*, p. 135.
[1690] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., *loc. cit.* – V. également, KEBIR (Mehdi), « Clause de conciliation préalable : application à une demande reconventionnelle », *AJDA* 2018, p. 308.
[1691] V. également, ARONICA (Charles), « La clause du client le plus favorisé », *AJCA* 2014, n° 2, p. 69 ; Lignes directrices n° SEC(2010) 411 final de la Commission, 10 mai 2010, sur les restrictions verticales, *JO* n° C 130, 19 mai 2010, § 129 ; Décision n° BP Kemi/DDSF de la Commission, 5 sept. 1979, *JO* n° 79 L 286/32 ; CJUE, 13 fév. 1979, n° C-85/76, *Hoffmann-La Roche & Co. AG c/ Commission des Communautés européennes* ; Avis du conseil de la concurrence, 25 juin 1981, *BOSP*, 12 déc. 1981.
[1692] BENABENT (Alain), *op. cit.*, pp. 329-332. – V. également pour un exemple d'application, CA Paris, 14 déc. 2016, n° 14/14793.
[1693] CHANTEPIE (Gaël), « Contrat : effet », *Rép. civ. Dalloz*, v° Contrat, 2018, n° 307.
[1694] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., *loc. cit.*
[1695] CALAIS-AULOY (Marie-Thérèse), « Le rôle du législateur et celui du juriste confrontes à l'idée de pacte républicain », *LPA* 31 août 1999, n° PA199917301, p. 4.
[1696] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., n° 12.

227. La capacité d'adaptation du paramétrage : intégration algorithmique des bénéfices et effets escomptés des règles relatives à l'exécution du contrat. En l'état de l'art, arguer que les *smart contracts* sont incapables de mettre à exécution des instructions complexes semble partiellement erroné puisqu'en réalité tout n'est qu'une question de programmation. Julien Gossa indique d'ailleurs que « il n'existe en théorie pas de limitation technique à l'expressivité des conditions du contrat, dès lors que l'on peut les traduire en langage informatique »[1697]. Dès lors que le programmeur est capable d'utiliser une opération algorithmique pour manipuler un élément juridique complexe, ce dernier n'est plus inexécutable. Simplement, l'accent n'est pas mis sur la façon de coder informatiquement ces instructions, et en particulier sur la question de savoir si elle utilise le même cheminement scientifique et intellectuel que celui décrit par la loi ou la pratique ou si elle a procédé à des adaptations, mais il est mis sur le résultat escompté de la programmation, lequel correspond au résultat exigé par le législateur ou par la pratique des relations contractuelles. Les parties à un *smart contract* pourraient, d'un commun accord, fixer un délai de *x* jours, éventuellement en lien avec la position jurisprudentielle, et correspondant à ce qu'ils entendent comme un « délai raisonnable » destiné à être mis en œuvre par le code pour accorder au débiteur qui tarde à remplir ses obligations un répit pour qu'il s'exécute. De la même manière, elles pourraient conjointement fixer les diligences dont elles considèrent qu'elles seront « utiles » ou « suffisantes ». Ainsi, en indiquant avec suffisamment de précision ce qui doit être analysé comme remplissant ou ne remplissant pas une condition, la technologie est capable d'en tirer les conséquences programmées et donc escomptées. Une porte de sortie à l'image de ce que Nick Szabo avait imaginé[1698], en cas de difficultés financières par exemple, pourrait s'appuyer sur une condition préfixée s'exécutant comme un bouton « marche/arrêt » temporaire permettant de contourner les effets d'une exécution automatisée qui deviendrait « aveugle », ainsi que le constatent Yves Poullet et Hervé Jacquemin[1699]. L'intérêt serait de trouver un moyen de suspendre l'exécution du *smart contract* en cas, par exemple, de difficultés financières pour le débiteur, le temps qu'une décision soit prise à l'amiable concernant les délais ou, que la situation soit étudiée par une tierce personne, telle qu'un juge. Une suspension temporaire dans l'exécution du code pourrait être envisagée. Elle pourrait être créée par le biais d'une inscription conjointement initiée par les contractants,

[1697] GOSSA (Julien), « Les blockchains et smart contracts pour les juristes », *D. IP/IT* 2018, n° 7-8, pp. 393 et s.
[1698] SZABO (Nick), « Formalizing and Securing Relationships on Public Networks », [online], 1st Sept. 1997, http://firstmonday.org/ojs/index.php/fm/article/view/548/469.
[1699] POULLET (Yves), JACQUEMIN (Hervé), « Blockchain : une révolution pour le droit ? », *Journal des Tribunaux*, n° 6748, 10 nov. 2018, p. 817.

dont le contenu aurait donc pour effet de créer une interruption et d'exécuter un sous-programme dans lequel les parties auraient inscrit les instructions à suivre en cas de difficulté rencontrée au cours de l'exécution du contrat. L'importance de ces solutions pour l'essor de la technologie témoigne de l'extrême nécessité d'un travail commun entre juristes et programmeurs.

228. Contribuant à inspirer la confiance lors de l'établissement des relations entre personnes privées sur la chaîne, le juriste intègre l'écosystème dans un rôle de conseil pour en devenir un maillon capital. Figure symbolique de la justice, au-delà de la personne physique[1700] le juge est assimilé à l'impartialité et à la justesse, si bien que « lorsque le juge dit le droit, il rend justice »[1701]. Dès lors, en toute logique, le sort du juge devrait être identique à celui du juriste. Mais encore faut-il qu'il dispose de suffisamment de liberté au sein de l'écosystème pour y intervenir.

[1700] GARAPON (Antoine), *Bien juger. Essai sur le rituel judiciaire*, éd. Odile Jacob, 1997, p. 228 ; ALLEN (Jessie), « Blind Faith and Reasonable Doubts: Investigating Beliefs in the Rule of Law », *Seattle University Law Review*, Vol. 24, 2001, p. 716.

[1701] GELINAS (Fabien), CAMION (Clément), BATES (Karine), « Forme et légitimité de la justice – Regard sur le rôle de l'architecture et des rituels judiciaires », *Revue interdisciplinaire d'études juridiques* 2014/2, vol. 73, pp. 37-74.

Chapitre 2. La décentralisation, une délicate intervention du juge étatique

229. Bien que sa légitimité puisse parfois être complexe à imposer à l'écosystème *blockchain* au regard de la philosophie qu'il a adoptée, le juge n'en demeure pas moins le garant national de la sécurité juridique. Par son application et son interprétation du droit, le juge est un acteur fondamental dans la gestion des litiges et devrait, par principe, jouir des mêmes pouvoirs concernant la gestion des conflits pouvant survenir sur une *blockchain* (Section 1). Toutefois, contrairement au juriste, si le juge doit intervenir, il sera contraint de le faire non en amont de l'inscription définitive sur la chaîne du *smart contract*, mais en aval, et parfois même lorsque l'exécution automatique et « aveugle »[1702] a d'ores et déjà créé un préjudice. À l'évidence, il ne s'agit pas tant d'un obstacle direct à son intervention mais bien davantage de la preuve que son intervention est nécessaire. En revanche, il ne fera pas l'économie des limites entachant, sur certains points, l'application du droit (Section 2).

Section 1. Le pouvoir du juge étatique dans la gestion des conflits

230. L'objectif poursuivi lors de la création de *Bitcoin* et, indirectement, de la *blockchain*, était d'ancrer au sein des règles de fonctionnement du protocole décentralisé le principe selon lequel la règle découle du code. Cette vision idéaliste du point de vue des opérateurs initiaux de la chaîne de blocs rend *a priori* difficile l'intervention d'un juge étatique. Il conviendra alors d'étudier la manière dont, en pratique, le principe « *Code is Law* » est appliqué (§ 1). Cependant, il s'avère que même les fois où le protocole intègre des solutions d'auto-gestion des litiges, le résultat obtenu n'est pas aussi satisfaisant qu'il pourrait l'être. Aussi sommes-nous conduits à douter de la capacité de la technologie à gérer, du moins seule, les contentieux, et à défendre les droits des utilisateurs. Si bien que l'autorité protectrice du juge finit par s'imposer, conduisant à une recrudescence de son rôle en la matière (§ 2).

[1702] POULLET (Yves), JACQUEMIN (Hervé), « Blockchain : une révolution pour le droit ? », *Journal des Tribunaux*, n° 6748, 10 nov. 2018, p. 817.

§ 1. L'application du principe « *Code is Law* »

231. La *blockchain* fut originellement programmée dans le seul et unique but de disrupter l'État et ses monopoles de puissance faillibles[1703], pour finalement édifier un environnement libéré de toute normalisation centralisée (A). Cependant, sans solutions de règlement des contentieux initialement intégrés à la technologie, son déploiement s'est révélé lacunaire, ce qui a conduit l'écosystème à prendre en considération l'importance d'intégrer un mécanisme de règlement des conflits, dont il s'agira d'évaluer les propositions (B).

A. Le refus de normalisation de l'État

232. L'absence de l'État dans la régulation de la *blockchain* : un choix édicté par les leçons du passé. Alors que la seconde guerre mondiale se prépare, en 1936 une bataille d'une toute autre nature retentit en Europe, illustrant l'affrontement théorique entre deux camps, à savoir, d'une part, les libéraux attachés à la doctrine de la « main invisible »[1704] et, d'autre part, les interventionnistes prônant l' « État-Providence »[1705]. Face à une économie qui s'effondre progressivement, fixer la place que doit tenir l'État dans la régulation de l'économie devient urgent. Huit décennies plus tard, le pouvoir régulateur de l'État est à nouveau désapprouvé. Alors qu'initialement la question était de savoir s'il fallait « réguler ou ne pas réguler le *bitcoin* ? »[1706], désormais il convient de se

[1703] Sur la crise de confiance et le remplacement par l'outil informatique, *supra* n° 3.

[1704] Expression imaginée par Adam Smith pour exprimer la théorie selon laquelle le marché économique se régule par lui-même *via* cette « main invisible » guidant, imperceptiblement, les intérêts égoïstes de chaque individu qui *a posteriori* contribuent forcément à l'intérêt général, l'intérêt de tous. Toute intervention de l'État au niveau économique est alors strictement proscrite ; une seule action de celui-ci pourrait interférer et finalement nuire fondamentalement à ce mécanisme d'autorégulation naturel et spontané. Apparue pour la première fois en 1755 pour évoquer les « événements irréguliers de la nature » [SMITH (Adam), « History of Astronomy » (1755), *in Essays on Philosophical Subjects*, ed. Clarendon Press, 1981, p. 49], c'est en 1776 qu'elle prend son sens et finalement sa place de concept économique [SMITH (Adam), *An Inquiry into the Nature and Causes of the Wealth of Nations*, Londres, ed. W. Strahan and T. Cadell, Livre IV, ch. 2, 1776 ; d'après réédition *Recherches sur la nature et les causes de la richesse des nations*, éd. Flammarion, 1991, tome II, pp. 42-43]. – V. également, BACHOFEN (Blaise), BIZIOU (Michaël), BRAHAMI (Frédéric) *et al*., *Le libéralisme au miroir du droit : l'État, la personne, la propriété*, éd. ENS, 2008, p. 200 ; IBANDA KABAKA (Paulin), « L'intervention de l'État dans l'économie : du laisser-faire à la régulation », *HAL* [en ligne], <hal-01287474>, 13 mars 2016, p. 1, https://hal.archives-ouvertes.fr/hal-01287474/document.

[1705] Au contraire, cette expression expose l'idée que l'intervention de l'État dans les domaines économiques et sociaux est primordiale. Autrement dit, les pouvoirs publics doivent impérativement prendre en charge le volet normatif concernant l'activité économique (politique économique). *A fortiori*, c'est à eux que revient la tâche de prendre les décisions qui orienteront l'activité économique vers un but précis et voulu, et ce, à court (politique conjoncturelle) ou long terme (politique structurelle). – Pour plus de précisions, v. également, EWALD (François), *Histoire de l'État providence : Les origines de la solidarité*, éd. Le livre de poche, coll. Biblio essais, 1996 ; POULON (Frédéric), *Économie générale*, éd. Dunod, coll. Manuel, 8e édition, 2015, pp. 79-90. – IBANDA KABAKA (Paulin), art. cit., pp. 2-5.

[1706] GAFFURI (Ariane), « Bitcoin: réguler ou ne pas réguler? », *RFI* [en ligne], 19 févr. 2018, http://www.rfi.fr/economie/20180219-bitcoin-reguler-pas-reguler.

demander s'il faut « réguler ou ne pas réguler la *blockchain* ? ». En effet, tandis que, pour beaucoup, il est nécessaire que l'État intervienne, impliquant l'instauration de « politiques *blockchain* conjoncturelles », l'essentiel des utilisateurs et participants revendiquent l'auto-régulation[1707]. Attachés à leur idéal décentralisé, leur opposition rappelle vaguement celle qui a conduit Milton Friedman à s'élever contre la temporalité de l'intervention étatique[1708], et d'autres économistes des années 1970 à finalement regretter les interventions de l'État mises en place après-guerre, jugées profondément déstabilisantes[1709]. De même que ces économistes, les utilisateurs et participants de la *blockchain* semblent se méfier des conséquences que pourraient avoir l'usage du pouvoir normatif de l'État sur la technologie, de sorte que le système actuel est marqué par un refus de l'organisation et de l'intervention étatique. Mais cela ne fait pas de la *blockchain* un système désorganisé. Au contraire, selon un auteur, la *blockchain* est en elle-même un environnement volontairement autonome, et qui dispose des moyens nécessaires pour s'auto-réguler[1710]. La confiance n'est pas le résultat d'une réglementation de l'État, mais provient du système lui-même.

233. Le rôle de « l'effet de masse » dans la régulation de la *blockchain* : les avantages du P2P. L'essentiel de l'argumentaire délivré par les « libéraux de la *blockchain* » met en exergue les fondements de la technologie, autrement dit son but ultime qui consiste en un réseau P2P s'exécutant en dehors de toute immixtion étatique

[1707] Pour une vision d'ensemble, v. par exemple, *id.* ; BONNEAU (Thierry), VERBIEST (Thibault), *Fintech et Droit : Quelle régulation pour les nouveaux entrants du secteur bancaire et financier ?*, éd. RB, coll. Les essentiels de la banque et de la finance, 2017, p. 80 ; Banque de France, « Focus n°10 : Les dangers liés au développement des monnaies virtuelles : l'exemple du bitcoin », Banque de France [en ligne], 5 déc. 2013, https://publications.banque-france.fr/sites/default/files/medias/documents/focus-10_2013-12-05_fr.pdf ; MEKKI (Mustapha), « Les mystères de la blockchain », *D.* 2017, n° 37, pp. 2160 et s., n°30 ; FÉNÉRON PLISSON (Claire), « La blockchain, un bouleversement économique, juridique voire sociétal », *Information, données & documents* 2017/3, vol. 54, p. 22 ; MARC (François), « Comptes rendus de la commission des finances : Enjeux liés au développement des monnaies virtuelles de type bitcoin - Table ronde », *Sénat* [en ligne], 15 janv. 2014, http://www.senat.fr/compte-rendu-commissions/20140113/fin.html#toc3.

[1708] FRIEDMAN (Milton), « The Effects of a Full-Employment Policy on Economic Stability », *in* « Essays in Positive Economics », *University of Chicago Press* [online], 1953, pp. 3-43, https://campus.fsu.edu/bbcswebdav/orgs/econ_office_org/PowerPoint_Files/2023-Joe_Calhoun/2023_Chapter_01/Friedman-Essays_in_Positive_Economics.pdf, cité dans : MENARD (Claude), « Du "Comme si..." au "Peut-être...". De Milton Friedman à la Nouvelle Économie Institutionnelle », *Revue d'Histoire des Sciences Humaines* 2005/1, série « Discipliner la ville – L'émergence des savoirs urbains (XIXe-XXe siècle) », n° 12, pp. 163-172. – V. également, VINTRAY (Alexis), « Milton Friedman et la critique du keynésianisme », *Contrepoints* [en ligne], 31 juill. 2012, https://www.contrepoints.org/2012/07/31/92049-milton-friedman-et-la-critique-du-keynesianisme : « loin d'atténuer les crises, elle ne fait que les aggraver. Les politiques contra-cycliques (destinées à lisser l'évolution économique) sont en fait pro-cycliques (elles accentuent les cycles économiques) » ; GATTY (Jean), « Sur Milton Friedman et son économie de la liberté », *Commentaire* 1996/3, n° 75, pp. 717-724.

[1709] IBANDA KABAKA (Paulin), art. cit., p. 1.

[1710] CHARENTENAY (Simon), « Blockchain et Droit : Code is deeply Law », *Gaz. Pal*. 14 nov. 2017, n° GPL305g1, p. 15.

perçue comme étant indigne de confiance à la suite des évènements ayant conduit à la crise économique de 2008[1711]. L'écosystème promulgue l'égalité, la liberté individuelle et l'intégrité. En principe, la loi du plus fort ne peut exister dans un tel système puisque personne ne gouverne à titre individuel et que *tous* gouvernent à titre collectif. Nul besoin de contraintes financières ou physiques à l'instar de celles prévues par le Code civil et le Code pénal pour faire respecter les règles du code informatique. En effet, dans le contexte d'un protocole *blockchain*, seule suffit la contrainte menée par l' « effet de masse »[1712]. La justification généralement donnée à cette thèse réside dans l'idée que le comportement individuel des utilisateurs et des nœuds importe peu au sens où, qu'ils soient bienveillants ou malveillants, c'est la somme de tous les comportements qui sera prise en compte. La confiance n'est de surcroît pas accordée à une ou plusieurs personnes en particulier, mais elle est placée dans la technologie elle-même, laquelle est reconnue intègre car neutre. Plus exactement, la technologie inspire confiance eu égard à ses multiples qualités. En fournissant à ses utilisateurs et participants un environnement dont elle garantit la sécurité, et au sein duquel ils peuvent inscrire des informations de différentes natures dont elle assurera la fiabilité et l'inviolabilité sans intermédiaire centralisé ni législateur[1713], la technologie pourrait à terme opérer un glissement de la confiance initialement accordée, presque de manière aveugle, aux organisations exclusivement humaines, à l'image des tiers nommés « de confiance »[1714]. De cette manière, la confiance devient presque une notion superflue.

234. L'essor d'un système spontané et auto-organisé. Huit ans avant la première récompense en *bitcoin*, un auteur annonçait que « *Code is Law* » serait la prochaine règle en vigueur sur Internet[1715]. En effet, selon les dires de Lawrence Lessig, la digitalisation des sociétés conduira à terme le cyberespace à être régulé par le code informatique. En

[1711] Pour plus de précisions sur l'apparition d'une crise de confiance et le remplacement par l'outil informatique, *supra* n° 3.
[1712] *Id.*
[1713] DE CHARENTENAY (Simon), « Blockchain et Droit : Code is deeply Law », art. cit., *loc. cit.*
[1714] BARRAUD (Boris), « Les blockchains et le droit », *RLDI* 2018/4, nº 147, p. 16. – LESSIG (Lawrence), « Code Is Law: On Liberty in Cyberspace », *Harvard Magazine* [online], 1st Jan. 2000, https://www.harvardmagazine.com/2000/01/code-is-law-html.
[1715] LESSIG (Lawrence), art. cit. : « *Ours is the age of cyberspace. It, too, has a regulator. This regulator, too, threatens liberty. But so obsessed are we with the idea that liberty means "freedom from government" that we don't even see the regulation in this new space. We therefore don't see the threat to liberty that this regulation presents. This regulator is code--the software and hardware that make cyberspace as it is. This code, or architecture, sets the terms on which life in cyberspace is experienced. It determines how easy it is to protect privacy, or how easy it is to censor speech. It determines whether access to information is general or whether information is zoned. It affects who sees what, or what is monitored. In a host of ways that one cannot begin to see unless one begins to understand the nature of this code, the code of cyberspace regulates.* »

considérant que les parties qui interagissent sur une *blockchain* – que ce soient les développeurs, les mineurs ou même les utilisateurs – évoluent dans un cadre déterminé, et dont les modalités sont dictées par le protocole, la justesse des observations de l'auteur se vérifie. Parfois nommée « *lex cryptographia* », cette maxime est finalement fondée sur l'acceptation d'une gouvernance auto-gérée par la technologie[1716]. Selon Primavera de Filippi, la technologie *blockchain* consiste donc en « une organisation spontanée, qui s'auto-organise avec les propriétés de coordination d'un marché, les propriétés de gouvernance d'un commun, et une capacité de prise de décision semblable à celle d'un État »[1717] et, constatant l'archaïsme des États, concède qu'ils sont voués à disparaître au profit de la technologie[1718].

Toutefois, bien que profondément disruptive, sa mise en œuvre n'est pas encore achevée et il apparaît notamment qu'aucune règle n'a été adoptée dans l'objectif de gérer les différends pouvant survenir entre les utilisateurs, laissant ces derniers dans l'incertitude. Cette pratique ne peut néanmoins échapper aux nombreuses difficultés qu'elle soulève, si bien que l'écosystème s'est proposé d'y remédier.

B. Les propositions de mécanismes intégrés de règlement des conflits

235. L'échec du système libertaire en matière de règlement des conflits. En vertu de la philosophie soutenue par l'écosystème, il est en principe exclu de faire appel aux juridictions étatiques tels que les tribunaux civils. Toutefois, comme le constate un auteur, un environnement entièrement dépourvu de litige, y compris au sein d'une *blockchain*, est irréaliste[1719]. Les premières versions des protocoles de *blockchains*, et en particulier de *Bitcoin*, ne prévoyaient aucun mode de résolution des litiges, si bien qu'en cas de contentieux sur la chaîne, les utilisateurs étaient libres dans la manière de régler leurs différends[1720]. La gestion des contentieux, et notamment contractuels, était donc laissée

[1716] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 18.
[1717] DE FILIPPI (Primavera), « Perspectives et enjeux des blockchains de demain », *in* Blockchain France, *La blockchain décryptée : Les clefs d'une révolution*, éd. Netexplo, 2016, p. 36.
[1718] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 16. – Pour plus de détails sur le sujet, v. directement, DE FILIPPI (Primavera), WRIGHT (Aaron), *Blockchain and the Law: The Rule of Code*, ed. Hardcover, 2018.
[1719] CIEPLAK (Jenny), « 5 reasons dispute resolution is critical for blockchain's growth », *World Economic Forum* [online], 14 Dec. 2020, https://www.weforum.org/agenda/2020/12/dispute-resolution-is-critical-for-blockchains-successful-growth-heres-5-reasons-why/.
[1720] CESSAC (Cécile) *et al.*, « La blockchain, c'est quoi ? », *CRE* [en ligne], 2 mai 2018, http://www.smartgrids-cre.fr/index.php?rubrique=dossiers&srub=blockchain&action=imprimer.

aux parties, dans un modèle-type amiable. Seulement, sans cadre défini[1721], une telle configuration peut rapidement se transformer en un environnement où règne la « loi du plus fort ». La nécessité d'une gestion active, sinon efficace, des différends au sein des *blockchains* a marqué le début de mises à jour importantes des protocoles.

236. Une gestion des conflits nécessaire : l'organisation en interne d'une solution de règlement amiable des différends[1722]. Les mises à jour protocolaires ont permis de proposer un mécanisme faisant intervenir, à la demande des parties, un tiers indépendant, qui peut être un utilisateur ou un autre participant du système, en tant que « médiateur sectoriel »[1723] ou « tiers-arbitre », impartial et neutre, pour les aider à rétablir l'équilibre de leurs relations. Tout en se substituant à la justice étatique, sa mission est de faciliter la discussion entre les parties pour leur permettre d'envisager un accord mettant fin à leur conflit dans des conditions raisonnables. Ces hypothèses témoignent à nouveau de l'importance d'anticiper lors de la rédaction du code informatique afin de pouvoir intégrer ces décisions. La résolution des contentieux de transactions de nombre de ces chaînes repose ainsi sur une forme de médiation conventionnelle, telle qu'instituée par les art. 1532 et s. du CPC[1724].

Semblable au modèle français des « modes alternatifs de règlement des conflits » (MARC) ou « modes alternatifs de règlement des litiges » (MARL) des art. 1528 à 1568 du CPC, et équivalent aux « *Alternative Dispute Resolutions* » (ADR) anglo-saxonnes[1725], ce type de démarche est par ailleurs vivement promu par l'UE en matière de règlement extrajudiciaire des litiges de consommation[1726]. Sous l'angle des ADR, le mécanisme de règlement amiable des différends mis en place au sein du protocole pourrait être assimilé aux solutions automatisées des *Online Dispute Resolutions* (ODR) qui consistent, selon un auteur, en la « mise à disposition des ressources des TIC au service

[1721] En comparaison avec la convention de procédure participative des art. 2062 et s. du C. civ., le règlement amiable permet aux « parties à un différend » de s'engager « à œuvrer conjointement et de bonne foi à la résolution amiable de leur différend ou à la mise en état de leur litige », avec l'assistance d'un avocat.
[1722] Cette solution correspond au « mécanisme privé de résolution des litiges » (*Private Dispute Resolution Mechanisms and Protocols*) évoqué dans le rapport du World Economic Forum en collaboration avec Latham & Watkins [World Economic Forum, Latham & Watkins, « Bridging the Governance Gap: Dispute resolution for blockchain-based transactions », World Economic Forum [online], Dec. 2020, p. 13, http://www3.weforum.org/docs/WEF_WP_Dispute_Resolution_for_Blockchain_2020.pdf].
[1723] LORRE (Pierre-Marie), « Blockchain : évolution ou révolution pour les contrats en France ? », Courbevoie : Institut Léonard de Vinci [en ligne], 2016, p. 16, https://www.forumatena.org/files/livres blancs/LORE_BLOCKCHAIN_CONTRATS-FA.pdf.
[1724] COIFFARD (Didier), « Entretien du mois : La Blockchain a un sens pour répartir une partie de la confiance en rendant une information infalsifiable mais cette confiance est très en deçà de celle conférée par le notaire », *RLDC* 2017/4, n° 147.
[1725] HERZOG (Philippe E.), « Tendances actuelles concernant les méthodes alternatives de résolution des controverses (Alternative dispute resolution – A.D.R.) aux États-Unis », *RGDP* 1999, pp. 774 et s.
[1726] *Ibid.*, pp. 16-17.

de la résolution des litiges »[1727]. Puisqu'il fait appel à des « moyens simples, efficaces, rapides et peu onéreux de [résolution des] litiges nationaux et transfrontaliers »[1728], le recours aux MARC constitue un intérêt pour de nombreuses branches du droit procédural au-delà de celle de « la vente de marchandises ou de la prestation de services ». En matière de baux commerciaux, par exemple, le décret n° 2015-282 du 11 mars 2015, relatif à la simplification de la procédure civile, à la communication électronique et à la résolution amiable des différends, incite vivement les parties à mettre en œuvre les « diligences » nécessaires « en vue de parvenir à une résolution amiable du litige »[1729]. Cette solution fait également écho à la loi n° 2019-222 du 23 mars 2019[1730], qui met en avant le développement des modes de résolution amiable des différends notamment en ce qui concerne les demandes tendant au paiement d'une somme n'excédant pas 5 000 €, de sorte à désormais obliger le demandeur à y recourir en amont du procès civil (CPC, art. 750-1). Reprenant l'idée exprimée en 1790 par le député Louis-Pierre-Joseph Prugnon selon laquelle « rendre la justice n'est que la seconde dette de la société ; empêcher les procès, c'est la première et il faut que la société dise aux parties : pour arriver au temple de la justice, passez par celui de la concorde »[1731], les parties doivent désormais justifier de leur tentative pour résoudre le litige à l'amiable préalablement l'introduction de la cause. À défaut, le juge peut prononcer d'office l'irrecevabilité de la demande (CPC, art. 750-1). Bien que l'intervention d'un tiers soit inévitable, le recours préalable *via blockchain* pourrait ainsi permettre une solution plus rapide et limiter non seulement les risques de blocages[1732], mais également les recours à l'exception pour motif légitime (CPC, art. 750-1, 3°)[1733]. Programmées au sein d'un *smart contract*, les dispositions du compromis pourraient de surcroît bénéficier d'une exécution automatisée *via* la *blockchain*[1734].

[1727] POULLET (Yves), « L'ODR au service de l'ADR : Quelques réflexions en marge du Colloque de Vienne : Kollektiver Rechtsschutz du 23 février 2005 », *CRID* [en ligne], févr. 2005, p. 1, http://www.crid.be/pdf/public/5296.pdf.

[1728] Dir. n° 2013/11/UE du Parlement européen et du Conseil, 21 mai 2013, relative au règlement extrajudiciaire des litiges de consommation et modifiant le règlement (CE) n° 2006/2004 et la directive 58-2009/22/CE, *JOUE* L 165/63, 18 juin 2013, considérant n° 4. Directive transposée en droit français par l'Ord. n° 2015-1033, 20 août 2015, relative au règlement extrajudiciaire des litiges de consommation, *JORF* n° 0192, 21 août 2015, p. 14721, texte n° 43.

[1729] CPC, art. 56. – V. également, CPC, art. 58, 127.

[1730] Il s'agit de la L. n° 2019-222, 23 mars 2019, de programmation 2018-2022 et de réforme pour la justice, *JORF* n° 71, 24 mars 2019, texte n° 2, et de son décret d'application, le Décr. n° 2019-1333, 11 déc. 2019, réformant la procédure civile, *JORF* n° 288, 12 déc. 2019, texte n° 3.

[1731] PRUGNON (Louis-Pierre-Joseph), *Archives parlementaires*, t. XVI, 31 mai-8 juillet 1790, p. 739.

[1732] Cons. const., 21 mars 2019, n° 2019-778 DC, not. n° 19-20, *AJDA* 2019, p. 663.

[1733] MAUGAIN (Géraldine), « Cas de recours préalable obligatoire aux modes de résolution amiable des différends », *in* « Dossier : Réforme de la procédure civile », *Dalloz actualité*, 20 janv. 2020, obs. MAUGAIN (Géraldine), SCHREIBER (Ulrik), MOURRE-SCHREIBER (Marie-Pierre) *et al*.

[1734] DE CHARENTENAY (Simon), art. cit.

237. L'essor de *Kleros*, une juridiction sous forme de *smart contract*[1735]. C'est sur ce fondement, à savoir simplifier l'organisation de la procédure civile et inciter à la résolution amiable des différends, que certaines *start-ups* ont développé leur propre protocole *blockchain* de règlement des conflits, à l'image de *Kleros,* développé par la coopérative française éponyme. « Chance » en grec, *kleros* était une machine de pierre qui servait sous l'Antiquité à tirer au sort les citoyens-juges lors d'un conflit[1736]. Aujourd'hui, *Kleros* est une DAO programmée sur la *blockchain Ethereum*[1737] mettant en œuvre un système de juges volontaires et classés selon leurs domaines de compétences, mis au service des utilisateurs de *smart contracts* confrontés à un litige[1738]. En plus de mettre également en œuvre une solution automatisée d'ODR, la justice est, par ce biais, directement rendue aux mains des citoyens[1739].

Pour bénéficier du mécanisme de règlement des différends proposé par le protocole, il est nécessaire de conclure un *smart contract* dont l'objet est de désigner *Kleros* en tant que « protocole de juridiction »[1740]. Lorsqu'un litige est déclaré, le protocole fait une sélection des informations contenues dans la *blockchain* et les transmet au juge sélectionné de manière transparente par tirage au sort parmi les utilisateurs volontaires et spécialisés pour arbitrer le conflit. Dès lors qu'un accord est trouvé pour résoudre le différend, celui-ci est automatiquement exécuté et des « frais d'arbitrage » sont directement versés au juge *via* le *smart contract* originel. La mise en place d'un second degré de décision[1741], associé à l'implémentation de la théorie des jeux au sein du protocole à travers la mise en place d'une incitation à l'honnêteté permettent de garantir l'intégrité de la décision du juge décentralisé[1742]. Ainsi, une décision réformée au cours d'une demande de réexamen de l'affaire conduira le système à saisir les frais d'arbitrage

---

[1735] Cette solution correspond aux exemples de mécanimes d' « arbitrage par un tiers » (*Third Party Arbittration*) évoqué dans le rapport du World Economic Forum en collaboration avec Latham & Watkins [World Economic Forum, Latham & Watkins, préc., p. 15].

[1736] ALLISON (Ian), « Kleros: Ethereum smart contracts meet ancient Greek legal democracy », *International Business Time* [online], 6 Mar. 2018, https://www.ibtimes.co.uk/kleros-ethereum-smart-contracts-meet-ancient-greek-legal-democracy-1665300 – PEYTON (Antony), « Blockchain and Bitcoin round-up: 23 January 2018 », *FutureTech* [online], 23 Jan. 2018, https://www.bankingtech.com/2018/01/blockchain-and-bitcoin-round-up-23-january-2018/.

[1737] « Kleros : la justice décentralisée », *Journal du Coin* [en ligne], 14 juin 2018, https://journalducoin.com/ico/kleros-la-justice-decentralisee/.

[1738] « Kleros Joins Thomson Reuters Incubator to Build a Justice Protocol for the Internet », *Venture Beats* [online], 8 May 2018, https://venturebeat.com/2018/05/08/kleros-joins-thomson-reuters-incubator-to-build-a-justice-protocol-for-the-internet/.

[1739] KIM (Jay), « In The Future Blockchain Will Solve Most Real-World Problems - Even Arbitration », *Forbes*, 4 Apr. 2018, https://www.forbes.com/sites/kimjay/2018/04/04/in-the-future-blockchain-will-solve-most-real-world-problems-even-arbitration/#4021179bbd2f.

[1740] V. le site officiel de Kleros, https://kleros.io/fr/, Accueil > Rubrique > « Protocole de résolution des litiges sur la blockchain ».

[1741] AUDIT (Mathias), « Le droit international privé confronté à la blockchain », *Rev. crit. DIP* 2020, p. 669.

[1742] KIM (Jay), art. cit.

versés au premier juge, pour rétribuer le second[1743]. La *blockchain* assure par ailleurs qu'aucune partie ne puisse altérer les preuves ni manipuler la sélection du jury.

Rapide, sécurisé et à moindre coût, le protocole propose divers domaines d'application, tels que les réseaux sociaux, les jeux en ligne, le *e-commerce* ou encore l'investissement participatif. Il peut, par exemple, intervenir lorsqu' « un commentaire déplacé est posté sur un réseau social décentralisé qui va à l'encontre des termes et conditions de la plateforme. Les juges de *Kleros* peuvent [alors] décider de supprimer ce contenu et […] d'enlever des points de réputation à l'utilisateur à l'origine de ce contenu »[1744]. Il peut en aller également ainsi concernant un « produit acheté en ligne [et qui] ne correspond pas à sa description. *Kleros* peut décider d'arbitrer en faveur de l'acheteur et de lui rembourser son achat »[1745]. Enfin, si « un *freelancer* réalise un *smart contract* avec un client sur un autre continent [et que] le service rendu ne correspond pas aux attentes du client », celui-ci peut faire appel à *Kleros* afin d' « analyser les preuves, voter et donner le verdict »[1746]. La pratique actuelle indique que les litiges portant sur des contrats importants de droit des affaires échappent progressivement à la sphère juridictionnelle pour migrer vers des modes de résolution extrajudiciaire tels que l'arbitrage privé[1747]. C'est dans ce contexte que la solution d'une juridiction décentralisée et transparente apparaît prometteuse[1748]. La pratique révèlera si la justice sera à nouveau rendue par des jurés munis de « *klèrôtèrion* » (*κληρωτήριον*) et désignés par une boule blanche[1749].

238. Bien que le développement de *Kleros* fasse l'objet d'une attention particulière, notamment depuis sa nomination au Prix du Conseil européen de l'innovation (EIC) sur les *blockchains* œuvrant pour le bien social[1750], l'analyse du principe de règlement

[1743] AUDIT (Mathias), art. cit., *loc. cit.*
[1744] V. le site officiel de Kleros, https://kleros.io/fr/, Accueil > Rubrique > « Cas d'utilisation ».
[1745] *Id*.
[1746] *Id*.
[1747] FABRE-MAGNAN (Muriel), *Le droit des contrats*, éd. PUF, coll. « Que sais-je ? », 2018, p. 110.
[1748] KIM (Jay), art. cit.
[1749] Le système démocratique sous l'Antiquité grecque était le suivant ; les jours d'essai, les Grecs qui voulaient faire partie du jury prenaient une plaque de bronze appelée « *pinakion* » et la plaçaient dans un grand bloc de pierre avec de nombreuses fentes appelées « *klèrôtèrion* ». Un fonctionnaire du système judiciaire sélectionnait ensuite des jurés en lançant des boules blanches et noires sur la *kleroterion*. La rangée disposant d'une boule blanche faisait partie du jury. Une balle noire signifiait pour l'autre rangée qu'elle était renvoyée. Ce système a permis au processus de sélection des jurés d'être équitable et transparent, en plus d'empêcher toute falsification [v., RATTO (Stefania), *Greece: Volume 3 de Dictionaries of civilization Dizionari delle civiltà*, ed. University of California Press, Vol. 3, 2008, pp. 63-65].
[1750] Le Prix du Conseil européen de l'innovation (EIC) sur les *blockchains* pour le bien social a attribué cinq millions d'euros à six lauréats sélectionnés, au sein desquels figure *Kleros*, dans le cadre d'un appel à identifier des solutions de *blockchain* évolutives, déployables et à fort impact pour les défis sociétaux. C'est dans la catégorie Économie Circulaire Décentralisée que la plateforme CKH2020 de *Kleros*, qui propose donc un mécanisme de résolution des litiges de consommation dans le *e-commerce* ou dans l'économie

décentralisé des litiges, quelle que soit la forme qu'il prend, mène à interroger tant l'application des principes juridictionnels traditionnels que la maturité technique de ces solutions.

§ 2. La recrudescence du rôle du juge

239. Sous l'angle du droit des contrats, le législateur a toujours eu tendance à osciller entre, d'une part, la protection de la partie faible au contrat, adoptant alors une vision de la sécurité juridique comme « garantie de la justice par le droit », et, d'autre part, l'autonomie de la volonté, approuvant une vision de la sécurité juridique cette fois comme garantie d'un « droit des contrats très peu interventionniste, [presque] discr[et] »[1751]. Face à ces opinions divergentes quant à l'intervention du juge et du droit de manière générale, le législateur de 2016 s'est efforcé de trouver un certain équilibre[1752]. Par ailleurs, l'absence de conflits étant irréaliste, la solution réside donc dans l'utilisation d'un modèle extrajudiciaire de règlement des conflits[1753]. Cependant, en l'état de l'art, l'utilisation des mécanismes intégrés de règlement des différends est assortie d'un certain nombre de limites. Malgré leur encourageante progression, leur capacité à mettre en œuvre une protection suffisante des parties, notamment de la plus faible d'entre-elles, continue de prêter à discussion. Par conséquent, les imperfections des mécanismes intégrés de règlement des conflits, si elles ne sont pas corrigées, pourraient rapidement conduire la technologie à connaître une dépréciation de la confiance de ses utilisateurs (A). En la matière, le juge, sous diverses qualifications, constitue depuis longtemps le garant national de la sécurité juridique et du droit en tant que principal intermédiaire des parties et autorité décisionnelle. Ces divers constats suggèrent que le juge étatique puisse retrouver l'essentiel de son autorité en la matière afin de rééquilibrer le rapport de force contractuel actuellement imposé par le code, rendant dès lors nécessaire une collaboration entre la technologie et le juge (B).

---

collaborative, a été sélectionnée [Digibyte, « The Commission's European Innovation Council awards €5 million to blockchain solutions for social innovations », *European Commission* [online], 30 Jun. 2020, European Commission > Strategy > Shaping Europe's digital future > News, https://ec.europa.eu/digital-single-market/en/news/commissions-european-innovation-council-awards-eu5-million-blockchain-solutions-social].

[1751] FABRE-MAGNAN (Muriel), *Le droit des contrats*, *op. cit*., p. 109.

[1752] Rapp. au Président de la République n°2016-131, 11 févr. 2016, relatif à l'ordonnance du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, *JORF* n°0035, 11 févr. 2016, Titre Ier, Sous-titre Ier, Chapitre Ier : « Les articles 1102, 1103 et 1104 énoncent ensuite les principes de liberté contractuelle, de force obligatoire du contrat et de bonne foi. Ce choix de mettre en exergue trois principes fondamentaux exprime l'un des objectifs essentiels poursuivis par l'ordonnance : il s'agit de trouver un équilibre entre justice contractuelle et autonomie de la volonté. »

[1753] CIEPLAK (Jenny), art. cit.

240. Un mécanisme de règlement amiable des litiges innomé : problème de qualification et autres hypothèses restant sans réponse. En vertu des Livres IV et V du Code civil, les parties à un différend peuvent choisir la voie extrajudiciaire afin de résoudre leur litige. Selon les modalités et conditions établies pour chaque régime, les parties peuvent ainsi faire appel à un médiateur (CPC, art. 1532), à un conciliateur de justice (CPC, art. 1528), ou à un arbitre (CPC, art. 1442). Toutefois, la liberté laissée aux utilisateurs quant à l'aménagement du mécanisme de règlement des litiges intégré à une *blockchain* rend difficile la distinction entre les modes de résolution amiable des différends communément admis. À l'évidence, la question se pose de savoir s'il s'agit d'une conciliation ou d'une médiation, étant donné que le mécanisme mis en place en interne semble s'imposer sans requérir l'acceptation des utilisateurs, ni laisser le choix aux parties des modalités de règlement de leur litige (CPC, art. 1442 et s.). Le médiateur comme le conciliateur donnent un avis sur le différend qui leur est soumis. Mais, contrairement au médiateur[1754], le conciliateur formule une solution, laquelle figurera sous la forme d'un constat d'accord qui devra être accepté par les parties[1755]. Néanmoins, rien ne précise, en ce qui concerne le mécanisme mis en place en interne, s'il est également procédé par accord nécessairement inscrit sur la chaîne. Par ailleurs, en vertu du décret n° 78-381 du 20 mars 1978 relatif aux conciliateurs de justice, le conciliateur dispose du statut de conciliateur de justice et doit par conséquent être nommé « par ordonnance du premier président de la cour d'appel, après avis du procureur général, sur proposition du magistrat coordonnateur des tribunaux d'instance »[1756]. À nouveau, les règles de fonctionnement du mécanisme interne de résolution des litiges ne semblent pas indiquer précisément la manière dont cette tierce personne est nommée sur la *blockchain*, ni énoncer les règles applicables à cette désignation. Celles-ci prévoient-elles la désignation d'un tiers connu des parties, ou organisent-elles un tirage au sort, éventuellement encadré ? De la même manière, la désignation s'opère-t-elle au sein de l'ensemble des utilisateurs et mineurs de la chaîne, ou au sein d'utilisateurs uniquement volontaires ? Aussi semble-t-il que la résolution des contentieux de transactions de

[1754] VERGÈS (Étienne) (dir.), « ETUDE : Les procédures amiables », *Encyclopédie Procédure civile*, Lexbase, 20 déc. 2018.
[1755] CPC, art. 1540.
[1756] Décr. n° 78-381, 20 mars 1978, relatif aux conciliateurs de justice, *JORF* n° 0070, 23 mars 1978, art. 3, modifié par le Décr. n° 2018-931, 29 octobre 2018, modifiant le décret n° 78-381 du 20 mars 1978 relatif aux conciliateurs de justice, *JORF* n° 0252, 31 oct. 2018, texte n° 9, art. 3.

nombre de chaînes repose davantage sur une forme de médiation conventionnelle, telle qu'instituée par les art. 1532 et s. du CPC[1757]. En effet, bien que la qualification de « médiation » au sens de l'art. 1532 reste malgré tout incertaine, en particulier parce que rien ne précise si le tiers intervenant au sein de la *blockchain* « possède […] la qualification requise eu égard à la nature du différend ou justifie, selon le cas, d'une formation ou d'une expérience adaptée à la pratique de la médiation » (CPC, art. 1533, 2°), son régime semble être ce qui s'en rapproche le plus.

Il n'empêche que ce flou dans l'organisation d'un tel système n'est pas sans soulever de nombreuses difficultés, en particulier vis-à-vis de la protection de la partie faible au contrat conclu. En vertu des règles attenantes aux multiples mécanismes de résolution extrajudiciaires des conflits, le tiers choisi doit de surcroît faire preuve d'impartialité et de diligence dans la réalisation de sa mission, en plus de devoir disposer des compétences nécessaires (CPC, art. 1530). Or, rien sur la chaîne ne semble permettre de l'assurer. Par ailleurs, étant donné qu'aucun contrat ne laisse aux parties le choix des règles applicables, dans l'hypothèse où les parties n'ont donc pas eu la possibilité de choisir directement leur médiateur ou conciliateur, est-il permis à l'une d'elles de demander à le remplacer ? De la même manière, la question se pose de savoir si les parties pourraient avoir accès à un second degré de décision qui leur permettrait de demander un nouvel examen des prétentions et des intérêts en présence. Elles pourraient effectivement estimer que la décision est non-proportionnée, voire illégitime ou illégale, et pourraient dans ce cas requérir l'avis d'un juge étatique pour s'en assurer, d'autant plus si l'utilisateur désigné pour être juge ne dispose pas des connaissances juridiques requises, ou d'une formation ou expérience adaptée à sa mission. Ne pas pouvoir qualifier précisément pose la question de l'application des règles propres à chaque régime, et en particulier la question de la responsabilité de l'intermédiaire. Alors que l'arbitre « bénéficie, en tant que juge, d'une immunité juridictionnelle de sorte qu'il n'est responsable que de sa faute personnelle qui, pour engager sa responsabilité, doit être équipollente au dol, constitutive d'une fraude, d'une faute lourde ou d'un déni de justice »[1758], le conciliateur de justice n'est pas un auxiliaire de justice. Par conséquent, les conséquences financières de sa responsabilité civile « professionnelle » sont assumées et prises en charge par l'État[1759]. Dans la mesure où il ne rend pas de décision, sa mise en cause ne peut toutefois intervenir qu'en des cas limités, par exemple, de défaut d'impartialité, de violation de l'obligation de confidentialité et d'une manière générale

[1757] COIFFARD (Didier), art. cit., n° 147.
[1758] Cass. Civ. 1ère, 15 janv. 2014, n° 11-17.196, *Bull.* 2014, I, n° 1.
[1759] Rép. min. n° 16745, *JO Sénat*, 5 janv. 2012, p. 33.

d'infraction aux règles déontologiques[1760]. Plus limitée encore est l'étendue de la responsabilité du médiateur puisqu'il n'a qu'une obligation de moyen, si bien qu'il ne peut engager que sa responsabilité civile à raison d'une faute personnelle ou déontologique[1761]. Mais il n'empêche qu'en matière de mécanisme décentralisé de règlement des conflits, la question de la responsabilité des intervenants ne pourra se résoudre, ni par l'argument de l'immunité juridictionnelle, ni par la garantie de l'État.

241. Une juridiction sous forme de *smart contract* : une solution envisageable. Selon un auteur, la solution la plus adaptée parmi les trois modes de résolution extrajudiciaire des litiges réside malgré tout dans le recours à l'arbitrage[1762]. En effet, au-delà des avantages soulevés vis-à-vis du caractère international de la technologie[1763], l'auteur souligne deux caractéristiques déterminantes. D'une part, présente un intérêt pour les parties la flexibilité du régime de l'arbitrage, et en particulier de l'arbitrage commercial international, qui les laisse libres de déterminer l'ensemble des modalités du processus de règlement des litiges, sous réserve de respecter le droit procédural et les droits fondamentaux (CPC, art. 1508). D'autre part, l'issue permise par l'arbitrage, qui consiste en une décision qui s'impose aux parties (CPC, art. 1484, al. 1er), peut contribuer à réduire les difficultés précédemment rencontrées en la matière. En application des principes éthiques établis par le National Center for Technology and Dispute Resolution de l'Université du Massachusetts (USA), le système de règlement extrajudiciaire des conflits devrait simplement garantir un certain nombre de fonctionnalités, telles que l'accessibilité du service à tout utilisateur, la confidentialité, la sécurité et le triptyque juste-impartial-neutre[1764]. Des *start-ups* comme Datarella's Codelegit Certified Blockchain Arbitration Librar ont d'ores et déjà testé et développé ce type de mécanisme[1765]. C'est de cette idée qu'est née la plateforme *Kleros*. En effet, cette solution consistant en un « protocole de juridiction » désigné par les parties à un *smart contract*

[1760] *Id.*
[1761] GORCHS (Béatrice), « La responsabilité civile du médiateur civil », *Dr. et pr*. 2015, p. 194.
[1762] GILLIOZ (Fabien), « Du contrat intelligent au contrat juridique intelligent », *D. IP/IT* 2019, n° 1, pp. 16 et s.
[1763] Il s'agit notamment des avantages tirés de la Convention sur la reconnaissance et l'exécution des sentences arbitrales étrangères de 1958 qui facilite la reconnaissance à l'étranger des sentences arbitrales. – Sur les difficultés liées au caractère international de la technologie *blockchain*, *infra* n°s 254 et s.
[1764] V. ICODR Standards sur le site officiel du National Center for Technology and Dispute Resolution, https://icodr.org/standards/. – V. également, WAHAB (Mohamed S. Abdel), KATSH (Ethan), RAINEY (Daniel), *Online Dispute Resolution: Theory and Practice*, ed. Eleven International Publishing, 2012.
[1765] « CodeLegit White Paper on Blockchain Arbitration », [online], https://docs.google.com/document/d/1v_AdWbMuc2Ei70ghITC1mYX4_5VQsF_28O4PsLckNM4/edit#heading=h.p2owquwx39n. – V. également le site officiel, http://codelegit.com.

sous la forme d'une clause compromissoire[1766], semble pouvoir être assimilée à une convention d'arbitrage qui serait susceptible d'être directement implantée sur la chaîne et liée à un *smart contract* principal (CPC, art. 1442). En vertu des art. 1442 et s. du CPC régissant le régime de l'arbitrage comme mode de résolution amiable des conflits, l'exercice doit aboutir à une décision ayant autorité de la chose jugée, au même titre qu'une décision juridictionnelle, rendue par un ou des juges privés que les parties ont désignés. Outre le choix dans le protocole *Kleros* des appellations des utilisateurs-arbitres nommés « juges », investis d'une mission d'arbitrage amiable et délivrant des « décisions », il semble acceptable de considérer la désignation de *Kleros* comme la référence à un règlement d'arbitrage, lequel prévoit les modalités de désignation de l'arbitre (CPC, art. 1451-1454). Leur choix quant aux modalités de règlement des conflits inscrites sur une *blockchain* se résume ainsi à s'accorder contractuellement sur la désignation de *x* ou *y* protocole, équivalent donc au règlement d'arbitrage de l'art. 1444 du CPC. Simplement, puisque l'arbitre de *Kleros* appartient à une « foule » d'utilisateurs volontaires[1767], il est important que son identité fasse l'objet de vérifications suffisantes afin de remplir les conditions de fond attachées à la rédaction de la sentence arbitrale, à savoir l'indication du nom de l'arbitre qui l'a rendue (CPC, art. 1481, 3°).

Toutefois, le « protocole de juridiction » auquel sont censées se soumettre les parties *via smart contract* semble garder le silence quant à la possibilité pour ces dernières de révoquer le « juge » arbitre désigné par la plateforme, à l'instar de ce que prévoit le régime d'arbitrage traditionnel (CPC, art. 1458). Cette solution laisse également entière la question de savoir s'il est admis d'organiser spécialement en amont, dans le *smart contract* principal, cette faculté.

Au-delà de ces imprécisions, certaines caractéristiques entourant l'application du protocole de la plateforme sont sujettes à discussion, si bien que le système actuel pourrait être limité dans son déploiement.

242. Une juridiction sous forme de *smart contract* : une solution limitée par un champ d'application restreint et par la nécessité d'une anticipation. Implanter une forme de tribunal *ad hoc* décentralisé directement sur la *blockchain* rendrait le règlement des litiges indubitablement rapide, sûr et moins onéreux qu'une procédure traditionnelle devant un juge d'une juridiction étatique[1768]. Seulement, d'un point de vue technique, et

[1766] Kleros, site officiel : https://kleros.io/fr/ > Rubrique : « Protocole de résolution des litiges sur la *blockchain* ».
[1767] *Id.*
[1768] COIFFARD (Didier), art. cit., n° 147.

en l'état de l'art, ce système ne couvre pas l'intégralité des cas d'utilisations de la *blockchain*.

En effet, les protocoles de juridiction *Kleros* ne sont opérationnels qu'à la double condition, non seulement d'avoir noué une relation contractuelle *via smart contract*, mais également d'avoir désigné, au sein du *smart contract* principal, le « protocole de juridiction » comme règlement d'arbitrage intervenant en cas de litige. Soumettre ainsi son application à la rédaction d'une clause compromissoire, autrement dit non-obligatoire, ne peut que limiter son efficacité. Pour qu'il soit exécuté, un tel système doit être programmé. Par conséquent, il doit impérativement recueillir le consentement préalable des parties à l'acte[1769], ce qui requiert de leur part une anticipation dès l'inscription du *smart contract* sur la chaîne. Or, confrontées à la rigidité de la chaîne de transactions, et en particulier à l'impossibilité de modifier les inscriptions[1770], *quid* des parties en litige qui, par erreur, omission ou ignorance, n'auraient pas désigné un tel protocole de résolution des litiges dans leur *smart contract*[1771] ? Il semble qu'elles retomberaient dès lors dans le mécanisme originel consistant à tenter une résolution à l'amiable, éventuellement encadrée par un « médiateur sectoriel », ou encore appelé « tiers arbitre », sans toutefois relever du régime de l'arbitrage. Or cette solution ne serait pas satisfaisante du point de vue de la sécurité juridique. Le risque est pourtant d'exposer la technologie à une altération importante de la confiance de ses utilisateurs. De plus, eu égard au caractère décentralisé des chaînes, chaque *blockchain*, voire chaque utilisateur, pourrait établir des règles de fonctionnement différentes, si bien que la question ne serait plus de savoir ce qu'il serait possible de faire en l'absence d'exécution d'une solution de règlement des litiges comme *Kleros*, mais plutôt de savoir comment protéger les individus de l'émergence d'un « *No Law's land* » en la matière[1772]. D'une telle liberté non-contrôlée pourraient découler des inégalités entre utilisateurs, une hiérarchie des juges, le monopole d'un juge, ou même des choix stratégiques de chaînes selon leur système propre de règlement des litiges, qui prendrait alors la forme d'un « *dumping code laws* »[1773]. Force est de reconnaître que le champ de contrainte des conventions d'arbitrage et des clauses

[1769] *Id.*
[1770] *Supra* n°s 183 et s., notamment n°s 212-213.
[1771] BERBAIN (Côme), « La blockchain : concept, technologies, acteurs et usages », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 4.
[1772] THÉOCHARIDI (Eva), « La conclusion des smart contracts : révolution ou simple adaptation ? », *RLDA* 2018/6, n° 138.
[1773] BAÏKOFF (Stéphane), RBINEAU (Marie), « La blockchain : un outil juridique bientôt incontournable ? », *Solutions numériques* [en ligne], 15 janv. 2018, https://www.solutions-numeriques.com/la-blockchain-un-outil-juridique-bientot-incontournable/.

compromissoires, lesquelles sont susceptibles d'être directement exécutées sur la chaîne, tendent à limiter leur propre déploiement.

Tandis que demeurent certaines incertitudes quant à l'application effective des règles de droit en la matière, une autre conséquence de la décentralisation du système semble faire également obstacle, y compris à des règles d'ordre public (CPC, art. 1461). En effet, le régime de l'arbitrage requiert l'appui du président du tribunal judiciaire ou, si la convention le prévoit expressément, du président du tribunal de commerce, autrement dit d'un juge étatique, qui doit de surcroît être désigné au sein de la convention d'arbitrage (CPC, art. 1459). De la même manière, en vertu de l'art. 1449 du CPC, un juge étatique devrait pouvoir intervenir tant que le tribunal arbitral n'est pas constitué, aux fins de délivrer une mesure d'instruction ou une mesure provisoire ou conservatoire.

243. Quand bien même l'apport de la technologie en la matière serait conséquent, ces éléments, pris dans leur ensemble, ne permettent pas, pour l'instant, de supposer l'existence d'un système aussi protecteur que l'est en principe le système juridictionnel actuel. Aussi semble-t-il que seules l'expérience, les mises à jour et les années pourront inverser cette tendance. Le World Economic Forum en collaboration avec Latham & Watkins évoquent d'ailleurs la nécessité d'un consensus entre les protocoles existants[1774]. Il n'empêche qu'en l'absence de garantie d'une sécurité juridique sans condition, il apparaît difficile de se fier aux mécanismes de gestion des conflits proposés par la technologie sans maintenir la possibilité de recourir au juge. Cela dit, la confiance n'exclut pas le contrôle, ce qui mène à interroger la faisabilité d'un système à deux temps prévoyant, d'une part, une solution de règlement des conflits directement implantée sur la *blockchain* et, d'autre part, la faculté pour le juge étatique de retrouver l'essentiel de son autorité en la matière afin notamment de rééquilibrer le rapport de force contractuel actuellement imposé par le code. Indirectement, il semble que l'intervention du juge étatique pourrait même permettre le consensus préconisé.

B. De la protection de la partie faible vers une collaboration entre la technologie et le juge

244. Le juge, garant national de l'application du droit et de la sécurité juridique. La protection de la partie faible à la relation contractuelle peut justifier, dans certains cas particuliers, l'intrusion du juge dans le contrat liant les parties. Il en va ainsi, par exemple,

[1774] World Economic Forum, Latham & Watkins, préc., p. 8.

dans un contrat d'adhésion. En effet, par définition, ce type de convention admet que l'un des contractants soit forcément empêché de négocier l'ensemble ou une partie des termes de ses propres engagements. Étant donné que l'autre partie jouit souvent d'une supériorité dans le contrat, le législateur impose un certain nombre d'obligations dont la violation est susceptible d'engager sa responsabilité (C. civ., art. 1171). Des auteurs constatent qu' « en réservant la sanction du déséquilibre significatif aux seuls contrats d'adhésion, le gouvernement a relancé une controverse historique sur une catégorie doctrinale créée par Saleilles »[1775]. Or, il s'agit typiquement d'une relation pouvant naître au sein de la chaîne, notamment au sein d'un *smart contract*. En effet, alors même que la négociation de bonne foi (C. civ., art. 1104) paraît difficile à mettre en œuvre à travers l'algorithme d'une *blockchain*[1776], en règle générale, les contrats conclus prennent la forme de contrats « dont les conditions générales, soustraites à la négociation, sont déterminées à l'avance par l'une des parties » (C. civ., art. 1110). Autrement dit, les inscriptions et les *smart contracts* en particulier correspondent le plus souvent à ce que le droit français qualifie de contrats d'adhésion. Si le législateur reconnaît la validité de ce type de relations contractuelles, il l'encadre toutefois strictement en prohibant tout déséquilibre « significatif »[1777]. Sa qualification confère au juge un rôle essentiel qui consiste à contrôler l'équilibre et donc le contenu du contrat, et à intervenir s'il l'estime nécessaire afin de garantir l'égalité et l'équité dans la relation, tout en veillant à préserver cet équilibre contractuel.

Le juge étatique dispose également d'un pouvoir de révision du contrat dès lors que son exécution est devenue économiquement difficile. En cas de situation d'imprévision, ce pouvoir se transforme en devoir d'adaptation des dispositions contractuelles dont l'exécution est devenue « excessivement onéreuse pour une partie qui n'avait pas accepté d'en assumer le risque » (C. civ., art. 1195, al. 1er). Dans ce cadre, le juge dispose de moyens d'action conséquents lui permettant, par exemple, d'éteindre les obligations contractuelles entre les parties dans le cas où celles-ci ne parviendraient pas à trouver un accord (C. civ., art. 1195, al. 2).

En raison de son caractère décentralisé, le juge-arbitre, qu'il soit institué en interne ou par liaison à un protocole de juridiction, n'a théoriquement pas à respecter les exigences liées aux fonctions du juge judiciaire. Cependant, un tel contexte suggère que

[1775] CHANTEPIE (Gaël), SAUPHANOR-BROUILLAUD (Natacha), *Rép. civ. Dalloz*, v° Déséquilibre significatif, 2019, n° 172.
[1776] GUILHAUDIS (Élise), « Comprendre la blockchain à travers l'étude d'un cas pratique : le covoiturage "Blockcar" », *RLDI* 2017/12, nº 143, pp. 10-11.
[1777] Largement inspiré par les règles des art. L. 212-1 et s. du C. consom. que le législateur a reconnues « d'ordre public » (C. consom., art. L. 212-3), il semble que désormais le contractant à un contrat d'adhésion ne pourrait y déroger.

la partie faible au contrat conclu *via blockchain* ne bénéficie pas d'une protection effective de ses droits, de ses intérêts matériels et moraux, ni des garanties essentielles dont dispose chaque citoyen pour assurer le respect et la défense de ses droits[1778]. Il en va ainsi, par exemple, de l'hypothèse de la sanction automatique par verrouillage du véhicule loué en cas d'impayé. Par son caractère souvent unilatéral[1779], ce type de sanctions pourrait se voir opposer les dispositions protectrices relatives au contrat d'adhésion, et en particulier être sanctionné au titre des clauses instaurant un déséquilibre significatif.

De la même manière, le juge est le protecteur des parties viciées. Dans un contexte d'erreur, de dol ou de violence (C. civ., art. 1109), le juge est la figure étatique de la sécurité contractuelle et, par conséquent, de la confiance. Il est également le juge de la proportionnalité (C. civ., art. 1121) et est à ce titre investi du pouvoir de contrôler et d'interrompre les mesures d'exécution injustes, intempestives ou disproportionnées[1780], quand bien même les parties n'auraient pas prévu *ab initio* ces hypothèses. Dans le cas d'un contrat auto-exécuté ou de l'intervention d'un « juge décentralisé », la question se pose de savoir si des notions à contenu variable fondamentales en droit des contrats[1781] telles que les notions « légitime », « excessif », « raisonnable », ou encore « disproportionné », feront l'objet d'un contrôle et, si oui, par qui et comment ? Puisqu'en effet, force est de reconnaître que si ces concepts se révèlent souvent être une source de difficulté pour la traduction en langage algorithmique, est tout aussi délicat leur contrôle par des « juges » choisis parmi des utilisateurs lambdas. Une multitude d'autres difficultés mettant en cause la sécurité juridique se présentent. La question se pose par exemple de savoir de quelle manière un « juge décentralisé » interviendrait s'il était confronté à un preneur à bail de locaux à usage d'habitation qui rechercherait la responsabilité de son bailleur pour défaut d'exécution d'une de ses obligations, alors que ce dernier propose d'exécuter son obligation en nature[1782] ? Quelle serait également son appréciation de la situation d'un acheteur qui, exerçant son droit d'option concernant la poursuite forcée de la vente plutôt que sa rupture (C. civ., art. 1184), contraindrait le vendeur à livrer un produit dont la fabrication a été arrêtée[1783] ? Un auteur constate qu'il n'est pas déraisonnable de penser que les dispositions d'un contrat sur une *blockchain*

[1778] GUINCHARD (Serge), DRAGO (Guillaume), « Réforme de la procédure civile en 1958 et Constitution de la V^e^ République », *Rép. pr. civ. Dalloz*, v° Droit constitutionnel et procédure civile, 2018, n° 15.
[1779] GUERLIN (Gaëtan), « Considérations sur les smart contracts », *D. IP/IT* 2017, n° 10, p. 512.
[1780] RODA (Jean-Christophe), « Smart contracts, dumb contracts ? », *D. IP/IT* 2018, n° 2, p. 397, n° 11.
[1781] *Id.* ; POULLET (Yves), JACQUEMIN (Hervé), « Blockchain : une révolution pour le droit ? », art. cit., pp. 817-818.
[1782] Cass. Civ. 3^e^, 27 mars 2013, n° 12-13.734, *D*. 2013, p. 910.
[1783] Cass. Com., 5 oct. 1993, n° 90-21.146. – Sur l'impossibilité de poursuivre l'exécution forcée choisie par un locataire exigeant la délivrance d'un local alors que celui-ci a entretemps été loué à un tiers, v. également, Cass. Civ. 1^ère^, 27 nov. 2008, n° 07-11.282.

pourraient constituer un abus de droit dès lors qu'elles ne sont pas sanctionnées[1784]. Par ailleurs, l'autorité dont bénéficie le « juge décentralisé » suscite également une réelle interrogation sur le plan du pouvoir de contrainte. En effet, a-t-il la faculté de contraindre un débiteur récalcitrant à s'exécuter ou de requérir du créancier une réduction du prix en proportion du travail mal effectué[1785] ? Le juge étatique, quant à lui, dispose en toutes circonstances des outils juridiques nécessaires pour remplir cet office[1786]. C'est en cela que la philosophie *blockchain* semble se heurter le plus avec la philosophie du droit positif[1787]. Nombre d'auteurs du libéralisme idéalisent un modèle de relations humaines basé sur la présupposition d'un consentement librement exprimé[1788]. Un tel système admettrait un postulat de départ légitimant l'instauration inévitable d'une loi du plus fort au sein des relations contractuelles, puisqu'aucune régulation protectrice ne pourrait intervenir. Il est donc indéniable que des incompatibilités subsistent[1789]. Pour autant, cette finalité est en réalité contraire à l'intention originelle de la *blockchain* qui a toujours été d'instituer une démocratie décentralisée capable de faire renaître la confiance nécessaire à son expansion, et non une nouvelle forme de hiérarchie consolidée par les inégalités.

En définitive, l'état actuel du développement de la technologie atteste à nouveau de l'importance mais également de la nécessité de l'intervention du juge étatique dans la gestion des conflits opposant des utilisateurs d'une *blockchain*[1790].

245. L'intervention du juge comme juridiction alternative. Comme le souligne Simon De Charentenay, « tout un cortège de questions se posent sur la possibilité de corréler l'accroissement de sécurité technique avec autant de sécurité juridique »[1791]. Cette forme de collaboration temporaire pourrait être appréciée si le point de vue initialement donné était renversé. De cette manière, le juge et la technologie pourraient être, l'un pour l'autre, une source à la fois de sécurité et de confiance. Bien que la profession se montre encore réticente sur ces questions, il est clair que l'évolution se fera dans le sens d'une dématérialisation accrue. Force est de constater toutefois qu'en l'état de l'art, la technologie *blockchain* repose sur des règles encore trop éloignées, tant des

[1784] POULLET (Yves), JACQUEMIN (Hervé), « Blockchain : une révolution pour le droit ? », art. cit., p. 817.
[1785] C. civ., art. 1223.
[1786] RODA (Jean-Christophe), art. cit., *loc. cit*.
[1787] *Id.*
[1788] Tel que Friedrich Hayek. Sur la « catallaxie », v., VON HAYEK (Friedrich August), *Droit, législation et liberté*, t. II : Le Mirage de la justice sociale, 1976, trad. Raoul Audouin, éd. PUF, coll. Quadrige, 1981, p. 130-131.
[1789] BARREAU (Catherine), « La régulation des smart contracts et les smart contracts des régulateurs », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 76.
[1790] LEGEAIS (Dominique), « Blockchain », *JCl. Sociétés Traité*, fasc. 2160, n° 17 ; POULLET (Yves), JACQUEMIN (Hervé), « Blockchain : une révolution pour le droit ? », art. cit., *loc. cit*.
[1791] DE CHARENTENAY (Simon), art. cit.

besoins des parties que de la réglementation protectrice dont il est difficile de se détacher. C'est en cela qu'il pourrait se révéler intéressant de permettre à la technologie de s'autogérer à l'occasion de litiges mettant en cause ses utilisateurs, tout en laissant la possibilité technique au juge de se substituer au protocole, à tout moment, afin de permettre aux usagers de faire valoir leurs droits. Il s'agirait notamment de permettre aux parties en difficulté qui, par erreur, omission ou ignorance, n'auraient pas prévu de recourir à un juge décentralisé, de pouvoir saisir le juge étatique. Plus encore, les stipulations contractuelles n'excluent en principe pas la mise en œuvre des solutions issues du droit commun des contrats. Il pourrait ainsi être question de mettre en place une option proposant, d'une part, l'exécution du protocole de résolution des litiges et, d'autre part, la prise en charge de la sécurité juridique par le juge sous la forme d'un arbitrage juridictionnel. Ce choix pourrait, par exemple, s'exercer à la suite d'une carence de la gestion décentralisée d'un litige, ou encore en cas de recours contre une décision rendue de manière décentralisée.

Finalement, ces deux outils de sécurité, l'un technique, l'autre juridique, ont tendance à s'affronter pour des raisons essentiellement idéologiques, tandis qu'une collaboration serait beaucoup plus bénéfique à chacun. Si toutefois elle a lieu, l'efficacité de l'intervention du juge étatique conduira à prendre deux éléments en considération, à savoir la possibilité technique à la fois d'intervenir sur la chaîne et d'accéder à son contenu.

246. Les conditions de l'intervention du juge étatique sur la *blockchain*. Le juge est le symbole de la justice et de la sécurité juridique. En principe, son intervention ne devrait être soumise à aucune condition. Mais, force est de constater qu'il résulte des spécificités de la technologie qu'il n'est pas tant question de la légitimité de son intervention, mais bien davantage celle de savoir s'il a la possibilité technique d'agir. Cette solution de la collaboration, laquelle fait s'associer deux paramètres *a priori* incompatibles, est en effet principalement dominée par le caractère décentralisé et par conséquent immuable de la technologie. La *blockchain* rend naturellement difficile, si ce n'est impossible, toute tentative de gestion par une entité centrale. Il importe dès lors d'examiner les éléments qui conduiraient à solliciter, plus qu'une coopération, mais une adaptation de ces deux paramètres l'un à l'autre.

D'une part, il s'agit pour la technologie d'intégrer un mécanisme de prise en compte des décisions juridictionnelles classiques rendues en dehors de la chaîne, au même titre qu'elle admet les décisions des arbitres décentralisés. Autrement dit, le juge doit être

en mesure de mettre en œuvre sa décision à distance. Dans un rapport, l'organisme de Facilitation des Procédures Commerciales et le Commerce Électronique des Nations unies (UN/CEFACT) suggère que les tribunaux soient en mesure d'exiger des parties l'inscription d'une nouvelle transaction ayant pour effet de modifier la première afin de prendre en compte la solution donnée par le juge[1792]. Dans l'intérêt supérieur des utilisateurs, pour la protection des justiciables et le bon fonctionnement de la justice, il est essentiel de parvenir à une alliance entre les mécanismes de règlement des conflits quels qu'ils soient – internes ou ajoutés – de la technologie, et les juges, ce qui supposera une première adaptation de la technologie à la pratique du droit.

D'autre part, il s'agit pour le juge de se conformer à certaines pratiques de la technologie afin d'accéder à son contenu et de remplir son office. Intimement lié au principe de l'autonomie de la volonté, en application des dispositions des art. 1188 et s. du C. civ., l'interprétation d'un contrat doit respecter « la commune intention des parties plutôt [que s'arrêter] au sens littéral de ses termes ». Ainsi, les parties ne sont-elles liées que pour les obligations qu'elles ont subjectivement voulues[1793]. Par conséquent, dès lors qu'un litige apparaît, le juge ne peut se substituer aux parties mais, dans un objectif général de bonne administration de la justice, il doit s'assurer de leur commune volonté, ce à quoi chacune d'elle était précisément tenue en vertu du contrat[1794] selon leur intérêt commun[1795]. Souvent utilisé comme outil d'immixtion du juge dans le contrat[1796], le principe de bonne foi tel que consacré à l'art. 1104 du C. civ. permet de déterminer l'esprit du contrat[1797]. Bénéficiant d'un pouvoir d'appréciation en la matière[1798], le juge attache une grande importance au contrôle de la conformité de l'exécution du contrat aux volontés originelles des parties. Bien qu'il ne soit pas toujours aisé de s'en assurer, il devra pour cela être en mesure d'analyser la volonté des parties inscrite dans des lignes de code[1799]. Eu égard aux spécificités de la technologie, les parties pourraient faciliter l'office du juge

---

[1792] White Paper No. ECE/TRADE/457 UN Economic Commission for Europe, Blockchain in Trade Facilitation (revised version), submitted by the UN/CEFACT Bureau, UNECE [online], Sept. 2020, p. 36, https://unece.org/DAM/trade/Publications/ECE-TRADE-457E_WPBlockchainTF.pdf.

[1793] BENABENT (Alain), *Droit des obligations*, éd. LGDJ, 18e édition, coll. Précis Domat, Privé, 2019, p. 229.

[1794] *Ibid.*, p. 230.

[1795] CA Paris, 4e ch., 12 févr. 2003, *Comm. com. électr*. 2003, comm. n° 57, note Caron C.

[1796] V. par exemple, CA Paris, 21 mai 1999, *JCP* 2000. I. 272, n° 8 (les juges ont interprété la clause d'un contrat de cautionnement bancaire à la lumière des anciens art. 1134, al. 3, et 1135). – V. également, BENABENT (Alain), « La bonne foi dans l'exécution du contrat », *in Travaux de l'Association Henri Capitant. La bonne foi*, (Journées. Louisianaises 1992), t. XLIII, éd. Litec, 1994, p. 294.

[1797] LE TOURNEAU (Philippe), POUMARÈDE (Matthieu), « La bonne foi dans l'exécution du contrat », *Rép. civ. Dalloz*, v° Bonne foi, 2019, n°s 66-67.

[1798] Si le juge s'en écarte, sa décision n'en sera pas forcément cassée. V. en ce sens, Cass. Civ. 1ère, 19 déc. 1995, *Bull. civ.*, I, n° 466.

[1799] BARBRY (Éric), « Smart contracts... Aspects juridiques ! », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 78.

en anticipant dans le contrat originel des règles d'interprétation, sinon en concluant un avenant de contrat constituant un « avenant interprétatif », et ce dès lors qu'elles prennent conscience du caractère limité du support choisi pour inscrire leurs volontés[1800]. Seulement, qu'il s'agisse de contrats traditionnels ou de *smart contracts*, il s'avère que les parties n'envisagent pas systématiquement les situations pouvant intervenir pendant, voire après, l'exécution de leur contrat. Ainsi que le souligne Alain Bénabent, personne n'a la capacité réelle de tout prévoir, que ce soient les contractants ou même le législateur[1801]. L'enjeu réside donc dans l'appréciation de la jurisprudence, remplissant ainsi une mission fondamentale consistant en la résolution de situations exceptionnelles ou intermédiaires, y compris imprévues[1802]. En pratique, le juge devra d'abord se référer à ce que les parties auraient elles-mêmes voulu – recherche *in concreto* –, y compris au sein du code informatique. Ce n'est qu'à défaut qu'il pourra rechercher ce qu'aurait raisonnablement voulu toute autre personne placée dans la même situation – recherche *in abstracto* – (C. civ., art. 1188)[1803].

247. Finalement, toute innovation, et davantage celle qui prétend renouveler la confiance, a besoin du droit pour se construire et se déployer[1804]. C'est parce que l'action humaine est par nature faillible – que ce soit du point de vue de la programmation ou de la mise en place de juridictions décentralisées – qu'elle sera certainement source de contentieux[1805]. Ces limites, inhérentes à la technologie, résultent principalement des choix actuellement opérés. Par conséquent un déploiement plus tardif reste envisageable, à la condition toutefois d'une adaptation réciproque. Paul Vidal de La Blache ne soulignait-il pas que « l'adaptation équivaut à une économie d'efforts qui, une fois réalisée, assure à chaque être, à moins de frais, l'accomplissement paisible et régulier de ses fonctions »[1806] ? Par ailleurs, au-delà de la problématique des pouvoirs du juge dans la gestion des conflits pouvant survenir sur une *blockchain*, ce sont les difficultés de conciliation entre certains aspects de la technologie et différents pans du droit objectif qui semblent, en l'état, constituer de potentiels obstacles à l'appréhension de l'ensemble des contentieux. Aussi la question n'est-elle plus de savoir si le juge peut imposer son autorité

[1800] BENABENT (Alain), *op. cit.*, p. 231.
[1801] *Id.*
[1802] *Ibid.*, p. 235.
[1803] *Ibid.*, p. 232 ; LE TOURNEAU (Philippe), POUMARÈDE (Matthieu), *op. cit.*, n° 71.
[1804] FÉNÉRON PLISSON (Claire), art. cit., p. 4.
[1805] BARBRY (Éric), art. cit., *loc. cit.*
[1806] VIDAL DE LA BLACHE (Paul), *Principes de géographie humaine*, éd. Librairie Armand Colin, 1922, pp. 106-107.

en la matière puisque, à l'évidence, il s'agit davantage d'une nécessité, mais plutôt d'examiner la façon dont il pourra faire respecter ces règles de droit.

Section 2. Les limites du juge étatique dans l'application des règles de droit

248. Bien que l'intervention du juge ne puisse, semble-t-il, pas être directement bridée par l'organisation P2P du réseau, il apparaît cependant que l'application du droit positif, par le juge, puisse indirectement l'être. Deux conséquences de cette décentralisation, à savoir la complexité de la technologie et sa distributivité, mènent en particulier à interroger le traitement juridictionnel des problèmes de compétence(s) (§ 1), et de la question de la (des) responsabilité(s) décentralisée(s), notamment dans l'hypothèses de défaillances techniques (§ 2).

§ 1. Des problèmes de compétence(s)

249. La question de la compétence est, en réalité, protéiforme. Il peut être question de compétence juridictionnelle d'une manière générale ou, plus précisément, de compétence judiciaire, administrative, territoriale, matérielle, ordinaire, exclusive, partagée, d'appui, d'attribution, particulière, etc. En d'autres termes, la compétence « est un titre juridique qui habilite à exercer un pouvoir »[1807]. Mais pas uniquement, car la compétence est également, dans son acception courante et non au sens juridique, la « capacité que possède une personne de porter un jugement de valeur dans un domaine dont elle a une connaissance approfondie »[1808]. En ce qui concerne l'*officium* du juge, deux caractéristiques prêtent particulièrement à discussion.

D'une part, il s'avère que le juge doit être capable de rechercher la vérité, quels que soient l'endroit et la forme sous laquelle elle se trouve. Or, la *blockchain*, qui est un système relativement complexe à raison de son caractère décentralisé et distribué, ne fait pas *a priori* partie de ses compétences. Ne serait-ce que du point de vue de l'appréciation des preuves précédemment évoqué[1809], ces lacunes sont susceptibles de faire obstacle au respect des règles de procédure et à la correcte application des règles de droit par les

[1807] DEBARD (Thierry), GUINCHARD (Serge), *Lexique des termes juridiques 2020-2021*, éd. Dalloz, 28e édition, août 2020, v° Compétence.
[1808] CNRTL [en ligne], v° Compétence, https://www.cnrtl.fr/lexicographie/competence.
[1809] Sur l'utilisation de la fonction *ledger* de la *blockchain* en justice, *supra* n°s 140 et s.

tribunaux. Ainsi, dans l'intérêt d'une bonne administration de la justice, la formation du corps juridique se révèle nécessaire (A). Il est en effet essentiel que le juge puisse acquérir quelques notions techniques ou, du moins, qu'il soit entouré de juristes et experts qui ont assimilé suffisamment les tenants et aboutissants de la technologie décentralisée pour éclairer son appréciation vis-à-vis de ces amas de codes informatiques.

D'autre part, une autre spécificité de la technologie des blocs a été de rassembler des millions d'utilisateurs et de nœuds à travers le monde. Il reste que, dans ce contexte transfrontalier, les difficultés sont nécessairement démultipliées, ne serait-ce que pour soumettre un contrat à la loi et aux autorités d'un État. Pourtant, cette spécificité ne peut, en pratique, conduire à rendre inapplicables les lois étatiques[1810]. La complexité apparente de la technologie nécessite une adaptation des méthodes, ce qui suscite l'intérêt des organisations internationales et européennes. L'objectif étant de permettre l'application du droit international privé afin de déterminer tant le droit applicable que la compétence juridictionnelle pour chaque transaction, l'appréhension de cette technologie sans frontières est inévitable (B).

A. Compétence technique : la nécessaire formation du corps juridique

250. Innovation et problématique de l'admission en justice. L'histoire du droit de la preuve témoigne des multiples débats précédant l'introduction de nouvelles techniques utilisables dans le cadre d'une procédure spécifique ou au cours d'une audience. D'ailleurs le juge lui-même se montre le plus souvent réfractaire, presque protectionniste, avant d'admettre sur le plan probatoire un procédé inédit. Un jugement a des conséquences et repose sur des principes tels que le juge ne peut se permettre de prendre une décision hâtive. Après l'ordalie, le témoignage, la *fama*, l'aveu, l'empreinte, l'ADN, la balistique, l'expertise, le SMS et la carte de crédit[1811], c'est désormais au tour de la technologie *blockchain* de soulever la problématique de l'admission en justice. Si l'expérience de la *blockchain* et la connaissance des rouages de celle-ci constituent la clé de son introduction en justice, il n'est dès lors guère étonnant qu'une période d'adaptation sera nécessaire pour que la *blockchain* entre définitivement dans les mœurs des tribunaux,

[1810] AUDIT (Mathias), art. cit.
[1811] Pour plus de détails sur le sujet, v. notamment, LEMESLE (Bruno) *et al., La preuve en justice : de l'Antiquité à nos jours*, éd. PUR, 2015.

à l'instar des correspondances[1812], de la filature loyale[1813] ou encore des fichiers contenus sur les clés USB[1814]. Selon un auteur, l'enjeu, non seulement sur le plan probatoire mais également en matière d'action en justice, réside finalement dans la question de l'opposabilité aux tiers[1815]. En effet, alors que la technologie se démocratise progressivement, peu d'individus disposent de connaissances solides en lien avec cette chaîne virtuellement sécurisée et rendue infalsifiable *via* des blocs encastrés les uns dans les autres et à la vue de tous. Aussi, la question se pose-t-elle de savoir si un *smart contract* pourra être opposable à un tiers au contrat et donc si *a fortiori* le juge l'admettra ? Pour répondre à cette question, le juge pourra dans un premier temps compter sur les règles générales de procédure lui permettant de bénéficier de l'expertise d'un professionnel. Mais il lui importera de pouvoir se fier et s'associer à un corps de juristes ayant intégré, dès leur formation, les compétences nécessaires à la manifestation de la vérité.

251. La solution à court terme : l'assistance d'un technicien. D'une manière générale, en vertu des règles procédurales applicables, le juge pourra toujours faire appel à un technicien, avant (CPC, art. 145)[1816] ou pendant tout le cours des débats (CPC, art. 232 et s.), « pour l'éclairer par des constatations, par une consultation ou par une expertise sur une question de fait »[1817]. Bien que la technologie puisse malgré tout paraître très

[1812] Cass. Civ. 1ère, 5 avr. 2012, n° 11-14.177 (« Prive sa décision de base légale, la juridiction qui écarte des débats une lettre missive au motif que la production de celle-ci violerait l'intimité de la vie privée de son rédacteur et le secret des correspondances sans rechercher si cette production n'était pas indispensable à l'exercice du droit à la preuve et proportionnée aux intérêts antinomiques en présence. »).
[1813] Cass. Civ. 1ère, 25 févr. 2016, n° 15-12.403 (« Le droit à la preuve ne peut justifier la production d'éléments portant atteinte à la vie privée qu'à la condition que cette production soit indispensable à l'exercice de ce droit et que l'atteinte soit proportionnée au but poursuivi. Viole, dès lors, les articles 6 et 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, 9 du code civil et 9 du code de procédure civile une cour d'appel qui, pour rejeter la demande tendant à voir écarter des débats des rapports d'enquête privée produits par un assureur à l'occasion de l'instance en indemnisation du préjudice subi par la victime d'un accident, retient que ces rapports ne portent pas une atteinte disproportionnée au respect dû à la vie privée de cette dernière, tout en relevant que les investigations, qui s'étaient déroulées sur plusieurs années, avaient eu une durée allant de quelques jours à près de deux mois et avaient consisté en des vérifications administratives, un recueil d'informations auprès de nombreux tiers, ainsi qu'en la mise en place d'opérations de filature et de surveillance à proximité du domicile de l'intéressé et lors de ses déplacements, ce dont il résultait que, par leur durée et leur ampleur, les enquêtes litigieuses, considérées dans leur ensemble, portaient une atteinte disproportionnée au droit au respect de sa vie privée. »).
[1814] VOIRON (Émile), « Le contrôle des clés USB appartenant aux salariés hors de leur présence est une preuve recevable », *Harmonia Juris Avocats* [en ligne], 14 mai 2014, https://www.harmoniajuris.com/controle-cles-usb-appartenant-aux-salaries-presence-preuve-recevable/.
[1815] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 13.
[1816] CPC, art. 145 : « S'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé. »
[1817] CPC, art. 232.

complexe pour celui dont ce n'est pas la spécialité[1818], et bien qu'*a fortiori*, le travail de recherche résultant des potentielles difficultés d'interprétation et/ou de traduction des algorithmes puisse se révéler lourd, et le contentieux complexe, l'éluder ne serait que plus problématique[1819]. Pour éviter que le procédé n'évolue dans le sens de cette « complexité » accrue et que son potentiel ne soit atrophié à son insu, il est indispensable que le juge soit au plus vite entouré de personnes compétentes en la matière. Le juge, en sa qualité de juriste, a forcément besoin d'avoir un appui technique dans le domaine des autres spécialités. C'est cet appui qui pourra lui apporter les réponses dont il a besoin pour mener à bien sa propre mission et faire appliquer la règle de droit. En définitive, le droit doit s'assurer la collaboration étroite et régulière d'informaticiens et experts en *blockchain*. C'est dans cette idée d'intégrer l'usage de la preuve par *blockchain* tant dans la vie des affaires que devant les tribunaux et de casser les derniers obstacles psychologiques naturellement réfractaires vis-à-vis de la *blockchain*, que la *start-up* BlockchainyourIp a mis l'accent sur la collaboration entre les métiers du droit et de l'informatique en travaillant directement avec un huissier de justice[1820].

252. La solution à long terme : de la collaboration à la pluridisciplinarité. Quand bien même les experts seraient sans nul doute d'un grand secours pour les juges qui accepteraient de laisser une chance à la *blockchain*, il est clair que l'évolution se fera dans le sens de la pluridisciplinarité. Il est alors acceptable de considérer qu'il appartiendra par la suite à l'ensemble du milieu juridique, y compris éventuellement le juge, de se munir de certaines connaissances dans le domaine. Tout avocat, huissier ou juriste, spécialisé dans les nouvelles technologies, pourrait être mené à devoir interpréter ou contester l'interprétation faite d'un contrat *blockchain*, confirmer ou infirmer la teneur d'un algorithme et de ses lignes de code, ou produire la preuve technique à l'appui de ses prétentions et ce, afin que le juge puisse nourrir sa propre réflexion. Grâce au travail effectué en amont, le juge devrait être capable de s'assurer que les instructions codées sont, d'une part, en adéquation avec la volonté des parties et, d'autre part, conformes aux

[1818] DE COETLOGON (Perrine) (dir.), « Réunion d'information #GTnum #Blockchain4E », Villeneuve d'Ascq (Laboratoire Cristal, M3, Cité scientifique), 26 juin 2018, non publié. – RODA (Jean-Christophe), art. cit., n° 19.
[1819] RODA (Jean-Christophe), art. cit., *loc. cit*.
[1820] *Supra* n° 145. – V. également, FAUCHOUX (William), « La startup qui voulait révolutionner la preuve des créations et des innovations », *BlockchainyourIp* [en ligne], 9 oct. 2017, https://blockchainyourip.com/startup-voulait-revolutionner-preuve-creations-innovations/ ; « BlockchainyourIp veut révolutionner la preuve des créations et des innovations », *Le monde du Droit* [en ligne], 16 oct. 2017, https://www.lemondedudroit.fr/on-en-parle/54042-blockchainyourip-la-startup-qui-voulait-r%C3%A9volutionner-la-preuve-des-cr%C3%A9ations-et-des-innovations.html.

règles de droit[1821]. Dans une dynamique de renouvellement des compétences, le « juriste codeur » ou « augmenté » pourrait ainsi succéder au juriste traditionnel[1822]. Il aurait dès lors un rôle actif dans la traduction des lignes de langage informatique en langage naturel. Seulement, en l'état actuel, tous les juristes quels qu'ils soient ne sont pas des « spécialistes dans le droit des technologies avancées »[1823]. L'enjeu réside donc dans la formation. En pratique, les juristes peuvent choisir « l'auto-formation » *via* les forums, ou opter pour une offre plus structurée proposée par les diverses associations et entreprises spécialisées[1824]. À l'instar de la nécessité de construire l'ossature du *smart contract* avant qu'il ne soit intégré à un bloc de la chaîne, comprendre le développement et la phase d'écriture du code informatique régissant toute *blockchain* sera primordial, mais pas suffisant. Pour que l'ensemble du système *blockchain* puisse se développer, il apparaît essentiel que cette formation soit appréhendée sur le long terme et organisée de manière à intégrer un ordre de priorité. L'attention devrait effectivement, dans un premier temps, être portée vers les métiers de l'informatique afin d'assurer, dès la conception des algorithmes, l'intégration de règles de sécurité conformes au droit. Il semble ensuite essentiel de fournir les éléments de compréhension et de réflexion aux organes de conseil et de représentation tels que les avocats et éventuellement les juristes d'entreprise. En parallèle, les formations juridiques spécialisées, à l'instar des cursus universitaires « droit des nouvelles technologies », sont vivement suggérées, d'autant plus qu'elles présentent un intérêt tant pour les entreprises que pour le règlement des contentieux en la matière. La nouvelle génération de juristes pourra ainsi progressivement compléter le corps juridique déjà formé. Enfin, la mise en œuvre de cette formation devra aboutir à armer la magistrature des outils nécessaires pour appréhender les situations soumises à son jugement.

253. L'essor de la technologie *blockchain* ne réside pas dans la désintermédiation, mais plutôt dans la ré-intermédiation[1825]. En d'autres termes, l'enjeu se trouve dans le renouvellement des métiers, tant juridiques qu'informatiques. Plus encore, la technologie nécessite un mélange des connaissances et, probablement à terme, une pluridisciplinarité importante. En effet, de nouvelles compétences devront être développées afin de dépasser

[1821] GUILHAUDIS (Élise), art. cit., p. 13.
[1822] GUICHETEAU (Carine), « Cap sur le juriste "augmenté" et stratège au cœur du business », *Affiches Parisiennes* [en ligne], 28 août 2017, https://www.affiches-parisiennes.com/cap-sur-le-juriste-augmente-et-strategе-au-coeur-du-business-7363.html.
[1823] *Id.*
[1824] LORRE (Pierre-Marie), art. cit., p. 47.
[1825] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., n° 19.

les frontières de la complexité technologique et de la maîtrise du droit[1826]. Il s'agira d'acquérir les connaissances suffisantes non seulement pour contrôler et auditer les codes[1827], mais également pour être capable d'anticiper les relations entre le justiciable, l'outil technologique et la justice.

Mais, la compétence n'est pas qu'une question de capacité et de connaissances approfondies[1828] puisque, du point de vue juridique, la compétence « est un titre […] qui habilite à exercer un pouvoir »[1829]. Or, lorsque le droit objectif se trouve confronté à un objet juridique sans frontières, la mise en œuvre des règles de droit international privé permet de déterminer tant le droit applicable que la compétence juridictionnelle pour chaque transaction. Il convient donc désormais d'en analyser l'application.

B. Compétence internationale : l'inévitable appréhension d'une technologie sans frontières

254. Entre vide juridique et imprécisions, l'application du droit international privé confronté au caractère décentralisé de la *blockchain*. Selon certains auteurs, l'origine des difficultés d'application du droit objectif réside dans la jeunesse de son développement[1830]. Il n'empêche que le contexte transfrontalier du cyberespace peut, en pratique, se révéler problématique[1831]. La chaîne de blocs interroge effectivement en matière de compétence internationale, tantôt vis-à-vis du droit applicable, tantôt à l'égard du juge compétent. Si aucun régime juridique propre à la *blockchain* ne se charge de répondre à ces questions, aucun vide juridique n'existe pour autant. En effet, étant donné que « la nature a horreur du vide »[1832], qu'il s'agisse de réparer le dommage subi par un utilisateur de nationalité française du fait de l'inexécution d'un contrat conclu avec un utilisateur de nationalité étrangère, de sanctionner la tentative de falsification d'un bloc par un nœud, ou, d'une manière générale, de rechercher le système juridique applicable et l'autorité compétente, le droit trouve à s'appliquer en toute circonstance[1833]. Plus exactement, tout conflit, de loi ou de juridiction, se résout à travers les règles de droit international privé ou, selon le cas, de droit européen[1834]. Ainsi, à partir du moment où la

[1826] BERBAIN (Côme), art. cit., p. 5.
[1827] LORRE (Pierre-Marie), art. cit., p. 47.
[1828] CNRTL [en ligne], v° Compétence, https://www.cnrtl.fr/lexicographie/competence.
[1829] DEBARD (Thierry), GUINCHARD (Serge), *Lexique des termes juridiques 2020-2021*, éd. Dalloz, 28e édition, août 2020, v° Compétence.
[1830] GUERLIN (Gaëtan), art. cit., *loc. cit*.
[1831] *Id.* – V. également, ZOLINSKY (Célia), « Fintech - Blockchain et smart contracts : premiers regards sur une technologie disruptive », *RD bancaire et fin.* 2017, dossier 4, n° 8 ; AUDIT (Mathias), art. cit.
[1832] Aristote.
[1833] FÉNÉRON PLISSON (Claire), art. cit., p. 22.
[1834] GUILHAUDIS (Élise), art. cit., p. 8.

blockchain prend la forme d'un réseau distribué et décentralisé, laissant intervenir des utilisateurs, participants, et mineurs n'étant pas localisés uniquement en France, cette situation forme l'élément d'extranéité essentiel menant à la transposition des règles de conflit et de l'approche de Savigny[1835]. Simplement, il apparaît que les principes traditionnels du droit international privé souffrent d'une « applicabilité limitée » par le caractère décentralisé de la technologie[1836]. L'auteur constate notamment que les différents lieux pouvant permettre de déterminer le système juridique applicable ainsi que la juridiction compétente pour statuer, à savoir le domicile, le lieu d'affaires, ou le lieu d'exécution de la prestation, s'ils ne sont pas renseignés au sein de la transaction inscrite sur la *blockchain*, ne peuvent être localisés et peuvent avoir pour effet de rendre l'analyse délicate. Alors que certains proposent de pallier ce problème en reconnaissant l'existence d'un ordre juridique international spontané dans la technologie, reposant sur des règles spéciales de droit international à l'image de la théorie soutenue notamment par la Commission des Nations unies pour le droit commercial international (CNUDCI) selon laquelle des règles « véritablement internationales car a-nationales » s'avèrent nécessaires, d'autres mettent en exergue les similitudes avec le développement d'Internet pour miser sur une régulation progressive des États qui viendra fixer un cadre sécurisé au déploiement de la technologie[1837]. D'autres encore font état d'une extrême flexibilité du droit international privé et de ses catégories de rattachements, ce qui suppose d'interroger le processus de qualification des problèmes juridiques rencontrés sur les *blockchains*[1838].

À l'origine de ces multiples complexités, l'utilisation des *blockchains* n'exclut pas la mise en œuvre des règles issues du droit international privé, à condition de procéder à certains ajustements. Il n'est dès lors guère étonnant que les organisations internationales et européennes se soient saisies de la question.

[1835] Il s'agit de Friedrich Carl von Savigny. – V., VIGNAL (Thierry), *Droit international privé*, éd. Sirey, 2017, n° 40.

[1836] GILLIOZ (Fabien), « Du contrat intelligent au contrat juridique intelligent », *D. IP/IT* 2019, n° 1, pp. 16 et s. V. également, JAULT-SESEKE (Fabienne), « La blockchain au prisme du droit international privé, quelques remarques », *D. IP/IT* 2018, n° 10, p. 544.

[1837] *Id*. – V., par exemple, le projet de loi monégasque n° 995 du 12 juin 2019 actuellement en étude auprès de la Commission pour le Développement Numérique du Conseil National de Monaco [Projet de loi n° 995, 12 juin 2019, relative à la technologie Blockchain], dont l'art. 5 propose l'application du droit monégasque « aux *blockchains* (chaînes de blocs), aux *smart contracts* (contrats intelligents), aux entreprises processus algorithmiques et aux monnaies cryptographiques qui produisent des effets sur le territoire de la Principauté de Monaco », précisant que « l'effet est réputé se produire sur le territoire de la Principauté de Monaco dès lors qu'un de ses faits constitutifs ou une de ses conséquences a eu lieu sur ce territoire ». Pour une critique de cette proposition, v. notamment, AUDIT (Mathias), art. cit.

[1838] JAULT-SESEKE (Fabienne), art. cit., *loc. cit.*

255. Une intervention progressive des organismes internationaux. La communauté internationale tend en effet à se saisir du sujet et intervient, pour cela, de manière ponctuelle, en particulier dans le domaine commercial[1839].

Point de départ de multiples mouvements en matière de commerce international, les rapports respectifs du G20[1840] et de l'ONU[1841] ont mis en évidence que, pour que l'essor de la technologie coïncide avec une sécurité juridique accrue, il est essentiel qu'une coopération mondiale interdisciplinaire soit mise en place. C'est avec cet objectif que sont intervenues les commissions onusiennes, à l'instar de la Commission des Nations Unies pour le Droit du Commerce International (CNUDCI) qui a justement pour mission de moderniser le droit commercial international grâce à de nouveaux outils technologiques capables de soutenir le commerce transfrontalier[1842]. S'en est suivi un important travail de rédaction de textes à portée internationale en lien avec la technologie des *blockchains*. Ont ainsi vu le jour la Convention des Nations unies sur l'utilisation des communications électroniques dans les contrats internationaux[1843], la Convention sur le contrat de transport international de marchandises effectué entièrement ou partiellement par mer[1844] ou encore la loi-type (CNUDCI) sur les sûretés mobilières[1845]. En parallèle, la Commission économique pour l'Europe des Nations unies (UNECE) a, au même titre que la CNUDCI, procédé à des analyses d'impact afin de déterminer la manière dont « l'outil *blockchain* » pourrait être utilisé pour faciliter le commerce et les processus commerciaux connexes[1846]. En soulignant les spécificités de la technologie et leur impact

[1839] DEVILLIER (Nathalie), « Jouer dans le "bac à sable réglementaire" pour réguler l'innovation disruptive : le cas de la technologie de la chaîne de bloc », *RTD com*. 2017, p. 1037.

[1840] Pour plus de précisions sur le sujet, v. notamment, G20 Financial Inclusion Action Plan, « G20 Principles for Innovative Financial Inclusion - Executive Brief », GPFI [en ligne], 2010, http://www.gpfi.org/sites/default/files/documents/G20%20Principles%20for%20Innovative%20Financial%20Inclusion%20%20AFI%20brochure.pdf. ; ALOIS (JD), « Financial Stability Board issues report on FinTech: "Regulators need to understand the impact" », *Crowdfund Insider* [online], 28 Jun. 2017, https://www.crowdfundinsider.com/2017/06/112078-financial-stability-board-issues-report-fintech regulators-need-understand-impact/.

[1841] ITU-T - Study Group 17, « Proposal for a new question on security aspects for distributed ledgers technologies », Genève, 29 Aug.-6 Sept. 2017, cité dans : DEVILLIER (Nathalie), art. cit., p. 1037.

[1842] UNCITRAL, « 50e session Programme for the Congress Modernizing International Trade Law to support innovation and sustainable development », Austria : Vienna International Center [online], 4-6 Jul., 2017, http://www.uncitral.org/pdf/french/congress/CALL_FOR_PAPERS_CONGRESS_Final-FR.pdf.

[1843] Conv. New York, 23 nov. 2005, sur l'utilisation des communications électroniques dans les contrats internationaux.

[1844] Conv. New York, 16-27 avr. 2007, sur le contrat de transport international de marchandises effectué entièrement ou partiellement par mer (« Règles de Rotterdam »).

[1845] L. type Vienne n° A/CN.9/WG de la CNUDCI, 2017, sur les sûretés mobilières. – Pour une liste exhaustive des textes en la matière, v. notamment, DEVILLIER (Nathalie), art. cit., p. 1037.

[1846] HIGGINS (Stan), « A UN agency is exploring blockchain's impact on trade », *Coin Desk* [online], 3 May 2017, www.coindesk.com/un-agency-seeks-experts-to-help-craft-blockchain-white-papers/ ; White Paper No. ECE/TRADE/C/CEFACT/2019/8 UN Economic Commission for Europe, 17 Jan. 2019, on the technical applications of Blockchain to United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) deliverables, submitted by the UN/CEFACT Bureau to the twenty-fifth session of the Plenary for noting [online], https://unece.org/DAM/cefact/cf_plenary/2019_plenary/

sur son interopérabilité avec les processus existants, l'UNECE constate l'importance d'une harmonisation des cadres juridiques et de l'élaboration de normes minimales de certification ou de conformité[1847]. D'après elle, l'organisme de Facilitation des Procédures Commerciales et le Commerce Électronique des Nations unies (UN/CEFACT) devra fournir des recommandations, et éventuellement des normes et des instruments propres à faciliter cette uniformisation[1848]. Dans un rapport rédigé sous la direction du Vice-président de l'UN/CEFACT, Virginia Cram Martos souligne que dès lors qu'un *smart contract* remplace un contrat *fiat* existant, il sera, dans la majorité des cas, régi par les mêmes principes juridiques que le contrat *fiat* initial, y compris concernant la question des identités des contractants[1849]. Ainsi, si le *smart contract* correspond à une transaction commerciale, en principe toutes les parties sont connues et par conséquent, quand bien même elles ne dépendraient pas du même système juridique, les principes de droit commercial international seraient pleinement efficaces pour établir la juridiction et la loi compétentes[1850]. D'ailleurs, l'auteure précise que ce n'est qu'en cas de complet silence sur leur identité, que les parties connaîtront des difficultés pour transposer les règles de conflit existantes[1851]. En dehors de cette hypothèse, y compris si le contrat n'existe que sous forme informatique, le *smart contract* devrait être assimilé à un contrat écrit[1852].

Dans le secteur de l'entreprenariat, un comité exclusivement consacré à l'étude de la chaîne de blocs a été institué. Il s'agit du comité technique *ISO/TC 307* « *Blockchain and electronic distributed ledger technologies* »[1853]. Partant du constat que l'existence de plusieurs incohérences entre l'organisation des *blockchains* et le droit objectif peut décourager le marché économique et ainsi nuire au déploiement de la technologie, le comité entend élaborer des normes[1854]. En mettant en place un cadre standard de règles, incluant à la fois des règles génériques et des règles pluridisciplinaires, il espère promouvoir la confiance dans la technologie et permettre aux acteurs économiques de tirer parti de ses multiples avantages, en particulier en matière de sécurisation des

ECE_TRADE_C_CEFACT_2019_08E.pdf ; White Paper No. ECE/TRADE/457 UN Economic Commission for Europe, Sept. 2020, Blockchain in Trade Facilitation (revised version) [en ligne], https://unece.org/DAM/cefact/cf_plenary/2019_plenary/ECE_TRADE_C_CEFACT_2019_08E.pdf.

[1847] White Paper No. ECE/TRADE/C/CEFACT/2019/8 UN Economic Commission for Europe, préc., p. 13.

[1848] *Id.*

[1849] White Paper No. ECE/TRADE/457UN Economic Commission for Europe, préc., p. 36.

[1850] *Id.*

[1851] *Ibid.*, p. 37.

[1852] *Id.*

[1853] V. le site internet officiel, https://www.iso.org/committee/6266604.html.

[1854] PEYRAT (Olivier), LEGENDRE (Jean-François), « Pourquoi la normalisation s'intéresse-t-elle à la blockchain ? », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 97.

investissements[1855]. Un auteur indique d'ailleurs que cette initiative constitue pour nombre de gérants de *start-ups*, notamment français, l'opportunité non seulement de rendre acceptable l'utilisation de la *blockchain*, mais également d'accompagner, et peut-être accélérer, la mutation numérique[1856].

256. La solution de l'anticipation *via* le contrat. Si les normes internationales sont susceptibles de faciliter l'intervention du juge et l'application des règles de droit[1857], rien n'empêche les parties d'éluder la question en déterminant préalablement l'ordre juridique et la compétence juridictionnelle dans le *smart contract*[1858] ou, d'une manière générale, dans l'opération inscrite sur la chaîne[1859]. En effet, bien qu'en toute hypothèse les règles de droit international privé pourront, en principe, toujours s'appliquer[1860], la seule condition étant de trouver « un point d'ancrage »[1861] permettant de solutionner les éventuels conflits de droit ou de juridiction[1862], le contrat ne constitue-t-il pas l'instrument d'anticipation le plus efficace[1863] ? Cette possibilité est d'ailleurs consacrée par l'art. 3 du Règl. (CE) n° 593/2008, dit « Rome I »[1864]. En intégrant par exemple au contrat une clause attributive de juridiction (d'élection du for) ainsi qu'une clause sur la loi applicable[1865], le problème pourrait être contourné. Virginia Cram Martos encourage également tout acte visant à anticiper ces questions, et promeut plus particulièrement le recours à l'arbitrage institutionnel par l'insertion dans le contrat, ou dans un document auquel il est fait référence dans la convention principale (CPC, art. 1443), d'une clause compromissoire (C. civ., art. 2059 et s.)[1866]. L'apport de cette clause peut d'ailleurs être évalué à la lumière de l'avantage procuré par l'obtention d'une sentence arbitrale. En

[1855] *Id.*
[1856] *Id*.
[1857] DEVILLIER (Nathalie), art. cit., p. 1037.
[1858] MACLEAN (Fiona), « Governing the Blockchain: How to Determine Applicable Law », *Butterworths Journal of International Banking and Financial Law*, Jun. 2017, No. 6, pp. 359 et s. ; GUILLAUME (Florence), « Blockchain : le pont du droit international privé entre l'espace numérique et l'espace physique », *in* PRETELLI (Ilaria) (dir.), *Conflict of Laws in the Maze of Digital Platforms. Le droit international privé dans le labyrinthe des plateformes digitales. Actes de la 30e Journée de droit international privé du 28 juin 2018 à Lausanne*, éd. Schulthess Éditions Romandes, 2018, pp. 164-188, notamment p. 174.
[1859] COIFFARD (Didier), art. cit., n° 147.
[1860] Sur l'importance du rôle du juge malgré le principe « *code is law* », *supra* n[os] 139 et s. – V. également, JAULT-SESEKE (Fabienne), art. cit.
[1861] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., n° 28.
[1862] COIFFARD (Didier), art. cit., *loc. cit.*
[1863] « Contracter c'est prévoir. Le contrat est une emprise sur l'avenir », RIPERT (Georges), *La règle morale dans les obligations civiles*, éd. LGDJ, 4[e] édition, 1949, n° 84.
[1864] Règl. (CE) n° 593/2008 du Parlement européen et du Conseil, 17 juin 2008, sur la loi applicable aux obligations contractuelles (Rome I), *JOUE* L 177/6, 4 juill. 2008.
[1865] LE TOURNEAU (Philippe), *Contrats du numérique*, éd. Dalloz, coll. Dalloz Référence, 2021-2022, pp. 166 et s., n[os] 116.141 - 116.151.
[1866] White Paper No. ECE/TRADE/457UN Economic Commission for Europe, préc., *loc. cit.*

effet, un auteur constate qu'au contraire de l'exécution des décisions de justice, la solution rendue par un arbitre bénéficie de la Convention sur la reconnaissance et l'exécution des sentences arbitrales étrangères de 1958[1867], laquelle a pour vocation de faciliter le règlement des différends à caractère international en donnant plein effet aux conventions d'arbitrage[1868] et en facilitant la reconnaissance et l'exécution de sentences arbitrales étrangères dans les États contractants[1869]. Selon certains, et en particulier Vitalik Buterin[1870], une telle clause serait également susceptible de contourner les réserves de l'ordre public ou d'éventuelles lois de police[1871]. Solution rapide et moins onéreuse, l'anticipation contractuelle pourrait d'ailleurs se programmer informatiquement par le biais d'une fonction d'activation directement insérée dans le contrat ou dans le *smart contract* inscrit sur la chaîne[1872]. De cette façon, le recours à l'arbitrage semble pouvoir intervenir quand bien même les parties n'auraient pas précisé leurs identités dans le contrat principal. Finalement, force est de reconnaître que « la souplesse des règles du droit international privé devrait lui permettre de s'adapter au modèle de la *blockchain*, alors même qu'il est vain de chercher à la localiser »[1873].

257. Il n'empêche que, comme le souligne Claire Fénéron-Plisson, « la liberté donne des ailes mais les *start-ups* demandent à être sécurisées », notamment en ce qui concerne l'étendue de leur responsabilité ou, au contraire, de leur droit à réparation, dans le cas où elles mettraient en œuvre ou accueilleraient des solutions informatiques basées sur la technologie *blockchain*[1874]. Il est donc essentiel de parvenir à dresser un état des lieux susceptible de préciser les contours de cette notion de responsabilité(s) décentralisée(s).

§ 2. Une question de responsabilité(s) décentralisée(s)

258. La décentralisation de la *blockchain*, qui lui permet, en outre, de constituer un réseau de pair à pair mondial inédit, est également à l'origine de difficultés tendant à

[1867] Conv. New York, 10 juin 1958, sur la reconnaissance et l'exécution des sentences arbitrales étrangères.
[1868] *Ibid*., art. II, 3.
[1869] *Ibid*., art. III - VII. – La Convention compte en l'état actuel 156 États contractants. – V. également sur le sujet, GILLIOZ (Fabien), art. cit.
[1870] BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », *github* [liens de publication originaux supprimés] [online], Nov. 2013, https://github.com/ethereum/wiki/wiki/White-Paper. Trad. : Asseth (Stéphane Roche, Jean Zundel, Frédéric Jacquot, Alexandre Kurth et Etienne Jouin), v., http://www.asseth.fr/2016/11/09/traduction-whitepaper-ethereum/.
[1871] JAULT-SESEKE (Fabienne), art. cit.
[1872] GILLIOZ (Fabien), art. cit.
[1873] JAULT-SESEKE (Fabienne), art. cit.
[1874] FÉNÉRON PLISSON (Claire), art. cit., p. 21.

perturber le travail du juge étatique. En dehors de sa recherche de la vérité et de la détermination de son champ de compétence, c'est la problématique de la responsabilité des utilisateurs, mineurs et participants, et en particulier de ses développeurs, qui vient indubitablement se poser au juge en cas de dysfonctionnement. En effet, toute innovation comporte des risques. L'environnement volontairement décentralisé où règne parfois le pseudonymat complique nécessairement la qualification de ces risques et interroge l'application juridictionnelle des régimes de responsabilité correspondants. Décentralisé ou non, agissant au titre d'une clause compromissoire ou non, le juge doit intervenir. Seulement, en matière de *blockchain*, à raison d'une confiance sans réserve attribuée dès la naissance du protocole et de barrières résultant du pseudonymat souvent pratiqué (A), la recherche et la mise en œuvre de la responsabilité par le juge en cas de dysfonctionnement s'avèrent entravées (B).

A. Confiance initiale et barrières de la pseudonymisation

259. Un excès de confiance dans l'agent développeur ? Si l'environnement d'une *blockchain* contribue à remplacer ce besoin de confiance traditionnel entre les Hommes, le rendant de surcroît inutile tant entre les utilisateurs que vis-à-vis des mineurs, il implique toutefois de se fier, quasi aveuglément, au développeur. En effet, alors qu'à ses débuts elle ne rassemblait qu'à une communauté constituée d'une élite informatique capable de comprendre et de jongler avec les complexités de la technologie, sa démocratisation a progressivement rempli les rangs des utilisateurs d'individus qui n'ont, à l'heure actuelle, pas ou peu de connaissances en informatique ou en mathématiques. Par conséquent, ces individus utilisent la chaîne sans connaître son fonctionnement. Non dans l'idée d'étudier ou de vérifier ce que ses lignes de codes informatiques contiennent, bien souvent, ces nouveaux utilisateurs ne rejoignent l'écosystème que pour les multiples bénéfices que la technologie est susceptible de leur procurer. L'honnêteté de l'agent-développeur est alors présumée. Seulement, il ne s'agirait ici que d'une présomption simple, susceptible d'être renversée par toute preuve contraire.

260. Le dysfonctionnement reste humain. Bien avant que Prométhée ne dérobe le feu sacré aux dieux de l'Olympe pour l'offrir aux humains, l'Homme n'avait de cesse de créer. De toutes les innovations développées au fil des siècles, l'Homme en a toujours été à l'origine. Seulement, toute construction intègre tant les qualités que les défauts de son

créateur[1875]. Un programme informatique est le fruit d'une interprétation – celle du programmeur qui attribue un sens à une réalité pour ensuite la traduire en lignes de code dans un langage spécifique. Il peut cependant faire des erreurs, omettre des fragments de code ou en programmer plus qu'il n'en faut, si bien que la technologie ne peut garantir l'absence d'un dysfonctionnement. Tout évènement survient conformément aux instructions de l'algorithme. Certaines actions pourraient s'exécuter normalement tandis que d'autres actions ou conséquences, en principe non voulues mais en pratique programmées, pourraient se manifester et ainsi tout pourrait arriver tel que ce « tout » a été mal programmé dès le départ. Plus encore, par la traduction de leur propre interprétation, les développeurs décident autant de la forme que de la direction que prendra le système[1876]. Tel que le soulignait Lawrence Lessig, « *Code is law* »[1877]. Les « règles du jeu » sont établies, ce qui signifie dès lors que l'orientation du code informatique est prédéterminée et que le code constitue un véritable « acte politique »[1878]. Appréhendée en ce sens, la chaîne de blocs n'est ni neutre, ni objective.

Dans un cas comme un autre, force est de constater que ce type de construction n'est pas à l'abri des difficultés, d'autant plus si le fonctionnement de la technologie utilisée ne permet pas de déterminer efficacement l'identité des intervenants.

261. Le problème de l'identification du responsable au sein d'un système décentralisé. Pratique courante des *blockchains*, la pseudonymisation constitue un champ d'investigation juridique important à raison des multiples incertitudes qu'elle engendre[1879]. Il est parfois possible de parvenir à identifier un utilisateur, notamment en procédant à une authentification par le biais de l'identité civile déclarée par le détenteur d'un compte, d'un croisement d'adresse par topologie du réseau couplée avec une analyse des transactions inscrites, d'une triangulation d'adresses IP, d'un *wallet* hébergé *via* un site opérant à partir d'un établissement centralisé, tel qu'une banque, ou encore en utilisant les données collectées par des objets connectés et/ou intelligents, ou par des *cookies* dans certaines conditions, ou en obtenant, par l'intermédiaire d'un avocat, une ordonnance du juge autorisant une demande d'identification d'une adresse IP auprès de l'opérateur ou du fournisseur d'accès à Internet[1880]. Il existe donc divers procédés permettant de révéler l'identité d'un utilisateur, néanmoins il apparaît que, d'une manière

[1875] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 18.
[1876] *Id.*
[1877] *Supra* n° 234.
[1878] BARRAUD (Boris), « Les blockchains et le droit », art. cit., *loc. cit.*
[1879] BARREAU (Catherine), art. cit., *loc. cit.* – *Supra* n° 107-109.
[1880] Pour plus de précisions sur ces pratiques, supra n°s 114 et s.

générale, il soit plus facile pour les utilisateurs de dissimuler leur identité sur la chaîne. Dans la pratique, les propriétaires de crypto-monnaies sont contraints à une prudence particulière, notamment en termes de sécurité des transactions inscrites. Pour cela, ils s'astreignent à un changement systématique d'adresse « publique » à chaque opération inscrite et, le plus souvent, utilisent le protocole *Tor*, ce qui rend finalement inefficace toute tentative d'identification des acteurs[1881]. Plus encore, un tel fonctionnement constitue quasiment une garantie d'anonymat pour n'importe quel participant d'une *blockchain*, qu'il s'agisse d'un utilisateur, d'un mineur, ou de son ou ses développeurs. Ainsi, l'individu animé « par des desseins idéologiques ou autrement politiques »[1882], se comportant de manière malhonnête, non éthique ou illégale[1883], peut se dissimuler, masqué derrière une suite de chiffres et de lettres garantissant le secret de son identité[1884].

De la difficulté générale d'identifier un participant résulte un nouvel obstacle au déploiement de la technologie, à savoir la paralysie des recours en droit, et en particulier en droit des contrats, mais pas seulement. Après avoir rappelé l'avantage de la distribution lors des débats sur la question de la reconnaissance légale de la *blockchain*, le Parlement français a souligné la nécessité de vérifier que « chaque intervenant possède de manière effective les droits sur les différentes transactions qu'il souhaite effectuer » étant donné que, « lorsque la technologie aura été suffisamment développée et que du contentieux apparaîtra, les questions liées à la responsabilité des parties prenantes, […] ou encore la protection du consommateur se verront opposer un vide juridique »[1885]. Source d'incertitudes, la problématique de l'anonymat occasionnerait dès lors une inutile complication des procédures en matière de régimes de responsabilité. Il en va ainsi par exemple en cas de faille technique ayant perturbé l'inscription d'une ou de plusieurs transactions ou *smart contracts*, de *bug* informatique interne ou externe à la chaîne lors de l'exécution d'un *smart contract*[1886], de fuite de données personnelles ou de crypto-monnaies[1887]. En effet, la nature décentralisée de la *blockchain* contribue à brouiller les recherches du juge visant à déterminer tant l'origine que l'auteur d'un préjudice ou d'une

[1881] Sur les difficultés d'identification de réseaux s'appuyant sur des systèmes de type Tor, v., par exemple, l'étude sur le dossier Black Hand, LAURENT (Xavier), « Retour d'expérience sur le premier démantèlement d'une plateforme francophone du darkweb : le dossier Black Hand », *D. IP/IT* 2021, n° 2, p. 79.
[1882] BARRAUD (Boris), « Les blockchains et le droit », art. cit., *loc. cit.*
[1883] CAHEN (Murielle), « Traitement civil et pénal du bitcoin », *murielle-cahen.fr* [en ligne], 9 déc. 2014, https://www.murielle-cahen.fr/traitement-civil-et-penal-du-bitcoin/ ; ALMASEANU (Stephen), « Le traitement pénal du Bitcoin et des autres monnaies virtuelles », *Gaz. Pal.* 30 août 2014, n° 242, p. 11.
[1884] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., n° 12.
[1885] Question écrite n° 96014, *JOAN* Q, 24 mai 2016, p. 4369.
[1886] D'après le dictionnaire en ligne Larousse, le mot « *bug* » est utilisé pour désigner le « Défaut de conception ou de réalisation d'un programme informatique, qui se manifeste par des anomalies de fonctionnement de l'ordinateur. » [Dictionnaire Larousse [en ligne], v° Bug, https://www.larousse.fr/dictionnaires/anglais-francais/bug/567570].
[1887] BARRAUD (Boris), « Les blockchains et le droit », art. cit., *loc. cit.*

défaillance contractuelle et/ou technique[1888], et finalement à appliquer les régimes de responsabilité juridique. Or, comment assigner devant un juge une suite de chiffres et de lettres ?

B. Difficile recherche et mise en œuvre de la responsabilité

262. Régimes de responsabilité et éléments constitutifs d'un préjudice réparable. La question est de savoir *qui*, des contractants, des utilisateurs, des mineurs, des agents-développeur et des responsables de plateforme[1889], engagera sa responsabilité en cas de préjudice survenu à la suite d'un dysfonctionnement au sein d'un écosystème décentralisé tel qu'une *blockchain*. La source du préjudice détermine l'application d'un régime particulier du droit de la responsabilité. Ainsi, bien qu'il ne s'agisse pas du régime principalement visé par ce chapitre, la mise en œuvre de la responsabilité pénale suppose la commission d'une infraction au sens des art. 121-1 à 121-7 du C. pén.[1890], mais également des art. 706-3 à 706-14 du CPP en vertu desquels le préjudice résulte « de faits volontaires ou non qui présentent le caractère matériel d'une infraction »[1891]. De la même manière, concernant la mise en œuvre de la responsabilité civile, l'existence d'un préjudice est essentielle (C. civ., art 1240), qu'il s'agisse d'ailleurs de réparer les conséquences d'un préjudice de nature contractuelle[1892] ou extracontractuelle, délictuelle ou quasi-délictuelle[1893]. L'application d'autres régimes de responsabilité peut, dans le cadre d'une *blockchain*, également être sollicitée. Il s'agit principalement des régimes de responsabilité du RGPD, applicable notamment au responsable de traitement de données à caractère personnel[1894], et du régime de responsabilité des art. 1245 à 1245-17 du C. civ. Mais il pourrait s'agir également, dans une certaine mesure, des différents régimes de responsabilité des art. L. 32-3 à L. 32-3-4 du CPCE issus notamment de la loi n° 2004-575 dite « pour la confiance dans l'économie numérique » du 21 juin 2004[1895] transposant

[1888] White Paper No. ECE/TRADE/457UN Economic Commission for Europe, préc., p. 37.
[1889] En ce sens, v., CAPRIOLI (Éric A.), « La blockchain ou la confiance dans une technologie », *JCP G.*, 2016, n° 23-672, pp. 1162-1163.
[1890] Pour une étude plus détaillée, v. notamment, ALMASEANU (Stephen), art cit., p. 11 et s.
[1891] L. n° 90-589, 6 juill. 1990, modifiant le code de procédure pénale et le code des assurances et relative aux victimes d'infractions, *JORF* n° 159, 11 juill. 1990, p. 8175, art. 2.
[1892] C. civ., art. 1231-1.
[1893] C. civ., art. 1241.
[1894] Règl. (UE) n° 2016/679, préc., Chapitre V, art. 24 et s.
[1895] L. n° 2004-575, 21 juin 2004, pour la confiance dans l'économie numérique, *JORF* n° 143, 22 juin 2004, texte n° 2. Modifiée par la L. n° 2004-669, 9 juill. 2004, relative aux communications électroniques et aux services de communication audiovisuelle, *JORF* n° 159, 10 juill. 2004, texte n° 1.

la directive communautaire 2000/31/CE du 8 juin 2000[1896]. Ces régimes sont en effet applicables aux acteurs assurant le fonctionnement des communications électroniques, c'est-à-dire des « émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique » (CPCE, art. L. 32, 1°). Il s'agit des opérateurs de de communications électroniques[1897] « exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques » (CPCE, art. L. 32, 15°), des fournisseurs d'accès[1898] « dont l'activité est d'offrir un accès à des services de communication au public en ligne » (CPCE, art. 32-3)[1899] et dont la qualification bénéficie d'une appréciation élargie par la jurisprudence[1900], et enfin des hébergeurs[1901], assurant une prestation technique de stockage d'informations fournies par un destinataire du service[1902]. Le secret, potentiellement inscrit au sein d'une transaction, peut également être une source de responsabilité en cas d'atteinte. Il en va ainsi notamment dans le cadre des règles applicables aux secret des correspondances[1903], secret professionnel[1904] et secret des affaires[1905], lesquels font notamment l'objet de plus amples développements dans le cadre d'analyses de l'utilisation de crypto-monnaies telles que *Libra*[1906].

D'une manière générale, et à supposer même que l'auteur des faits soit identifié ou du moins identifiable, faut-il encore, pour que l'action en responsabilité civile soit recevable, que le demandeur soit en mesure de déterminer avec précision l'existence du dommage et la nature du préjudice, le fait dommageable et enfin leur lien de causalité (C.

[1896] Dir. n° 2000/31/CE du Parlement européen et du Conseil, 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »), *JOUE* L 178, 17 juill. 2000, pp. 1-16.
[1897] L. n° 2004-575, préc., art. 9.
[1898] *Id.*
[1899] *Ibid*., art. 6-1.
[1900] FAUCHOUX (Vincent), DEPREZ (Pierre), DUMONT (Frédéric) *et al*., *Le droit de l'internet*, éd. LexisNexis, 3e édition, coll. Droit & Professionnels, 2017, pp. 19-20.
[1901] L. n° 2004-575, préc., art. 6 et 6-1, modifiée par la L. n° 2018-898, 23 octobre 2018, relative à la lutte contre la fraude, *JORF* n° 0246, 24 oct. 2018, texte n° 1, art. 29.
[1902] *Ibid.*, art. 6, I, 2 : « personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ».
[1903] C. pén., art. 226-15. – CPCE, art. L. 32-3 (application aux fournisseurs de service de communication).
[1904] C. pén., art. 226-13. – L. n° 2004-575, préc., art. 6, III, 2, al. 2 (application aux hébergeurs, « pour tout ce qui concerne la divulgation de ces éléments d'identification personnelle ou de toute information permettant d'identifier la personne concernée »).
[1905] Dir. (UE) n° 2016/943 du Parlement européen et du Conseil, 8 juin 2016, sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (Texte présentant de l'intérêt pour l'EEE), *JOUE* L 157, 15 juin 2016, pp. 1-18, art. 1er, 3, et 4, § 2-3.
[1906] MAYMONT (Anthony), « La protection des particuliers face aux cryptomonnaies », *Contrats, conc. consom.* 2020, n° 3, alerte 10. – V. également, DEVÈZE (Jean) (dir.), « Innovations dans l'univers des cryptomonnaies », *Le Lamy Droit du Financement*, n° 2905.

civ., art. 1240). D'autant que la question de l'administration de la preuve dans ce contexte de recherche de responsabilité mériterait d'être également discutée[1907].

Dans cette perspective, il convient d'abord d'analyser ce qui peut raisonnablement constituer un dommage sur une *blockchain*.

263. Nécessaire qualification du dommage. Si la question de la qualification se pose en particulier concernant l'apparition de *bugs* informatiques, les hypothèses de dysfonctionnement ne sont pas limitées et il peut en résulter des conséquences importantes.

En matière de réseaux de communications, par exemple, la Cour de cassation a reconnu l'existence d'une obligation de résultat quant aux services mis en œuvre par les fournisseurs d'accès à Internet (FAI) au sein du contrat les liant à leurs clients. En principe, cette obligation les empêche d'organiser l'exonération de leur responsabilité en cas de panne ou d'interruption de l'accès à Internet, « hormis le cas de force majeure »[1908]. Toute défaillance technique non solutionnée par le FAI représente par conséquent une source potentielle de dommage. Cependant, la question se pose de savoir si, dans l'hypothèse d'une défaillance technique du protocole d'une *blockchain*, le régime de responsabilité applicable aux FAI, et en particulier l'obligation de résultat les concernant, pourrait être transposé au(x) développeur(s) de la *blockchain* dans un objectif d'indemnisation des victimes.

Bien que ce régime, ou d'ailleurs celui des produits défectueux précité, puissent sur certaines points apparaître pertinents, leur application dépend de l'origine de la défaillance, à savoir un *bug* émanant des lignes de code et, de plus s'agissant du second régime de responsabilité, constituant un éventuel défaut de sécurité connu (C. civ., art. 1245-10, 4°) ou, du moins, préexistant au moment de la mise en circulation du protocole (C. civ., art 1245-10, 2°).

Par exemple, en dehors de l'initiative du fondateur de la chaîne de soumettre au vote plusieurs solutions se proposant de réparer le préjudice subi par chacune des victimes à la suite du *hack* d'une application d'*Ethereum*[1909], la mise en œuvre de sa responsabilité pose un problème d'appréciation quant au défaut du produit. En effet, selon que la faiblesse dans la programmation est considérée comme un défaut antérieur ou postérieur à la mise en circulation de l'application d'*Ethereum* (C. civ., art. 1245-10, 2°), la

[1907] ZOLINSKY (Célia), art. cit., n° 22.
[1908] Cass. Civ. 1ère, 19 nov. 2009, n° 08.21-645 (clauses d'exonération de responsabilité abusives). – Confirmé par, Cass. Civ. 1ère, 31 mars 2011, n° 10.11-831. – V. également sur le sujet, FAUCHOUX (Vincent), DEPREZ (Pierre), DUMONT (Frédéric) *et al*., *Le droit de l'internet*, *op. cit.*, pp. 40-42.
[1909] Pour une étude détaillée de l'affaire « *TheDAO* », *infra* n°s 239 et s.

responsabilité d'*Ethereum*, et en particulier des développeurs de l'application, aurait ou non pu être retenue. La question est d'autant plus délicate qu'il s'avère que, dans le cadre d'une *blockchain*, les défaillances engendrant des préjudices importants pour les utilisateurs sont le plus souvent découvertes à l'occasion de son exploitation par l'attaquant (C. civ., art. 1245-10, 2° et notamment 4°). En matière de sécurité informatique, lorsqu'une faille est découverte, les développeurs doivent en principe être avertis et disposer d'un délai pour installer un correctif avant que cette vulnérabilité ne soit rendue publique[1910]. Seulement, dans la pratique, il arrive que des failles soient exploitées plutôt que révélées. Or, même permis par une erreur de programmation, le *hack* de l'application *d'Ethereum* n'est que le résultat d'une utilisation contraire au code algorithmique. Autrement dit, la défaillance du code de l'application d'*Ethereum* ne semblait présenter aucun défaut de sécurité au moment de sa mise en circulation avant qu'un des utilisateurs, animé d'intentions malveillantes, ne décide d'user et de créer, par sa seule intervention et donc par son seul fait, une faille de sécurité (C. civ., art. 1245-10, 2° ; art. 1245-13)[1911]. Les attaques régulièrement subies par les sites web n'engagent d'ailleurs pas leurs responsabilités dès lors qu'elles ne sont pas de leurs propres faits. Ce constat laisse entière la question de l'application du régime de responsabilité du fait des produits défectueux.

Par ailleurs, la responsabilité des développeurs de *blockchains* pourrait de surcroît ne pas être retenue au regard des régimes applicables, éventuellement aux FAI, du moins aux fournisseurs de systèmes numériques, dès lors qu'aucun contrat, y compris des conditions générales d'utilisation (CGU), ne régit leurs relations avec les utilisateurs. En parallèle, cette responsabilité pourrait être également limitée en présence d'un contrat si celui-ci contient des clauses visant à les exonérer de leur responsabilité telles qu'elles existent, par exemple, concernant la modification fortuite de la chaîne. En effet, nombre de plateformes de *trading* de crypto-monnaies incluent dans le contrat les liant aux utilisateurs une clause de non-responsabilité empêchant leurs clients d'obtenir réparation des conséquences découlant d'une décision de *fork*[1912], c'est-à-dire de duplication d'une

[1910] V. par exemple, HARRY (Guillaume), « Failles de sécurité des applications Web », *CNRS* [en ligne], 2012, https://hal.archives-ouvertes.fr/hal-00736013/document ; SYLVESTRE (Guillaume), « Les types de failles et de risques sécurité », *I2D - Information, données & documents*, vol. 54, n° 3, 2017, pp. 30-31 ; DEJEAN (Philippe), SARTRE (Patrice), « La cyber-vulnérabilité », *Études*, vol. juillet-août, n° 7-8, 2015, pp. 21-31 ; « Sécurité numérique et risques: enjeux et chances pour les entreprises », *Sénat* [en ligne], 2 févr. 2015, https://www.senat.fr/rap/r14-271-1/r14-271-143.html.

[1911] « Sécurité numérique et risques : enjeux et chances pour les entreprises », préc.

[1912] La jurisprudence semble davantage condamner le développeur d'une solution numérique en cas de dommages découlant exclusivement d'une anomalie de l'outil. V. en ce sens, Com., 11 déc. 2007, n° 04-20.782, *Igrec c/Gaya Software, NP, Gaz. Pal*. 2008., 1, Somm. 1124, obs. A. Arrigo (« le logiciel comportait une anomalie dans l'écriture du programme de sorte que lorsqu'il a été réinstallé après la panne ayant affecté le serveur, les bases de données reçues des clients et préalablement importées et les

blockchain permettant l'existence simultanée de deux versions d'une même *blockchain*[1913]. Il en va ainsi de la plateforme *Paymium*, qui envisage dans ses CGU l'exécution d'un *fork* ayant invalidé une transaction[1914].

Si la victime peut, en principe, obtenir réparation lorsque le préjudice subi est certain, c'est-à-dire dès lors qu'il est déjà réalisé ou qu'il est le prolongement d'un dommage qui s'est réalisé, la question peut se poser concernant un utilisateur qui aurait perdu, du fait d'une défaillance, une chance de bénéficier d'une éventualité lui étant favorable. Par exemple, en cas de *bug* au niveau du *Cloud mining*[1915], un mineur pourrait-il arguer la perte de chance de remporter la course à la vérification ainsi que la récompense due[1916] ? De la même manière, dans l'hypothèse d'une coupure d'électricité ou d'une défaillance du réseau Internet, ou les deux, y aurait-il perte de chance de conclure un contrat pour un utilisateur ? Partant de là, des questions identiques pourraient se poser vis-à-vis des contrats qui seront dans quelques années formés par les machines connectées, par exemple avec la machine *Samsung W9000*, créée spécialement pour le projet ADEPT[1917]. Si ces causes de responsabilités semblent être éludées par les CGU des plateformes de crypto-monnaies dès lors que le dysfonctionnement ne leur est pas directement imputable[1918], une issue favorable à la question de la perte de chance d'un

développements spécifiques n'étaient pas sauvegardés. [Ayant] retenu que cette anomalie était imputable à l'auteur du logiciel, la cour d'appel a, sans méconnaître la loi des parties, légalement justifié sa décision » de condamner le prestataire).

[1913] Définition du *fork*, *infra* n°s 321 et s. – V. également, Annexe n° 10. Schéma du contenu d'un bloc d'une *blockchain* : l'exemple de *Bitcoin* (blocs n°s 549 313 à 549 315), p. 442.

[1914] V., https://www.paymium.com, Ressources > Conditions d'utilisation : « PAYMIUM met en œuvre tous les moyens techniques raisonnables pour assurer la bonne exécution des transferts de Bitcoin. Le CLIENT reconnait toutefois que PAYMIUM n'est pas responsable des problèmes liés au réseau Internet ou au réseau Bitcoin. En particulier, PAYMIUM ne saurait être tenue responsable de l'apparition d'une fourche (ou « fork ») sur la chaîne de blocs Bitcoin qui invaliderait certaines transactions passées. »

[1915] Aussi appelé « *Cloud Hashing* », le *Cloud Mining* est connu pour sa rapidité, ses performances, mais également sa simplicité d'utilisation en matière de minage de *bitcoins*. Il repose sur l'exploitation de « *super rigs* » de minage à distance. Des sociétés fournissent le *hardware*, c'est-à-dire l'ensemble des machines nécessaires pour miner, et donc la puissance de calcul sur la chaîne, ce qui évite aux clients d'acheter du matériel de minage puisqu'ils peuvent louer la puissance de calcul dont ils ont besoin. – Pour plus de précisions sur le sujet, v. notamment, https://www.bitcoincours.com/2014/04/bitcoin-cloud-mining.html.

[1916] Cass. Crim., 18 mars 1975, n° 74-92118 (la perte de chance consiste en la « disparition actuelle et certaine d'une éventualité favorable »). Étant précisé que « l'élément de préjudice constitué par la perte d'une chance présente un caractère direct et certain chaque fois qu'est constatée la disparition, par l'effet du délit, de la probabilité d'un évènement favorable – encore que, par définition, la réalisation d'une chance ne soit jamais certaine – […] » [Cass. Crim., 1er juin 1990, nº 89-83.703]. – C. civ., art. 1240.

[1917] Sur le projet ADEPT, *supra* n° 88.

[1918] V., https://www.paymium.com, Ressources > Conditions d'utilisation : « Par ailleurs, les CLIENTS sont conscients qu'ils doivent s'adresser au fournisseur d'accès à Internet de leur choix pour accéder à Internet et à la Plateforme. Dans ce contexte, les CLIENTS sont conscients qu'il leur appartient de sélectionner leur fournisseur d'accès à Internet et de fixer les modalités de ses relations avec ce dernier. Ni PAYMIUM ni le PARTENAIRE BANCAIRE ne sauraient être responsables des risques relatifs à l'accès à Internet et des risques relatifs à la transmission de données à distance par les CLIENTS ou vers les CLIENTS, notamment en cas de conflit opposant les CLIENTS à ce fournisseur d'accès à Internet, en relation avec le caractère confidentiel/personnel des données transmises, le coût de transmission, la maintenance des lignes téléphoniques et du réseau Internet ou encore les interruptions du système. […]

mineur d'une *blockchain* semble peu envisageable eu égard à la faible probabilité objective de remporter cette course[1919]. La réalité de la perte de chance pourrait toutefois être établie par un utilisateur, et éventuellement accueillie par un juge, dans l'hypothèse de l'absence de conclusion d'un contrat dont le délai d'acceptation aurait, par exemple, été dépassé.

Cependant, à supposer même qu'il s'agisse d'un préjudice tel que le droit et la jurisprudence l'entendent et envisagent de le réparer, encore faut-il pouvoir déterminer le fait générateur d'un tel préjudice et, de surcroît, être en mesure d'en administrer la preuve.

264. De la complexité de déterminer la source du dommage à la difficile désignation du responsable dans un système décentralisé. En toute hypothèse, pour qu'un préjudice soit indemnisable, le demandeur doit être en mesure d'établir l'origine du fait dommageable. En matière de *blockchain* la difficulté ne résulte pas tant de l'impossibilité d'en apporter la preuve, puisqu'au contraire la technologie devrait constituer sur ce point un avantage *via* ses caractéristiques d'immuabilité et d'accessibilité[1920]. L'obstacle résulte plutôt de la configuration décentralisée et distribuée de la chaîne de blocs qui multiplie les sources potentielles de dommage et complique ainsi la recherche du juge, en particulier lorsque le pseudonymat est pratiqué. *A fortiori*, par sa proximité, le lien de causalité avec le dommage semble tout autant difficile à démontrer dans ces conditions.

Ainsi, dans l'hypothèse où une opération initiée n'aurait finalement pas été inscrite sur la *blockchain* et aurait entraîné un préjudice économique pour l'une des parties, ou dans le cas d'une information qui aurait été interceptée par un tiers, s'agirait-il automatiquement d'une défaillance du système pouvant objectivement engager la responsabilité de l'agent développeur, « fournisseur d'accès » à la *blockchain*[1921], et/ou de la plateforme ayant permis éventuellement l'accès à la chaîne ? Ou s'agirait-il d'une erreur de validation de nature à engager la responsabilité du mineur ayant validé et créé le bloc ? À condition néanmoins dans ces cas que le mineur puisse être tenu responsable pour les faits du nœud, son système d'exploitation, lequel consiste en un programme informatique. Or, cela semble de moins en moins envisageable eu égard au projet de

PAYMIUM ne pourra être tenue pour responsable des dysfonctionnements de dispositifs techniques indépendants de son contrôle. »

[1919] Civ. 1ère, 25 nov. 2010, n° 09-69.191, *D.* 2011, 348 (« La perte de chance subie par le justiciable qui a été privé de la possibilité de former un pourvoi en cassation par la faute d'un auxiliaire de justice se mesure à la seule probabilité de succès de cette voie de recours »).

[1920] Pour une étude détaillée de la *blockchain* comme variété de preuve algorithmique naissante, *supra* n°s 139 et s.

[1921] Question écrite n° 96014, *JOAN Q*, 24 mai 2016, p. 4369.

réforme de la responsabilité civile, présenté par la Chancellerie le 13 mars 2017, qui tend explicitement à restreindre l'application de l'art. 1242 al. 2 du C. civ. au fait des choses *corporelles*[1922]. Par ailleurs, s'agissant d'un « logiciel libre » et décentralisé, de type « *free software* » ou « *freeware* » selon les chaînes[1923], et appartenant par essence à chacun des membres du réseau et par extension à tous ceux qui veulent y participer, déterminer un responsable au sein des acteurs de l'écosystème *blockchain* semble aussi délicat que désigner systématiquement le développeur ou les mineurs responsables. En effet, si, comme le souligne un auteur, « les nœuds ne sont là que pour valider une opération sur la *blockchain* [de sorte qu']engager la responsabilité d'un nœud en particulier revient à déterminer que telle adresse IP a effectué une erreur qui a causé à l'une des parties un dommage (puis, encore faut-il être capable de déterminer une telle erreur...) »[1924], le rôle joué par les utilisateurs sur la chaîne n'est pas sans conséquence. Une défaillance au cours de la validation d'un bloc pourrait avoir pour origine première l'*exploit* d'une faille en interne par un utilisateur, ou à partir de l'extérieur par un tiers. L'enjeu réside ensuite dans l'identification à proprement dite de l'individu.

Alors que cette identification peut parfois aboutir, comme au cours de l'affaire de détournement de 341 millions de yens (équivalent à 2,7 millions d'euros) par le biais de la plateforme *MtGox* dont l'historique des transferts d'argent a permis aux juges de remonter jusqu'à Mark Karpeles[1925], elle est en règle générale aléatoire au sein des *blockchains* garantissant le pseudonymat. Il en a été ainsi, par exemple, pour le détournement de l'application *TheDAO* d'*Ethereum* par un de ses utilisateurs. Impossible de l'identifier, la responsabilité du *hacker* n'a donc jamais pu être engagée devant un juge.

265. La difficile mise en œuvre de la responsabilité au sein d'un système décentralisé : un besoin d'adaptation pour une meilleure sécurité juridique. En l'état

[1922] Projet de réforme de la responsabilité civile, 13 mars 2017, par Jean-Jacques Urvoas, garde des sceaux, ministre de la Justice, à la suite de la consultation publique menée d'avril à juillet 2016.
[1923] Tel que l'explique Christiane Féral-Schuhl [v., FÉRAL-SCHUHL (Christiane), *CyberDroit : Le droit à l'épreuve de l'Internet*, éd. Dalloz, coll. Praxis Dalloz, 8e édition, 2020, pp. 941-942], le *free software*, ou logiciel libre proprement dit, désigne une interface à la fois techniquement et légalement « gratuite » et « libre » d'utilisation, mais également de modification et de diffusion (ce qui pourrait s'appliquer à *Bitcoin*). Alors que l'appellation « *freeware* » qualifie l'interface « volontairement [concédée] gratuitement à l'utilisateur » mais qui reste un logiciel propriétaire dont le code source n'est pas ouvert à analyse ou à modification (ce qui pourrait s'appliquer à *Ethereum*).
[1924] COIFFARD (Didier), art. cit., n° 147.
[1925] NISHIMURA (Karyn), « Verdict vendredi pour Mark Karpelès, le baron déchu du bitcoin », *Wolters Kluwer* [en ligne], 13 mars 2019, Actualités du droit > Tech&Droit > Blockchain, https://www.actualitesdudroit.fr/browse/tech-droit/blockchain/20324/verdict-vendredi-pour-mark-karpeles-le-baron-dechu-du-bitcoin ; ROUSSEAU (Yann), « Au Japon, l'ancien "baron" français du bitcoin Mark Karpelès révolté contre sa peine de prison avec sursis », *LesEchos* [en ligne], 14 juin 2020, https://www.lesechos.fr/finance-marches/marches-financiers/au-japon-lancien-baron-francais-du-bitcoin-mark-karpeles-revolte-contre-sa-peine-de-prison-avec-sursis-1214511.

de l'art, aucun mécanisme de détection des *bugs* n'a été implanté au sein des protocoles de *blockchains*. Selon un rapport de Trail of Bits, plus de 246 types de vulnérabilités différents ont été découverts ces dernières années au sein des systèmes de *smart contracts*[1926]. Pour les opérateurs télécoms, les FAI et les fournisseurs d'outils numériques, le non-respect de leur obligation de notifier les utilisateurs concernés par la découverte d'une faille ou autre *bug* est de nature à engager leur responsabilité contractuelle[1927]. Une auteure en déduit qu'une telle obligation en matière de *blockchain* permettrait de combler les difficultés de remonter à la source du dommage[1928]. Seulement, à qui devrait incomber cette responsabilité au sein de la chaîne ? D'autant plus que, comme le souligne le rapport de Trail of Bits, il est pratiquement impossible en pratique de détecter et de tester ces failles tant leur nombre est important[1929].

Finalement, en plus de la difficulté de remonter à la source d'un dommage survenu au sein d'une *blockchain*, la détermination de la ou les personnes qui devront engager leur responsabilité prête à discussion. En tout état de cause, la mise en œuvre de la responsabilité au sein de la *blockchain* implique de déterminer préalablement si l'identification d'une faute est nécessaire et, le cas échéant, caractériser le(s) fait(s) pouvant en être à l'origine. En parallèle, il semble qu'il faille également évaluer le cas où il serait techniquement impossible de remonter à l'origine du dommage, de manière à, éventuellement, ne pas laisser des utilisateurs ou des cocontractants victimes subir un préjudice sans en obtenir réparation. Si un contractant, ayant exécuté les termes de son contrat, mais dont la mise à jour du *smart contract* contenant la preuve de son exécution n'aurait – pour une raison quelconque – pas été intégrée à la chaîne, a subi les lourdes indemnités d'inexécution automatiques prévues, il semblerait insatisfaisant voire injuste qu'il dédommage son cocontractant pour une inexécution de l'algorithme. En revanche, Lemy Godefroy souligne que « le code algorithmique, bien qu'autonome, est programmé […] et manié par des individus tenus d'endosser leur part de responsabilité »[1930]. Ainsi, en matière de *smart contract*, si le code informatique produit des effets inattendus à cause,

[1926] GROCE (Alex), « 246 Findings From our Smart Contract Audits: An Executive Summary », *Trail of Bits* [online], 8 Aug. 2019, https://blog.trailofbits.com/2019/08/08/246-findings-from-our-smart-contract-audits-an-executive-summary/. – V. également les publications de Trail of Bits sur GitHub, https://github.com/trailofbits/publications#security-reviews.
[1927] Ord. n° 2011-1012, 24 août 2011, relative aux communications électroniques, *JORF* n° 0197, 26 août 2011, p. 14473, texte n° 49, art. 34 *bis*. – Dir. n° 2002/58/CE du Parlement européen et du Conseil, 12 juill. 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *JOUE* L 201, 31 juill. 2002, pp. 37-47, art. 4, § 3.
[1928] DEVILLIER (Nathalie), art. cit., p. 1037.
[1929] GROCE (Alex), art. cit.
[1930] GODEFROY (Lêmy), « Le code algorithmique au service du droit », *D*. 2018, pp. 734 et s.

spécifiquement, d'une erreur de programmation des cocontractants, ceux-ci ne devraient pas, selon l'auteur, ouvrir droit à réparation.

Des adaptations sont nécessaires, d'autant plus que le risque réside dans la dilution des responsabilités[1931]. Il semble que le droit pourrait empêcher un tel risque, à condition de faciliter la détermination des potentiels responsables.

266. Propositions. Au-delà des difficultés techniques pouvant être rencontrées au cours de la recherche du fait générateur d'un dommage, nombre d'auteurs réfléchissent à définir, ou à redéfinir, en lien avec ses particularismes, le cadre juridique de la responsabilité au sein de la technologie *blockchain*.

Il en va ainsi de Catherine Barreau qui propose de retenir une responsabilité pour faute, laquelle pourrait éventuellement prendre la forme d'une faute lourde, à l'encontre des développeurs du protocole d'une *blockchain* en cas de défectuosité de la chaîne, c'est-à-dire dans l'hypothèse d'une impossibilité à « réaliser les actions promises »[1932]. Elle envisage également d'engager la responsabilité de tout utilisateur en cas de corruption de la chaîne, notamment si celle-ci a conduit à priver les parties à un *smart contract* de son exécution automatisée[1933]. Cette proposition semble conforme aux principes de la technologie autant qu'avec le droit objectif. Mais encore faut-il pouvoir identifier le ou les développeur(s) et utilisateur(s).

Dans le doute d'un pseudonymat persistant, certains proposent de créer un régime autonome de garantie permettant aux victimes d'obtenir la réparation de leur préjudice. Cette assurance décentralisée assurerait ainsi le risque de vulnérabilités dans l'espace décentralisé[1934]. À l'instar de ce que proposait le Parlement européen à la Commission concernant les systèmes robotiques[1935], des sociétés telles que la mutuelle Nexus ont mis en place une police d'assurance mutualisée spécifique pour garantir les risques en matière de *smart contracts*, y compris lorsque ceux-ci ont été créés pour des cas d'utilisation non encore testés comme des *dApp*[1936]. Bien que cette solution paraisse parfaitement

---

[1931] *Id*.
[1932] BARREAU (Catherine), art. cit., *loc. cit*.
[1933] *Id.*
[1934] GUILHAUDIS (Élise), art. cit., p. 10.
[1935] V., Résol. n° 2015/2103 (INL) du Parlement européen contenant des recommandations à la Commission, 27 janv. 2017, concernant des règles de droit civil sur la robotique, point n° 57 : « une solution envisageable, face à la complexité de l'imputabilité des dommages causés par des robots de plus en plus autonomes, pourrait résider dans la mise en place d'un régime d'assurance obligatoire, comme c'est déjà le cas, entre autres, pour les automobiles; relève néanmoins que, contrairement au régime d'assurance des véhicules routiers, qui couvre les actes et l'inaction des automobilistes, un régime d'assurance robotique devrait tenir compte de toutes les responsabilités potentielles d'un bout à l'autre de la chaîne ».
[1936] https://nexusmutual.gitbook.io/docs/users/docs, Home > Users > Understanding Nexus Mutual. V. également, SUBRAMANIAN (Hemang), « Decentralized Insurance for Smart contracts », *CryptoTech*

envisageable, la question se pose de la provenance des cotisations, de sorte que des difficultés d'adoption seront à considérer[1937].

Selon certains auteurs, le régime actuel de responsabilité tendrait à ne pas pouvoir s'appliquer aux spécificités de l'OVNI juridique qu'est la *blockchain* en la matière. Tandis que Lêmy Godefroy sollicite l'adoption d'un « droit général des algorithmes »[1938], Élise Guilhaudis évalue quant à elle la pertinence du régime de responsabilité des intermédiaires techniques d'Internet appliqué aux acteurs des *blockchains*[1939]. Il s'avère pourtant que, pour l'un, comme pour l'autre, l'enjeu principal réside dans la mise en place d'un système auquel les actuels comme futurs utilisateurs de la *blockchain* pourront se fier. Toutefois, les propositions de Lêmy Godefroy semblent presqu'entièrement dirigées vers une responsabilité du « concepteur »[1940], ce qui pourrait se révéler contre-productif et brider l'innovation en la matière. Une étude plus approfondie de ces différentes propositions se révèlera nécessaire. Si besoin est, la définition des mécanismes de responsabilité se devra d'être éclaircie afin de construire une confiance stable et durable, déterminante pour l'avenir de la technologie.

Par ailleurs, et d'une manière générale, l'obstacle majeur qu'il faut à nouveau chercher à solutionner est la pseudonymisation pratiquée au sein du protocole de la majorité des *blockchains.* Au même titre que pour la signature électronique[1941], la mise en place d'un système d'identification décentralisé et sécurisé sera indispensable pour ainsi laisser au droit la possibilité de s'appliquer et au juge de remplir son office en cas de contentieux, ou à tout le moins dès la survenance d'un préjudice. Une telle configuration sera de surcroît une source de confiance pour l'utilisation de la technologie. Plus encore, elle permettrait à la chaîne de se conformer aux diverses exigences de

---

[online], 24 Jul. 2020, https://www.cryptonewtech.com/2020/07/24/decentralized-insurance-for-smart-contracts/.

[1937] *Id.*

[1938] GODEFROY (Lêmy), « Le code algorithmique au service du droit », art. cit., *loc. cit.* – V. également, ZOLINSKY (Célia), art. cit., *loc. cit.*

[1939] L. n° 86-1067, 30 sept. 1986, relative à la liberté de communication (Loi Léotard), *JORF*, 1 oct. 1986, complétée par la L. n° 2004-575, préc.

[1940] *Id.* : « Un régime de responsabilité pour faute présumée serait invocable à l'encontre du concepteur face à un dommage dû à une programmation initiale erronée ou à une insuffisance de vigilance durant le fonctionnement de l'outil algorithmique ou de l'utilisateur si le dommage est causé à la suite du maniement de l'outil algorithmique. Un régime de responsabilité objective pourrait être instauré pour un dommage causé par l'autonomie fonctionnelle dont l'algorithme a été doté à sa fabrication et qu'il a développée au cours de l'apprentissage, puis tout au long de son fonctionnement. Dans cette situation, les conditions de la garde de la chose de l'article 1242, alinéa 1er, du code civil ne sont pas remplies en l'absence de pouvoir exercé sur l'algorithme au moment du dommage. La responsabilité du fait des produits défectueux visée aux articles 1245 à 1245-17 du code civil n'est pas non plus un fondement pertinent car l'éventuel défaut de sécurité n'existait pas avant la mise en circulation de l'outil algorithmique. En revanche, la charge de la réparation pèserait sur le concepteur qui détient le savoir technique parce qu'il connaît les potentialités dommageables de l'autonomie fonctionnelle de son algorithme. »

[1941] Sur les aléas de la pseudonymisation en matière de signature électronique, *supra* n°[s] 116 et s.

notification de faits litigieux, de collaboration avec les autorités[1942], etc. La seule condition demeure toutefois l'acceptation par l'écosystème d'une telle immixtion de l'État au sein de la chaîne. D'autant plus qu'à défaut d'engager la responsabilité afin d'obtenir une réparation des préjudices subis, il sera nécessaire, si la gravité des dommages le requiert, que le développeur puisse agir pour protéger les utilisateurs.

267. D'une manière générale, le potentiel des *blockchains* se heurte à ses propres limites, de sorte qu'une adaptation réciproque entre le droit et les règles de fonctionnement propres à la technologie constitue la clé de l'intégration de la technologie dans la société contemporaine. En entravant l'application des dispositions légales protectrices, la *blockchain* nuit à son accueil dans les secteurs où la confiance des acteurs économiques est primordiale et, de son côté, le droit ne peut assurer la sécurité des justiciables[1943]. Il appartient au juriste d'anticiper ces diverses incohérences afin, d'une part, de maintenir la sécurité juridique au sein d'une technologie en déploiement et, d'autre part, de soutenir l'innovation et le développement des pratiques actuelles. Cette adaptation est d'autant plus nécessaire que dans le domaine contractuel en général et, des affaires en particulier, les *blockchains* se révèlent être de puissants atouts, notamment en matière de sécurisation des données[1944] et, dernièrement, de RSE[1945]. Sous forme de registre ou de *smart contract*, la *blockchain* améliore tant la traçabilité des transactions et des produits en limitant le facteur de risque d'erreur humaine lié aux questions d'authenticité, d'acheminement et de « risque RSE », que l'application effective des normes en les automatisant[1946]. D'après Boris Barraud, l'avènement des *blockchains* « [marquerait] une rupture avec le droit moderne tel qu'on l'édicte, l'applique, le pratique, l'enseigne et l'étudie depuis des décennies » si bien que la technologie constitue « peut-être le parangon du "droit postmoderne" appelé à prendre demain le pouvoir »[1947]. Pour autant, cette adaptation ne pourra être complètement réalisée si la technologie n'inspire pas pleine confiance *via* une intégrité sans faille et, finalement, une promesse de sécurité

[1942] L. n° 2004-575, préc., art. 6, I et II.
[1943] GODEFROY (Lêmy), « Le code algorithmique au service du droit », art. cit., *loc. cit.* ; ZOLINSKY (Célia), art. cit., *loc. cit*.
[1944] ANCIAUX (Arnaud), FARCHY (Joëlle), MÉADEL (Cécile), « L'instauration de droits de propriété sur les données personnelles : une légitimité économique contestable », *Revue d'économie industrielle* 2017/2, n° 158, p. 30.
[1945] RESTREPO AMARILES (David), VAN WAEYENBERGE (Arnaud), COLOMBANI (Lorenzo), « *Responsabilité sociale des entreprises. Enjeux globaux et technologiques* », *Revue française de gestion* 2017/8, n° 269, pp. 166-172.
[1946] *Id.*
[1947] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 20.

numérique. Or, une telle exigence n'est pas encore tout à fait remplie par la *blockchain*. En effet, avant de pouvoir s'imposer en tant que valeur ajoutée sur le marché économique, elle devra d'abord régler les dysfonctionnements et autres risques technologiques qu'elle a, le plus souvent, indirectement générés.

TITRE 2. Problèmes créés de l'utilisation faite de la *blockchain* : un manque de fiabilité

268. Les nouvelles technologies sont souvent synonymes de progrès, de mutations, de modification des processus habituels, mais également de craintes. Ces craintes sont souvent multiples, il peut être question de craindre un remplacement du travail de l'Homme, de craindre l'impact d'une omniprésence technologique, ou encore de craindre des risques encore inconnus. Ainsi, lorsqu'une technologie vante ses qualités de « machine à créer de la confiance »[1948], les attentes sont nécessairement démultipliées, tout comme le risque de les décevoir. Chaque innovation opère un certain nombre d'améliorations, lesquelles corrigent le plus souvent des défauts de ses précurseurs, sans toutefois se révéler parfaitement infaillible. La technologie de la *blockchain* ne fait pas exception. Ses spécificités constituent à la fois ses forces et ses faiblesses, l'exposant à des dangers souvent inédits. Nouveau champ d'investigation pour les juristes, deux problèmes liés à son utilisation risquent particulièrement de faire obstacle à l'institution d'une confiance algorithmique étant donné que certaines personnes animées d'intention malveillantes sont susceptibles de les utiliser pour mieux servir leurs intérêts. Il s'agit, d'une part, de la difficulté d'instaurer une gouvernance au sein du protocole (Chapitre 1) et, d'autre part, de l'existence de vulnérabilités fonctionnelles (Chapitre 2).

[1948] « The promise of the blockchain: The trust machine », *The Economist* [online], 31 Oct. 2015, https://www.economist.com/leaders/2015/10/31/the-trust-machine.

Chapitre 1. Les enjeux de la gouvernance

269. Le terme « gouvernance » constitue un anglicisme[1949] s'apparentant à la manière de gouverner, d'exercer le pouvoir. Communément, le concept de gouvernance « renvoie à un système d'entités décisionnelles qui dirige un certain domaine d'activités, autrement dit à un "système de gouvernance", impliquant notamment une structure de gouvernance et un dynamisme de système (processus de gouvernance, activités de gestion, etc.) »[1950]. Parmi les multiples formes de gouvernance, une *summa divisio* s'établit entre gouvernance publique et gouvernance privée de sorte qu'en matière de *blockchain*, la question de la gouvernance se pose à tous les niveaux de la doctrine, scientifique autant que juridique et économique.

Originellement décentralisé et distribué, le protocole des *blockchains* publiques encourage l'auto-régulation *via* la neutralité de l'algorithme. Seulement, le dilemme posé par *TheDAO* a conduit la communauté à remettre en question le principe de neutralité de la chaîne pour assurer la protection des utilisateurs (Section 1). Alors que la *blockchain* originelle nécessiterait certaines adaptations, la pratique a révélé le développement d'autres modèles de régulation.

À l'exact opposé de la *blockchain* publique, la privatisation de la technologie a permis de constituer des formes de *blockchain* capable de faciliter leur gestion, mais il s'avère que leur mise en œuvre entraînerait la réinstauration d'une organisation hiérarchique (Section 2).

En conséquence, deux modèles de régulation fondamentalement opposés se font face, si bien qu'un état des lieux s'avère nécessaire.

Section 1. Le dilemme *TheDAO* : entre protection des utilisateurs et neutralité de la chaîne

270. Les DAO, *Decentralized Autonomous Organizations* – Organisations Autonomes Décentralisées en français –, incarnent la solution technique aux multiples imperfections des systèmes centralisés. Composées d'un ensemble de *smart contracts*, les DAO sont programmées pour établir et fournir des règles de gouvernance à un modèle décentralisé

[1949] Cambridge Dictionary [online], v° Governance, https://dictionary.cambridge.org/fr/dictionnaire/anglais/governance : « the way that organizations or countries are managed at the highest level, and the systems for doing this; the activity of governing something ».
[1950] ZENNER (Alain), *Le Dictionnaire ludique & érudit du Confinement*, Éditions Luc Pire, 2020, p. 236.

et distribué, contribuant ainsi à le rendre autonome[1951]. La DAO constitue finalement l'espoir d'une gouvernance neutre, impartiale et distribuée. Néanmoins, l'échec d'un projet de DAO a eu pour conséquence de décréditer, du moins momentanément, la *blockchain*, tantôt dans son fonctionnement, tantôt dans ses fondements. En effet, à la suite du détournement de *TheDAO*, l'application décentralisée d'*Ethereum*, par « *The DarkDAO* » (§ 1), la Fondation Ethereum est intervenue pour tenter de limiter les atteintes portées au système et à ses utilisateurs, si bien que cette intervention a été, pour certain, le signe d'une ré-intermédiation et a remis en cause l'intégrité et les principes du système des *blockchains* (§ 2). Afin d'en tirer les meilleurs enseignements, il conviendra d'analyser cette affaire en suivant la chronologie des évènements, et en prenant pour repère la solution proposée par la Fondation.

§ 1. De TheDAO à The DarkDAO

271. Il importe dans un premier temps de rappeler les enjeux ainsi que les conditions techniques du fonctionnement de cette DAO (A), avant de passer à l'examen des éléments factuels et techniques qui ont conduit à son détournement (B) et, plus tard, l'intervention de la Fondation.

A. Enjeux et conditions techniques du fonctionnement de TheDAO

272. La DAO, ou l'institution d'une société décentralisée, démocratique[1952] et autonome. Application dérivée de la technologie des *smart contracts*, les organisations autonomes décentralisées – ou distribuées – (DAO) ambitionnent de remplacer les plateformes existantes, voire de proposer une alternative à la personnalité morale, et de créer ainsi une nouvelle forme de relation sociale et économique fondée sur l'absence d'autorité centralisatrice. Nombre d'auteurs considèrent la DAO comme la finalité des *blockchains*[1953]. Organisée selon un modèle de décision horizontal, la DAO rompt avec la logique verticale ou pyramidale des sociétés étatiques et économiques traditionnelles[1954] et tend à édifier des normes propres[1955]. La DAO fournit en effet des

[1951] Pour une étude plus détaillée de la DAO, *supra* n° 42.
[1952] À l'image de la « démocratie liquide » qu'envisage Vitalik Buterin [BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », *github* [liens de publication originaux supprimés] [online], Nov. 2013, https://github.com/ethereum/wiki/wiki/White-Paper].
[1953] LEGEAIS (Dominique), « Blockchain », *JCl. Sociétés Traité*, fasc. 2160, n°ˢ 60-61.
[1954] BARRAUD (Boris), « Les blockchains et le droit », *RLDI* 2018/4, nº 147, p. 18.
[1955] LEGEAIS (Dominique), *op. cit.*, *loc. cit*.

règles de gouvernance transparentes et immuables à une communauté ce qui, d'après Boris Barraud, « [témoigne] de la capacité des nouvelles technologies de communication de coordonner différentes parties sans recourir à une instance régulatrice centrale ou surplombante »[1956]. En d'autres termes elle n'a ni personnalité juridique, ni représentant physique[1957], et elle met en œuvre un processus de décision entièrement transparent et neutre. Le « super *smart contract* »[1958] régissant l'organisation contient à la fois les règles de fonctionnement et les règles d'exécution programmées[1959]. Finalement, la DAO laisse envisager une véritable gouvernance à la fois décentralisée et autonome[1960]. Pour certains, une telle technologie pourrait servir à construire de nouveaux modèles non seulement économiques mais également sociaux et politiques, « plus libres, transparents et démocratiques »[1961]. En principe, la DAO est constituée de deux parties qu'elle œuvre à coordonner, à savoir, d'une part, les détenteurs de *tokens*, lesquels peuvent être assimilés à des actionnaires disposant d'un droit de vote et participant aux bénéfices, et, d'autre part, les prestataires qui vont soumettre des projets à financer. Selon Boris Barraud, la DAO mêle la coopération et la compétition pour organiser une « coopétition », permettant à des membres reliés les uns aux autres par un réseau horizontal sans système hiérarchique, de coordonner leur action et, en définitive, de s'auto-gérer[1962]. Il s'agissait d'ailleurs de l'objectif poursuivi par l'initiative de la Fondation Ethereum.

273. *TheDAO*, la création d'un financement participatif auto-gouverné ? Lancée sur le bloc n° 1 428 757 d'*Ethereum*[1963] le 28 mai 2016[1964], avec un total de 12 millions d'*ethers*[1965] pour 10 000 contributeurs, *TheDAO* constituait la première expérience dans le domaine[1966]. Portée par la *start-up* slock.it, *TheDAO* devait permettre de créer des collectes de fonds, sous la forme de financements participatifs (*crowdfundings*) anonymes

[1956] *Id.*
[1957] MEKKI (Mustapha), « Les mystères de la blockchain », *D.* 2017, n° 37, pp. 2160 et s., n° 9.
[1958] GUILHAUDIS (Élise), « Comprendre la blockchain à travers l'étude d'un cas pratique : le covoiturage "Blockcar" », *RLDI* 2017/12, nº 143, p. 9.
[1959] BARRAUD (Boris), « Les blockchains et le droit », art. cit., *loc. cit.*
[1960] *Id*.
[1961] *Id.* ; GUILHAUDIS (Élise), art. cit., *loc. cit.*
[1962] LEGEAIS (Dominique), *op. cit*., *loc. cit.* ; BARRAUD (Boris), « Les blockchains et le droit », art. cit., *loc. cit*.
[1963] Pour plus de précisions sur le sujet et le code source, v., https://etherscan.io/address/0xbb9bc244d798123fde783fcc1c72d3bb8c189413#code.
[1964] En réalité son lancement a été précédé par une levée de fonds dès la publication du « code *TheDAO* » *via* le *github* de *Slock.it* le 30 avril 2016 [v., https://github.com/slockit/DAO ; https://thedao.signup.team/].
[1965] 12 millions d'*ethers* équivalent environ à 140 millions de dollars (USD) au jour du lancement le 30 avril 2016 [v., BARRAUD (Boris), « Les blockchains et le droit », art. cit., *loc. cit*.].
[1966] « TheDAO : fin de la levée de fonds », *Bitcoin.fr* [en ligne], 28 mai 2016, https://bitcoin.fr/the-dao-fin-de-la-levee-de-fonds/.

et uniquement régis par des *smart contracts*. L'idée était de rassembler des participants, à l'image des contributeurs sur les plateformes Internet[1967], qui auraient pu financer, de manière anonyme, des projets divers par le biais de dons en *ethers*[1968]. Au-delà des traditionnels dividendes, chaque participant devait recevoir des *DAO Tokens* au prorata de sa contribution, lesquels lui auraient conféré un droit de vote concernant le financement d'un projet proposé par l'un d'entre eux. Les *ethers* octroyés devaient en principe être récoltés au sein d'un unique *smart contract*[1969], lequel aurait automatiquement réinvesti les sommes collectées dans le projet désigné par le vote. Par ailleurs, chaque participant devait avoir la possibilité de récupérer sa mise à n'importe quel moment, c'est la raison pour laquelle le *smart contract* était programmé de manière à retourner instantanément une partie ou l'intégralité des *ethers* stockés dès la réception d'une demande expresse d'un participant[1970]. Ensuite, la société suisse DAO. LINK devait faire le lien avec le monde réel et mettre en œuvre les financements[1971].

274. Les éléments de programme de *TheDAO* : aperçu des fonctions principales. D'un point de vue technique, l'algorithme de *TheDAO* comprenait essentiellement deux fonctions. D'une part, « *donate(adress)* » attribuait la somme d'*ethers* renseignée lors de l'appel de fonction (*donate*) – à l'adresse renseignée (*(adress)*), ce qui permettait la contribution. D'autre part, « *withdraw(amount)* » permettait à l'actionnaire-contributeur de demander à *TheDAO* de lui reverser (*withdraw*) un nombre d'*ethers* défini (*(amount)*). L'ensemble de ces informations étaient automatiquement enregistré dans un tableau interne au programme de *TheDAO*, ce qui permettait à la fois d'exécuter les mouvements de fonds au sein du *smart contract* principal, et d'en garder un historique immuable[1972].

Mais, l'algorithme comportait une faille. Quelques mois après la révélation du code informatique de *TheDAO* au public, l'application a été victime d'un *hacking*[1973]. Cet évènement souleva un certain nombre de difficultés, notamment en termes de

---

[1967] Direction générale du marché intérieur, de l'industrie, de l'entrepreneuriat et des PME (Commission européenne), « Le financement participatif expliqué. Un guide pour les petites et moyennes entreprises », *Office des publications de l'Union Européenne* [en ligne], 4 juin 2017, https://op.europa.eu/fr/publication-detail/-/publication/d5e626ba-d7c8-11e6-ad7c-01aa75ed71a1.

[1968] GUILHAUDIS (Élise), art. cit., *loc. cit.*

[1969] Il s'agissait en pratique du *smart contract* de *TheDAO*, correspondant à l'adresse « 0xbb9bc244d798123fde783fcc1c72d3bb8c189413 » [HUGUET (Benoît), « TheDAO Hack, état des lieux et perspective », *BitConseil* [en ligne], 23 juin 2016, https://bitconseil.fr/thedao-hack-etat-lieux-perspectives/].

[1970] HUGUET (Benoît), art. cit.

[1971] POLROT (Simon), « TheDAO : post mortem », *Ethereum France* [en ligne], 24 janv. 2017, https://www.ethereum-france.com/the-dao-post-mortem/.

[1972] FLORI (Jean-Pierre), « Sécurité et insécurité de la blockchain et des smart contracts », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 101.

[1973] POLROT (Simon), « TheDAO : post mortem », art. cit.

responsabilités, mais pas seulement puisque la sécurité et *a fortiori* l'intégrité de l'application en ont été affaiblis[1974]. Il convient désormais d'identifier les moyens et les causes de ce détournement.

B. Éléments factuels et techniques du détournement de TheDAO

275. « 03:34:48 UTC, block 1718497 », lancement de l'attaque « *The DarkDAO* » : état des lieux. Malgré les nombreux audits de sécurité effectués sur le code source de l'application, et bien que la communauté ait été alerté quelques jours auparavant[1975], le 17 juin 2016 à « 03:34:48 UTC, *block* 1718497 », 3,6 millions d'*ethers*, soit l'équivalent de 50 millions de dollars, sont dérobés directement dans les fonds de *TheDAO* par le pirate informatique « 0x4a574510c7014e4ae985403536074abe582adfc8 ». Nommé par les utilisateurs du réseau « *Dark token holders* »[1976] ou « *The DarkDAO* »[1977], le logiciel utilisé pour subtiliser les fonds collectés a profité d'une vulnérabilité du système informatique de *TheDAO* lui permettant de contourner les règles de l'application pour servir son propre intérêt. Or, il s'avère que ce n'est pas dans le protocole de la *blockchain Ethereum* mais dans le programme de l'application, et plus précisément dans le langage informatique qui a été utilisé pour traduire l'algorithme de *TheDAO*, que la faille a été localisée[1978].

[1974] GUILHAUDIS (Élise), art. cit., p. 9.

[1975] En effet, il apparaît que dès le 9 juin, un utilisateur utilisant le pseudonyme « Chriseth » [https://github.com/chriseth], s'est inquiété d'un possible vol de *wallet* auprès de Peter Vessenes, un autre contributeur du projet. – V. le blog mis à jour en temps réel des évènements, VESSENES (Peter), « More Ethereum Attacks: Race-To-Empty is the Real Deal », *Vessenes* [online], 9 Jun. 2016, https://vessenes.com/more-ethereum-attacks-race-to-empty-is-the-real-deal/ : « *Chriseth at github casually pointed out a terrible, terrible attack on wallet contracts that I had not considered. If there were a responsible disclosure avenue for ethereum contract developers, I would use it, but there doesn't seem to be. Not only that, this code has been out and published on github for long enough that I wanted to get the news out there quickly. In Brief: Your smart contract is probably vulnerable to being emptied if you keep track of any sort of user balances and were not very, very careful. As always, I'm available for smart contract review and audit, email me. You can read about other security considerations on my blog here. UPDATE: Chriseth notified me that warnings went out to key devs four days ago. He says as written, the attack is less worrisome than I say because by default send() only offers 21k gas, this will not be enough to pay for the nested calls. However, if you use call.value(amt).(), this is still a vulnerability. I am testing a few permutations and will update. UPDATE 2: In general, this reentrancy bug is widespread, but mitigated in the case of using vanilla send. I still strongly recommend a code review and update for all functions that might not have considered if they will be called repeatedly during execution. Thanks to Nick Johnson and Dennis Peterson for engaging on this as well. Update 3: I have been contacted by multiple DAO's with real concerns over this bug in the last week, and it appears the TheDAO is not only vulnerable, but that an attacker is draining TheDAO of millions of ether as we speak: discussion on reddit*. »

[1976] « *Holders* » au pluriel car le pirate a utilisé deux adresses de *wallet* pour lancer son attaque et récupérer plus de 3 millions d'*ethers* contenus dans le *smart contract* de l'application : 0xc0ee9db1a9e07ca63e4ff0d5fb6f86bf68d47b89 et 0xf835a0247b0063c04ef22006ebe57c5f11977cc4.

[1977] PFEFFER (Johannes), « The rise of the DarkDAO », *Medium* [online], 17 Jun. 2017, https://medium.com/@oaeee/the-rise-of-the-dark-dao-72b21a2212e3.

[1978] GUILHAUDIS (Élise), art. cit., *loc. cit.* ; BUTERIN (Vitalik), « CRITICAL UPDATE Re: DAO Vulnerability », *Ethereum Blog* [online], 17 Jun. 2016, https://blog.ethereum.org/2016/06/17/critical-

276. La présence d'une faille dans l'algorithme : l'erreur est humaine, le détournement l'est aussi. En matière de sécurité informatique, une faille dans un programme informatique constitue une vulnérabilité de conception ou de réalisation exploitable par un attaquant[1979]. En règle générale, ces failles proviennent d'anomalies logicielles en lien avec des erreurs, des omissions ou des mauvaises pratiques de programmation[1980], qu'une correction, si elle est découverte[1981], suffit à combler[1982]. Seulement, le délai nécessaire à la recherche et à l'élaboration d'un correctif laisse les utilisateurs exposés au risque d'*exploit*, c'est-à-dire au risque qu'un individu exploite une vulnérabilité du logiciel utilisé.

L'analyse du code informatique de *TheDAO* a révélé que l'élément à l'origine de la manœuvre d'*exploit* de *The DarkDAO* réside dans la fonction « *callback* ». Fonctionnalité propre au langage utilisé, la fonction a été introduite dans l'algorithme puisqu'essentielle pour le déploiement des *smart contracts*[1983]. Cependant, il apparaît que son fonctionnement n'était pas suffisamment connu des développeurs à l'époque de l'attaque. Or, cette fonction était, en pratique, facilement corruptible si elle n'était pas correctement employée.

Techniquement, l'algorithme avait pour instruction d'exécuter la fonction « *callback* » dès que le programme s'activait. Ainsi, n'importe qui, animé d'une intention malveillante, pouvait créer un programme « enfant » à partir de *TheDAO*, correspondant à la copie exacte du programme « parent », mais dont les instructions auraient pour effet de détourner son fonctionnement normal[1984]. En exécutant son programme « enfant », l'individu à l'origine de l'*exploit* procédait à une contribution (« *donate(amount)* ») puis,

update-re-dao-vulnerability/ : « *This is an issue that affects TheDAO specifically; Ethereum itself is perfectly safe.* »

[1979] V. par exemple, HARRY (Guillaume), « Failles de sécurité des applications Web », *CNRS* [en ligne], 2012, https://hal.archives-ouvertes.fr/hal-00736013/document ; SYLVESTRE (Guillaume), « Les types de failles et de risques sécurité », *I2D - Information, données & documents*, vol. 54, n° 3, 2017, pp. 30-31 ; DEJEAN (Philippe), SARTRE (Patrice), « La cyber-vulnérabilité », *Études*, vol. juillet-août, n° 7-8, 2015, pp. 21-31.

[1980] DENIS (Jérôme), « L'informatique et sa sécurité. Le souci de la fragilité technique », *Réseaux*, vol. 171, n° 1, 2012, pp. 170-171.

[1981] Par exemple, le Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques (CERT-FR) procède à une veille technologique (v. le site officiel, https://www.cert.ssi.gouv.fr/) des dernières vulnérabilités de systèmes informatiques identifiées.

[1982] *Id.*

[1983] V., https://www.reddit.com/r/TheDao/comments/4p754l/why_does_ethereum_have_callback_feature_that/. L'un des membres explique d'ailleurs que cette fonction « *callback* » est essentielle pour toute DAO et même pour tout *smart contract* puisque sans elle, les contrats ne pourraient pas implémenter des instructions complexes, et la DAO ne serait probablement impossible à construire. Précisément, c'est cette fonctionnalité qui permet aux contrats de communiquer entre eux. Mais le développeur doit s'assurer qu'ils n'autorisent que des appels vers des parties de code fiables ou connues. Ce qui n'a pas été le cas pour *TheDAO* puisqu'en effet le système ne disposait pas d'une sécurité suffisante pour éviter les *exploits* du type attaque récursive/ré-entrée par le biais d'appels à des adresses ou des contrats inconnus.

[1984] Pour plus de détails, v., *id.*

immédiatement après, demandait à se désister de sa contribution[1985]. Dès lors, automatiquement, l'algorithme exécutait un remboursement (« *withdraw(amount)* ») de la somme précédemment transférée au *smart contract* de *TheDAO*, et la fonction « *callback* » lui permettait finalement de récupérer une seconde fois le montant de sa contribution initiale[1986]. En multipliant et en automatisant les appels de fonctions par le biais d'un programme directement implanté au sein de l'application, le pirate informatique « 0x4a574510c7014e4ae985403536074abe582adfc8 » a créé une boucle d'instructions. S'agissant d'une attaque dite « récursive »[1987], *The DarkDAO* a ainsi indéfiniment extrait la somme d'argent associée, jusqu'à ce que le compte source soit vidé et/ou que son propre compte soit à court de *gas* pour faire exécuter le programme[1988].

277. De l'échec de l'identification à la recherche de solutions. Outre le débat engagé par la communauté *r/ethereum* sur *Reddit*[1989] pour savoir s'il s'agissait d'une simple « faute de frappe » des développeurs ou d'un réel manque de connaissance du langage[1990], la première question qui s'est posée a été de savoir s'il était possible d'identifier l'utilisateur responsable de cette attaque. Or, en la matière, à moins qu'un mécanisme d'identification à l'image de ceux précités[1991] n'ait été préalablement implanté sur la chaîne, ce qui n'était pas le cas pour *TheDAO*, il est difficile de mettre un nom ou une identité sur une adresse de crypto-monnaies[1992]. Faute de pouvoir identifier l'attaquant, la communauté s'est efforcée de trouver une solution. L'objectif n'était pas tant de sanctionner le pirate, mais davantage de réparer les dommages causés aux nombreuses

[1985] FLORI (Jean-Pierre), art. cit., p. 101.
[1986] *Id.*
[1987] Comme l'explique un auteur [PETTY (Corey), « TheDAO: What happened, Who did it, Where do we go? », *Medium* [online], 19 Jun. 2016, https://medium.com/the-bitcoin-podcast-blog/the-dao-what-happened-who-did-it-where-do-we-go-4897d7864e], si la condition est effectuée une fois, alors l'utilisateur malveillant peut extraire le double de ce que son adresse indique qu'il détient. Mais, comme pour « *The DarkDAO* », si les appels de fonctions sont directement introduits les uns dans les autres, alors l'appel de fonction s'appelle essentiellement lui-même et est infini, à condition de détenir toujours un solde supérieur à 0 sur son compte et d'avoir suffisamment de *gas* pour lancer le programme sur la *blockchain* donc. – V. également, MILLER (Andrew), WEN (Zikai Alex), « Hacking Distributed News Feed Scanning Live Ethereum Contracts for the "Unchecked-Send" Bug », *Hacking-Distributed* [on line], 16 Jun. 2016, http://hackingdistributed.com/2016/06/16/scanning-live-ethereum-contracts-for-bugs/.
[1988] Pour plus de précisions sur l'attaque d'un point de vue technique, v. notamment, DAIAN (Philip), « Chasing TheDAO Attacker's Wake », *Phil Does Security* [online], 19 Jun. 2016, http://pdaian.com/blog/chasing-the-dao-attackers-wake/ ; VESSENES (Peter), KRUG (Joey), PETERSON (Dennis), JOHNSON (Nick), « Deconstructing theDAO Attack: A Brief Code Tour », *vessenes.com* [online], 18 Jun. 2016, https://vessenes.com/about/ ; DAIAN (Philip), « Analysis of TheDAO exploit », *Hacking Distributed* [online], 18 Jun. 2016, https://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/.
[1989] Il s'agit du forum des développeurs d'*Ethereum*.
[1990] V., https://www.reddit.com/comments/4onbkj.
[1991] Sur les systèmes autonomes d'identification, *supra* n°s 132 et s.
[1992] PETTY (Corey), art. cit.

victimes[1993]. Certains utilisateurs ont ainsi envisagé différentes approches et l'un d'eux, Peter Vessenes[1994], a notamment proposé deux « *Remediation Approach* »[1995] reposant essentiellement sur une correcte réécriture des transactions.

En parallèle, aussitôt avertie de la situation, la Fondation Ethereum s'est saisie de l'affaire et a officiellement pris en charge le déploiement d'une solution.

§ 2. De l'apparence d'une ré-intermédiation à la remise en cause du système

278. La Fondation Ethereum a pris l'initiative de conduire les débats au sein de la communauté avant, finalement, de prendre position parmi ces amas de propositions et de confrontations, et de décider de soumettre au vote la solution du *fork* (A). Seulement, après avoir été adoptée, celle-ci a fait l'objet de multiples critiques, provenant en particulier des sphères scientifiques et juridiques qui y ont vu une réapparition forcée du tiers de confiance. L'analyse des réactions à la solution du *fork* révèlera la nécessité d'instaurer des règles sécuritaires mais, en parallèle, l'existence d'une crainte d'un retour à l'organisation hiérarchique par le biais d'une centralisation déguisée, qu'il sera inévitable de prendre en considération (B).

A. Entre propositions et confrontations

279. Faire face à l'urgence et protéger les intérêts des utilisateurs : l'accueil *a priori* favorable d'une première intervention modératrice et directrice du développeur. Si le correctif « *DAO v1.1* » qu'avait installé *Ethereum* à la suite de l'alerte lancée sur les réseaux sociaux quelques jours avant l'attaque n'a pas suffi pour supprimer les vulnérabilités exploitables[1996], lorsque l'attaque a été réalisée, la Fondation a immédiatement réagi. Pour cela, Vitalik Buterin a commencé par calmer les tensions et rassurer les contributeurs victimes[1997]. En effet, puisqu'il faut environ vingt-sept jours pour que la DAO « enfant » soit créée, le logiciel utilisé par le pirate ne permettait pas en lui-même à son utilisateur de retirer le montant d'*ethers* « *callbacked* » pendant ce

[1993] HOTTOT (Kevin), « TheDAO : un pirate dérobe 50 millions de dollars, la contre-attaque se prépare », *NextInPact* [en ligne], 22 juin 2016, https://www.nextinpact.com/news/100336-the-dao-pirate-derobe-50-millions-dollars-contre-attaque-se-prepare.htm.
[1994] VESSENES (Peter), préc.
[1995] « Procédure de restauration » [notre trad.].
[1996] VESSENES (Peter), préc.
[1997] BUTERIN (Vitalik), « CRITICAL UPDATE Re: DAO Vulnerability », préc.

délai[1998]. Plus encore, pour s'assurer que l'utilisateur malveillant ne puisse pas retirer le moindre *ether* au-delà de la fenêtre des vingt-sept jours, Vitalik Buterin et ses équipes ont développé et installé un logiciel qui exécute la fonction « *NOrollback* », empêchant toute restauration sur toute la chaîne et jusqu'au bloc n° 1 760 000[1999]. Cette première intervention des développeurs a été poursuivie dans un double objectif, à savoir, gagner du temps pour que la communauté puisse discuter de la suite des opérations et s'assurer que les détenteurs de *tokens* ne perdent pas définitivement leurs chances de récupérer leurs *ethers*.

Par la suite, la Fondation a pris l'initiative de concerter l'ensemble de la communauté sur l'éventualité de modifier le protocole *Ethereum* afin d'enrayer les conséquences de l'attaque. Néanmoins, cette proposition a marqué le début d'un désaccord d'une partie de la communauté et *a fortiori* d'un rejet de la politique menée par la Fondation[2000].

280. Entre volonté de réparer le préjudice et acceptation du risque numérique : la critique de la gouvernance du développeur. Tantôt jugée trop interventionniste, tantôt saluée, la seconde intervention de la Fondation a marqué un schisme entre les contributeurs. La controverse est née principalement de ce que les règles des *blockchains* ne permettent pas, en principe, d'agir à l'encontre du code informatique. Par conséquent, la légitimité d'une nouvelle intervention a été contestée et la question s'est posée de savoir si la communauté allait agir ou non[2001]. Deux groupes se sont formés avec, d'une part, les membres qui souhaitaient corriger le système pour l'avenir en plus de récupérer ce qu'ils avaient perdu et, d'autre part, les membres qui proposaient simplement de ne pas agir puisque, selon eux, l'utilisateur de *The DarkDAO* n'avait fait qu'exploiter une erreur préexistante de *TheDAO*[2002]. En définitive, alors que les premiers prônaient un *fork* de la chaîne, c'est-à-dire une duplication de la *blockchain Ethereum* avec modification, et plus

[1998] BOUQUET (Arthur), « Ethereum : deux forks à venir à la suite d'un hack ? », *Bitcoin.fr* [en ligne], 17 juin 2017, https://bitcoin.fr/ethereum-deux-forks-a-venir-a-la-suite-dun-hack/.
[1999] BUTERIN (Vitalik), « CRITICAL UPDATE Re: DAO Vulnerability », préc. : « *A software fork has been proposed, (with NO ROLLBACK; no transactions or blocks will be "reversed") which will make any transactions that make any calls/callcodes/delegatecalls that reduce the balance of an account with code hash 0x7278d050619a624f84f51987149ddb439cdaadfba5966f7cfaea7ad44340a4ba (ie. TheDAO and children) lead to the transaction (not just the call, the transaction) being invalid, starting from block 1760000 (precise block number subject to change up until the point the code is released), preventing the ether from being withdrawn by the attacker past the 27-day window. This will provide plenty of time for discussion of potential further steps including to give token holders the ability to recover their ether. DAO token holders and ethereum users should sit tight and remain calm*. »
[2000] POLROT (Simon), « To fork or not to fork, telle est la question ! », *Ethereum France* [en ligne], 27 juin 2017, https://www.ethereum-france.com/to-fork-or-not-to-fork-telle-est-la-question/.
[2001] POLROT (Simon), « TheDAO : post mortem », art. cit.
[2002] *Id*.

précisément *élimination*, des effets du piratage[2003], les seconds considéraient les 3,6 millions d'*ethers* détournés comme la conséquence d'une imprudence générale face à la faiblesse dans la conception de l'application[2004]. Sans prendre part aux débats, la Fondation Ethereum a pris l'initiative de la décision et s'est finalement prononcée en faveur d'un *fork*[2005].

Pour cette nouvelle intervention, la Fondation a publié une proposition consistant à appliquer une solution plus souple de *soft fork*, sinon à opter pour une solution de *hard fork* plus radicale[2006]. Techniquement, la méthode du *soft fork* ne vaudrait en principe que pour l'avenir et permettrait uniquement d'immobiliser les transactions, les contrats et donc les fonds réunis dans *TheDAO*. Autrement dit, appliquée à *TheDAO*, cette solution aurait pour effet de « geler » non seulement les *ethers* du pirate, mais également ceux des utilisateurs. Il est cependant évident que le déploiement d'une telle solution ne serait que temporaire, pour permettre à la communauté de gagner du temps dans la recherche d'une meilleure option donnant lieu à une restitution ou, à défaut, à une réparation. À l'inverse, la solution du *hard fork* modifierait l'algorithme originel de la *blockchain* si bien qu'il aurait un effet rétroactif et pourrait permettre de retourner les *ethers* dérobés à leurs détenteurs légitimes, et ainsi réparer les dommages causés par *The DarkDAO*[2007].

Finalement, face au message de l'auteur du détournement, de surcroît signé « *"The Attacker"* », adressé à la communauté et la menaçant d'agir en justice si elle tentait de lui reprendre son « *legitimate and rightful ether* » dont il considérait donc être le propriétaire légitime[2008], le *soft fork* a été voté.

[2003] Définition du *fork*, *infra* n°s 321 et s. – V. également, Annexe n° 11. Schéma d'un *fork* d'une *blockchain*, p. 443.

[2004] PETTY (Corey), art. cit.

[2005] POLROT (Simon), « To fork or not to fork, telle est la question ! », art. cit.

[2006] BUTERIN (Vitalik), « CRITICAL UPDATE Re: DAO Vulnérabilité », préc.

[2007] Pour plus de précisions sur le sujet, v., PETTY (Corey), art. cit. ; https://github.com/ethereum/go-ethereum/pull/2715 (pour l'opinion de la communauté *Ethereum*) ; https://blog.slock.it/what-the-fork-really-means-6fe573ac31dd (pour l'opinion de *Slock*.it) ; https://blog.ethcore.io/attack-on-thedao-what-will-be-your-response/ (pour l'opinion d'*EthCore*).

[2008] V. sur *Reddit*, https://www.reddit.com/r/TheDao/comments/4opba6/apparently_open_letter_from_an_attacker_was/ : « *To TheDAO and the Ethereum community, I have carefully examined the code of TheDAO and decided to participate after finding the feature where splitting is rewarded with additional ether. I have made use of this feature and have rightfully claimed 3,641,694 ether, and would like to thank TheDAO for this reward. It is my understanding that TheDAO code contains this feature to promote decentralization and encourage the creation of "child DAOs". I am disappointed by those who are characterizing the use of this intentional feature as "theft".* [...] *For reference please review the terms of TheDAO: "The terms of TheDAO Creation are set forth in the smart contract code existing on the Ethereum blockchain at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413. Nothing in this explanation of terms or in any other document or communication may modify or add any additional obligations or guarantees beyond those set forth in TheDAO's code. Any and all explanatory terms or descriptions are merely offered for educational purposes and do not supercede or modify the express terms of TheDAO's code set forth on the blockchain; to the extent you believe there to be any conflict or discrepancy between the descriptions offered here and the functionality of TheDAO's code at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413, TheDAO's code controls and sets forth all terms of TheDAO Creation." A soft or hard fork would amount to seizure of my legitimate and rightful ether, claimed legally through the terms of a smart contract. Such*

281. La proposition finale soumise au vote de la communauté : le choix d'une gouvernance pour la confiance. Le *soft fork* étant obligatoirement temporaire, la prise d'une décision définitive s'est imposée. La Fondation Ethereum a mis en place un mécanisme qui a su, dans un premier temps, faire consensus puisqu'il s'est agi d'organiser un vote. Chaque utilisateur a pu prendre part au vote au prorata des *ethers* qu'il détenait ou, en ce qui concerne les utilisateurs appartenant à des sociétés de *pools* de minage, participer au prorata de leur *hashrate*[2009], c'est-à-dire de la puissance de minage de leur nœud[2010]. L'opinion générale, recueillie par le biais de la plateforme *CarbonVote*[2011] s'est finalement prononcée pour le *hard fork*, à la quasi-unanimité des membres[2012]. Les débats précédant le vote ont souligné la volonté de « [corriger] une situation anormale » et injuste eu égard à « l'ampleur des dégâts » et aux « sommes en jeu », ainsi que de limiter les conséquences dommageables du « fiasco de *TheDAO* », et finalement de redonner confiance en prouvant, auprès des médias et des acteurs économiques, qu'une « réelle gouvernance existe dans *Ethereum* » puisque les « problèmes structurels posés par l'exécution de certaines transactions sont examinés et corrigés par la communauté »[2013]. Programmé pour le 20 juillet 2016[2014], le *fork* a donc divisé la *blockchain Ethereum* en deux branches. *Ethereum* (ETH) correspond désormais à la chaîne principale, regroupant la majorité des membres avec l'annulation des effets du *hack*, et *Ethereum classic* (ETC) constitue la chaîne minoritaire utilisée par les partisans du « laissez-faire » sur les *blockchains*[2015]. Puisque le passé ne peut être réécrit, seul le futur change ; le *hacker*

---

fork would permanently and irrevocably ruin all confidence in not only Ethereum but also the in the field of smart contracts and blockchain technology. Many large Ethereum holders will dump their ether, and developers, researchers, and companies will leave Ethereum. Make no mistake: any fork, soft or hard, will further damage Ethereum and destroy its reputation and appeal. I reserve all rights to take any and all legal action against any accomplices of illegitimate theft, freezing, or seizure of my legitimate ether, and am actively working with my law firm. Those accomplices will be receiving Cease and Desist notices in the mail shortly. I hope this event becomes a valuable learning experience for the Ethereum community and wish you all the best of luck. Yours truly, "The Attacker" »

[2009] POLROT (Simon), « To fork or not to fork, telle est la question ! », art. cit.

[2010] « Hashrate : définition et traduction », *Journal du Net* [en ligne], 25 juin 2018, https://www.journaldunet.fr/patrimoine/guide-des-finances-personnelles/1210258-hashrate/. – Pour plus d'informations sur les modalités de vote, v., POLROT (Simon), « Hard fork ou non : faites entendre votre voix ! », *Ethereum France* [en ligne], 11 juill. 2016, https://www.ethereum-france.com/hard fork-ou-non-faites-entendre-votre-voix/.

[2011] V., http://carbonvote.com/.

[2012] 97 % de membres ont voté pour, le reste des voix étant constitué de celle de l'attaquant lui-même ainsi que quelques opposants au principe du *hard fork*.

[2013] POLROT (Simon), « TheDAO : post mortem », art. cit.

[2014] POLROT (Simon), « Le Hard Fork "TheDAO" aura bien lieu, mode d'emploi », *Ethereum France* [en ligne], 19 juil. 2016, https://www.ethereum-france.com/le-hard fork-the-dao-aura-bien-lieu-mode-demploi/.

[2015] *Id.* – POLROT (Simon), « TheDAO : post mortem », art. cit. : « Dans cette chaîne, les conséquences du *hack* ont été annulées pour le futur : à partir du bloc du *fork* (qui a été miné en juillet 2016), les *ethers* qui étaient détenus dans des contrats *TheDAO* sont transférés d'autorité par les mineurs dans un simple contrat de retrait permettant aux détenteurs de DAO-*tokens* de les récupérer. Le contrat *TheDAO* est laissé vide, témoin de l'événement. »

détient toujours les 3,6 millions d'*ethers* détournés mais, n'étant membre que de la *blockchain* ETC utilisée par quelques utilisateurs, la valeur des *ethers* subtilisés a fortement diminuée.

282. La proposition finale soumise au vote de la communauté : un choix démocratique finalement controversé. Alors que la décision de procéder à un vote afin de déterminer la solution définitive à apporter au problème de l'application avait dans un premier temps été positivement accueillie par la communauté, les partisans des deux branches d'*Ethereum* ont à nouveau ouvert le débat.

D'une part, les membres d'*Ethereum Classic* ont souligné, dans leur manifeste, la primauté des principes d'immutabilité et de neutralité de la technologie *blockchain* en rappelant qu' « *Ethereum* est l'ordinateur du monde et personne ne doit pouvoir l'arrêter, le contrôler ou le censurer. Les *smart contracts* doivent être irréversibles. Un "*hard fork*" n'est envisageable que pour corriger des *bugs* réels de la plateforme »[2016]. Ainsi, selon eux, puisque ces principes ne devraient, en principe, souffrir d'aucune exception, la solution du *fork* ne devait être envisageable, quand bien même elle avait été le fruit d'un vote au sein de la communauté[2017].

D'autre part, la Fondation *Ethereum* est à nouveau intervenue, pour indiquer qu'elle ne soutiendrait à l'avenir que la chaîne principale. Seulement, une telle annonce du développeur a eu pour effet de vider de ses membres la chaîne de l'ETC, ce qui a immédiatement fait chuter le cours de l'*ether*. Finalement, dès lors que la Fondation a agi, *Ethereum Classic* a perdu la communauté sur laquelle elle reposait.

Même si, quelques mois plus tard, un des développeurs de *TheDAO* présentait ses excuses à la communauté *Ethereum*[2018], l'affaire a été à l'origine de multiples difficultés, remettant en cause tant les principes de gouvernance adoptés par la Fondation, que la pertinence et la légitimité de la règle « *Code is Law* ». Il convient désormais d'en dresser un état des lieux.

[2016] « Ethereum vs Ethereum Classic », *bitcoin.fr* [online], 27 Jul. 2016, https://bitcoin.fr/ethereum-vs-ethereum-classic/.
[2017] V., « Decentralized Governance », *Ethereum Classic* [online], https://ethereumclassic.github.io/ ; « Transaction Finality », *Ethereum Classic* [online], https://ethereumclassic.
[2018] POLROT (Simon), « TheDAO : post mortem », art. cit. – V. également la présentation de Christoph Jentzsch [format vidéo], https://youtu.be/466bmp6bs9g.

B. Entre nécessité d'instaurer des règles sécuritaires et risques d'une centralisation déguisée

283. Une intervention nécessaire en matière de sécurité. Selon Boris Barraud, l'affaire « *TheDAO* » est lourde d'enseignements et a principalement mené à prendre rapidement la mesure de l'importance d'une sécurité et d'une fiabilité accrue[2019]. L'attaque de *The DarkDAO* a effectivement révélé, au-delà de l'existence d'une « surface d'attaque » considérable au sein de l'application[2020], la gravité des conséquences qu'est susceptible d'entraîner une telle vulnérabilité en matière de *blockchains*. Plus encore, la confiance nécessaire à l'utilisation de la technologie a soulevé la nécessité de mesures destinées à garantir la sécurité des utilisateurs, suggérant que tout dysfonctionnement soit découvert et corrigé afin de limiter leur exposition à une éventuelle exploitation. Ainsi, si la gravité et l'urgence de la situation pourraient suffire à justifier une intervention immédiate des développeurs des *blockchains*, il n'en demeure pas moins qu'ils devront désormais veiller à assurer la sécurité de la conception à, éventuellement, l'utilisation de leur protocole[2021]. Il en va ainsi pour la Fondation Ethereum qui, depuis l'échec de *TheDAO*, a mis en œuvre un système de prévention des failles de sécurité en faisant appel à des auditeurs de code avant chaque nouvelle mise à jour et lancement d'application[2022]. Le développement d'un nouveau protocole, « *Viper* », devrait par ailleurs permettre à la Fondation d'accroître les performances d'*Ethereum* en termes de sécurité[2023].

284. Analyse du débat. Les divers éléments de controverse soulevés lors des débats entre les partisans du *fork* et les partisans du « laissez-faire » intègrent également les enseignements pouvant être tirés de cet évènement[2024]. En effet, en dehors des questions de réparation des *ethers* volés ou de savoir sur qui doit peser le risque de failles technologiques, ce sont, d'une manière générale, les principes des *blockchains* et, en particulier, la mise en œuvre de la gouvernance de *TheDAO*, qui ont montré leurs limites[2025]. Il conviendra donc de présenter ces limites et d'en analyser les tenants et aboutissants.

[2019] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 18.
[2020] POLROT (Simon), « TheDAO : post mortem », art. cit.
[2021] GUILHAUDIS (Élise), art. cit., p. 9.
[2022] *Id*.
[2023] V., https://github.com/ethereum/viper.
[2024] BARRAUD (Boris), « Les blockchains et le droit », art. cit., *loc. cit.*
[2025] LEGEAIS (Dominique), *op. cit.*, n°s 61-63.

285. La portée du principe « *Code is Law* » : un équilibre nécessaire entre neutralité des lois des *blockchains* et confiance des utilisateurs. Selon les détracteurs du *fork*, la règle « *Code is Law* » ne doit subir aucune exception. Si bien qu'exercer un *fork* d'*Ethereum* était, en principe, incompatible avec les fondements originels de la technologie. Plus encore, tout porte à croire que les détracteurs du *fork* auraient agi en dépit tant des préjudices subis par les contributeurs de *TheDAO* que des conséquences négatives en termes de confiance que le système aurait pu connaître, pourvu que la volonté du code informatique soit respectée[2026]. En effet, il est incorrect, d'après eux, de qualifier l'*exploit* d' « *exploit* » ou de « vol » dès lors que « la porte d'entrée n'a pas été verrouillée » [2027]. Ils considèrent somme toute que sans « effraction », le *hacker* n'a fait que respecter les instructions données à l'algorithme[2028].

Toutefois, s'il est question d'interroger la volonté du code informatique, il apparaît admissible de considérer que si les développeurs n'avaient initialement pas prévu de telles conséquences, cela signifie qu'elles n'étaient pas voulues. La volonté du code informatique est avant tout celle de son codeur[2029]. Un programme informatique est le fruit de l'interprétation du programmeur qui attribue un sens à une réalité pour ensuite la traduire en lignes de code dans un langage spécifique. Si bien que la vulnérabilité d'un algorithme est le résultat d'une erreur, d'un oubli. Bien que la question de la responsabilité du développeur en tant que concepteur de l'application aurait pu se poser et qu'un juge étatique aurait sans doute procédé à une juste réparation des victimes[2030], force est de constater que cette vulnérabilité n'est, à l'évidence, jamais la transcription de la volonté d'un code informatique. Il apparaît néanmoins que si un registre, dont la caractéristique principale est l'immuabilité, permettait de commettre une entorse telle qu'un « *hard fork* », ce registre serait susceptible d'en tolérer de nouvelles[2031].

Simon Polrot constatait d'ailleurs au moment du débat qu' « à partir du moment où une exception aura[it] été faite pour *TheDAO*, qu'on aura[it] modifié l'état de la *blockchain* pour corriger les effets d'un piratage, la brèche sera[it] ouverte ». Ce constat n'est pas sans soulever de nombreuses difficultés. Il prête d'autant plus à discussion qu'il semble que la certitude de l'impunité puisse également être une source de méfiance, encourageant à porter atteinte au système, à son fonctionnement, à la confidentialité ou à l'intégrité des données qu'il renferme. Une telle « brèche » non résolue pourrait, de

[2026] BARRAUD (Boris), « Les blockchains et le droit », art. cit., *loc. cit.*
[2027] *Id.*
[2028] *Id.*
[2029] Sur la confiance initiale et sur la nature irrémédiablement humaine des dysfonctionnements, *supra* n° 259 et s.
[2030] Sur la recherche et la mise en œuvre de la responsabilité, *supra* n°s 262 et s.
[2031] GUILHAUDIS (Élise), art. cit., *loc. cit*.

surcroît, nuire à au développement voire au déploiement de la technologie, notamment si les victimes ne peuvent obtenir réparation des préjudices en résultant. Par ailleurs, les utilisateurs ne sont, en principe, pas censés vérifier le code informatique d'une application qui leur est présentée, et même *vendue,* comme étant fiable et sécurisée. Cette question est pourtant elle-même sujette à débat puisque certains considèrent que, dans le cadre d'une *blockchain,* chacun reste responsable de ses propres choix[2032]. Cela n'empêche toutefois pas qu'une organisation, qu'elle soit économique, politique ou sociale, dès lors qu'elle est entachée d'une vulnérabilité ou d'un dysfonctionnement, doive, pour l'intérêt commun, être corrigée.

Simplement, dans un système volontairement neutre et immuable, l'enjeu réside dans la conciliation des intérêts en présence. Ce constat mène à interroger les diverses initiatives de la Fondation Ethereum au cours de l'épisode *TheDAO,* interventions qui ont pu apparaître, pour une minorité du moins, quelque peu intrusive.

286. Le rôle du développeur dans la gouvernance de la chaîne : l'importance de fixer le cadre des actions pouvant être menées par chacun. En agissant pour la fiabilité et la légitimité de la chaîne de blocs, tout en s'efforçant de donner à la communauté les moyens de s'exprimer, de débattre et enfin de déterminer l'issue du problème, la Fondation s'est glissée dans un rôle de médiateur exécutant la volonté du plus grand nombre.

Cependant, rien ne garantit qu'elle assumera de remplir cette mission dans la durée. Aussi, dans quelles circonstances son intervention pourra éventuellement être justifiée ? *A contrario,* dès lors que la Fondation est intervenue pour trouver une solution à la faiblesse de *TheDAO,* serait-elle susceptible, dans d'autres cas, de se voir reprocher une abstention si elle décidait de ne pas intervenir ? Par ailleurs, l'objectif poursuivi est également fondamental puisque, si la Fondation a organisé le vote de la communauté pour annuler un détournement de 3,6 millions d'*ethers,* quelle est ou sont la ou les condition(s) pour qu'un vol soit par la suite annulé au même titre que celui de *TheDAO* ? Plus encore, les conditions dans lesquelles le vote a été organisé, et en particulier le choix de l'électorat, a constitué un point capital du débat[2033]. En effet, les détracteurs du *fork* ont

[2032] POLROT (Simon), « TheDAO : post mortem », art. cit. : « Chacun doit être responsable de ses actes. Les personnes qui ont financé *TheDAO* n'ont pas lu le code correctement et leur perte a été causée par leur inconséquence. Ceux qui l'auraient lu correctement auraient pu anticiper le piratage. Dans tous les cas, l'investissement dans *TheDAO* était un investissement extrêmement risqué et tous les investisseurs avaient été prévenus. Si l'on corrige les effets du piratage, les investisseurs n'apprendront pas les leçons de leur erreur et réinvestiront dans un fonds non-sécurisé. »
[2033] *Id*.

fait valoir que ne laisser l'opportunité d'exprimer leur opinion qu'aux détenteurs de *tokens* dans *TheDAO*[2034], autrement dit qu'aux utilisateurs « victimes », en vue d'une décision qui engageait la communauté *Ethereum* entière puisqu'il s'agissait d'un *fork* de la chaîne complète, était somme toute injuste.

Bien que ce dernier point mériterait d'être discuté puisque, à l'évidence, le *fork* n'a entraîné aucune modification en dehors de la correction de la faille de *TheDAO* et de ses impacts, il résulte de ces constatations que si la communauté peut être amenée à prendre une décision, il est nécessaire que son initiative soit encadrée. La sécurité, et donc l'insécurité juridique, est au cœur de la réflexion[2035]. En proie à des effets pervers pouvant avoir d'importantes conséquences en termes de confiance, ces interrogations suggèrent de définir des règles encadrant les potentielles interventions des différents acteurs de la technologie, si possible dès la conception du système. Pour être efficace, cette régulation doit, à notre sens, établir les critères essentiels d'une intervention du développeur à la fois juste et préservant la neutralité de principe de la technologie. Elle pourrait ainsi fixer, par exemple, les conditions d'intervention du développeur, lesquelles peuvent éventuellement prendre en compte les requêtes des membres de la communauté ou des membres concernés et exiger un quorum, mais elle pourrait également déterminer l'objectif poursuivi par l'intervention ainsi que ses limites, et enfin les modalités de prise de décision au sein de la communauté suivant que les solutions proposées ont un impact sur une partie ou sur l'ensemble de la *blockchain* considérée.

287. De la fixation des limites de la gouvernance à la préservation de la confiance : un juste équilibre à trouver. À de nombreuses reprises, à travers ses interventions pour tenter de limiter les atteintes portées au système et à ses utilisateurs, la Fondation Ethereum a pu donner l'impression de réinstaurer une hiérarchie, à l'image de celles qui fondent les systèmes centralisés. Si elle n'a toutefois jamais pris position dans le débat, ni même participé au vote[2036], cette réaction n'exclut pas la prise en compte des inquiétudes révélées vis-à-vis d'une centralisation déguisée, en particulier en ce qui concerne l'organisation de la gouvernance des *blockchains*. Toute ré-intermédiation pourrait en effet remettre en cause l'intégrité et les principes du système des *blockchains*. Aussi la question n'est-elle plus de savoir si l'instauration d'une gouvernance pourrait être justifiée, mais plutôt de savoir comment la mettre en œuvre. Dans le domaine des *blockchains*, les modalités de gouvernance constituent depuis quelques années une

[2034] *Id.*
[2035] *Id.*
[2036] *Id.*

problématique fréquemment soulevée. Si l'auto-régulation a pour le moment posé ses propres limites, qu'en serait-il, à l'inverse, avec une régulation centralisée ? Une chaîne centralisée[2037] contreviendrait aux diverses caractéristiques des *blockchains*, non seulement en termes de décentralisation mais également de sécurité et d'intégrité, lesquelles sont assurées par son fonctionnement distribué. En revanche, elle aurait probablement contribué à simplifier le processus de correction du détournement de *TheDAO*. En effet un gestionnaire central aurait engagé sa responsabilité et, sommé de solutionner le problème, il aurait eu le pouvoir de prendre et d'exécuter instantanément une décision[2038]. Alors que cette solution pourrait de prime abord représenter *la* solution aux problèmes de gouvernance des protocoles, elle apparaît davantage comme une nouvelle forme de privatisation.

Section 2. Les différentes formes de privatisation de la technologie : entre gestion facilitée et réinstauration d'une organisation hiérarchique

288. Le choix de la gouvernance se révèle déterminant, tant en ce qui concerne l'organisation que le déploiement de la technologie *blockchain*. Il peut tantôt constituer un risque de ré-intermédiation et avoir des répercussions en termes de fiabilité, tantôt permettre d'assurer aux utilisateurs une certaine maîtrise des risques. Il n'empêche que, quelle que soit la forme de la gouvernance choisie, celle-ci aura un impact sur la confiance algorithmique qui sera instituée. En parallèle, l'histoire de l'innovation technologique témoigne de l'intérêt croissant pour le fait technique et des nombreuses tendances à l'appropriation des technologies afin d'en tirer un profit personnel[2039], si bien qu'une analogie semble s'établir entre le développement actuel de la *blockchain* et le développement qu'a connu Internet ces dernières années[2040]. Partant du constat que l'innovation n'a pas résisté à la privatisation progressive du web, il importera de définir les concepts nés de la mutation de la *blockchain* en une chaîne centralisée. Un panorama des chaînes désormais disponibles permettra notamment d'illustrer l'étendue des divergences résultant de la fermeture des chaînes de blocs (§ 1). Il conviendra ensuite d'examiner les conséquences d'une privatisation en matière de *blockchains* (§ 2).

[2037] *Infra* n°s 294-295, *i.e*. chaîne privée ou de consortium.
[2038] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 18. – GUILHAUDIS (Élise), art. cit., p. 9.
[2039] SMYRNAIOS (Nikos), *Les GAFAM contre l'internet*, éd. Ina, 2017, pp. 7-9.
[2040] *Id.*

§ 1. Analyse de la mutation de la *blockchain* en une chaîne centralisée : fermeture et autres divergences

289. La typologie actuelle révèle deux types de *blockchains*, à savoir, la chaîne « ouverte » au public, telle qu'originellement conçue (A), et les chaînes privées, « contrôlées » et « de consortium », postérieurement créées (B). Un examen approfondi des techniques et capacités proposées par chacune d'elles permettra non seulement de les différencier, mais également de les comparer.

A. Blockchain publique

290. Un bien avant tout commun, ouvert en lecture et en écriture. « Publique » ou « ouverte », la *blockchain* dans cette configuration s'apparente à un logiciel libre, publiquement accessible sur le web et appartenant à tous les membres de l'écosystème[2041]. D'ailleurs, les codes sources du protocole de la *blockchain* sont publics de sorte qu'elle est « ouverte en écriture et en lecture »[2042]. Chacun a ainsi la possibilité, gratuitement, d'écrire sur la chaîne et de lire son contenu[2043]. Par ailleurs, puisque le protocole appartient à ses membres[2044], il n'est guère étonnant que ces derniers puissent non seulement participer au processus de validation des blocs, mais également contribuer, en fonction de leurs connaissances et facultés, à son développement en proposant des modifications ou des mises à jour du protocole de base[2045]. À l'origine d'une véritable logique collaborative, l'essentiel de ce travail effectué par la communauté est harmonisé par le biais de plateformes de communication et d'échanges, à l'instar de *GitHub* pour les protocoles *Bitcoin* et *Ethereum*. Ces dernières années, *Bitcoin* a connu de multiples améliorations de son protocole, lequel est passé de la version 0.1 à 0.18.1[2046]. De plus, une *blockchain* publique ne comporte en principe aucun système de révocation de clés[2047], si bien que son accès est et reste libre. En définitive, au sein d'une *blockchain* telle que Satoshi Nakamoto l'avait imaginée, chaque membre est titulaire de droits égaux et aucun

[2041] COIFFARD (Didier), « Entretien du mois : La Blockchain a un sens pour répartir une partie de la confiance en rendant une information infalsifiable mais cette confiance est très en deçà de celle conférée par le notaire », *RLDC* 2017/4, n° 147.
[2042] DELAHAYE (Jean-Paul), « Qu'est-ce qu'une blockchain ? », *SPS* [en ligne], 11 oct. 2017, http://www.scilogs.fr/complexites/quest-quune-blockchain/.
[2043] GUILHAUDIS (Élise), art. cit., p. 2.
[2044] FÉNÉRON PLISSON (Claire), « La blockchain, un bouleversement économique, juridique voire sociétal », *Information, données & documents* 2017/3, vol. 54, p. 21.
[2045] GUILHAUDIS (Élise), art. cit., *loc. cit.*
[2046] V., https://bitcoin.org/fr/telecharger.
[2047] DEVILLIER (Nathalie), « Jouer dans le "bac à sable réglementaire" pour réguler l'innovation disruptive : le cas de la technologie de la chaîne de bloc », *RTD com.* 2017, p. 1037.

privilège d'accès ou de transaction n'est consenti, si bien que toute forme d'organisation hiérarchique est proscrite[2048] au profit d'un système entièrement P2P et décentralisé[2049].

291. Autonomie et décentralisation, garanties d'une sécurité et d'une fiabilité accrue. La technologie suit ses propres règles[2050], c'est-à-dire celles inscrites dans son protocole eu égard au principe « *Code is Law* »[2051]. En dépit des inconvénients qui peuvent parfois résulter de la règle du « pseudonymat » garanti sur ce type de *blockchain*[2052] ou celles de l'immuabilité et de la décentralisation[2053], c'est sa capacité à respecter et à faire respecter les principes originels qui assure l'extrême sécurité du système. D'une part, aucun tiers de confiance n'intervient puisque l'écosystème est auto-suffisant et parvient, à travers le travail de ses mineurs, à créer une « vérité partagée » et immuable[2054]. D'autre part, aucun tiers, y compris de confiance, ne peut, en principe, intervenir puisque le protocole est programmé de sorte à ne supporter aucune modification ou suppression d'information. Comme le souligne Sylvie de Thésut Dufournaud, la *blockchain* publique consiste en « (i) une technologie Open source (MIT, GPL V3 OU LGPV3...) fonctionnant sur ; (ii) un réseau complètement ouvert et accessible à tout internaute et mineur ; (iii) une cryptomonnaie (cybermonnaie), valeur d'échange pour l'ensemble des transactions et le minage ; (iv) un registre consultable par tout internaute, retranscrivant l'intégralité des transactions et attestant de la validité de la chaîne de blocs »[2055].

Nombre de pros-*blockchain* défendent la *blockchain* publique comme étant *la* véritable *blockchain*, au sens premier et original de la technologie voulue par Satoshi Nakamoto, laquelle était une chaîne décentralisée, distribuée, transparente et immuable[2056]. Par ailleurs, dans un souci de simplicité mais également d'efficacité,

---

[2048] LE TROCQUER (Anne-Hélène), « Blockchain, gouvernance d'entreprise et infrastructures de marchés », *in* « Dossier : Blockchain, une révolution juridique ? », *RLDA* 2017/9, n° 129.
[2049] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., n° 5.
[2050] *Id.*
[2051] *Supra* n° 234. – LESSIG (Lawrence), « Code Is Law: On Liberty in Cyberspace », *Harvard Magazine* [online], 1st Jan. 2000, https://www.harvardmagazine.com/2000/01/code-is-law-html.
[2052] Sur les difficultés engendrées par la pseudonymisation des utilisateurs et des données inscrites, *supra* n°s 115-116 ; 117 et s. (pour une étude détaillée). – BERBAIN (Côme), « La blockchain : concept, technologies, acteurs et usages », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 6 ; LE TROCQUER (Anne-Hélène), « Blockchain, gouvernance d'entreprise et infrastructures de marchés », art. cit., *loc. cit*.
[2053] Sur les incohérences entre *blockchain* et droit en termes d'immuabilité et de décentralisation, respectivement, *supra* n°s 183 et s. et 229 et s.
[2054] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., *loc. cit.*
[2055] DE THÉSUT DUFOURNAUD (Sylvie), « Les blockchains de consortium », *in* « Dossier : Blockchain, une révolution juridique ? », *RLDA* 2017/9, n° 129.
[2056] FÉNÉRON PLISSON (Claire), art. cit., p. 7.

l'ensemble des développements précédents ont été rédigés sous le prisme de la *blockchain* originelle qui est une *blockchain* publique.

292. Bien commun, décision commune. La pratique des *blockchains* a pu démontrer que la décentralisation n'exclut pas la mise en œuvre de solutions à visée sécuritaire. Il a en a effectivement été ainsi lors de l'affaire « *TheDAO* ». À l'origine d'un vif débat au cours duquel l'efficacité du fonctionnement P2P décentralisé de la technologie *blockchain* a été mise en doute[2057], l'intervention de la Fondation Ethereum a témoigné d'une ferme intention de maintenir la logique collaborative qui a donné naissance à la technologie. Le choix opéré est le produit de la volonté commune des utilisateurs, et ses conséquences sont l'aboutissement d'une décision prise par la communauté, pour la communauté[2058].

Il en va ainsi également en ce qui concerne *Bitcoin*. En effet, la chaîne de Satoshi Nakamoto a, à de nombreuses reprises, procédé par vote en utilisant le plus souvent les règles de majorité pour prendre une décision. Ces initiatives s'efforcent de soumettre aux participants des propositions. Elles visent la résolution de vulnérabilités détectées dans le système, tel qu'en 2012 lorsqu'un *hard fork* a été voté pour mettre fin à de multiples problèmes de transactions multi-signatures, lequel a réuni 55% des voix de la communauté, ou plus récemment en 2015 pour des raisons de sécurité du réseau. Mais elles ont pour but également de décider des nouvelles fonctionnalités et mises à jour à appliquer au protocole, lesquelles prennent la forme de BIP (*Bitcoin Improvement Proposal*) intégrées à la chaîne par le biais de *soft forks*, voire de *hard forks* pour les plus importantes[2059].

293. La philosophie de la *blockchain* publique à travers les théories du contrat social : une gouvernance de la majorité et de l'égalité juridique. Si Rebecca MacKinnon théorise une nouvelle entrée de l'Homme dans l'état de nature lorsqu'elle

[2057] Sur les étapes de l'affaire, *supra* n°s 272-282 et s. ; sur les éléments évoqués lors du débat et leur analyse, *supra* n°s 284-287.
[2058] LINCOLN (Abraham), *The Gettysburg Address*, M.T. Sheahan, 19 Nov. 1863 : « […] *government of the people, by the people, for the people* ». Disponible sur le site de la Bibliothèque du Congrès des États-Unis [https://www.loc.gov/, Home > « Prints & Photographs »], sous le numéro d'identification : cph.3g12220. – Const., 4 oct. 1958, *JORF*, 5 oct. 1958, art. 2, al. 5.
[2059] « Hard fork / soft fork », *bitcoin.fr* [en ligne], 27 juin 2016, https://bitcoin.fr/hard fork-soft fork/ : « De nombreux "*soft fork*" ont déjà été activés dans *Bitcoin*, notamment les BIP [*(*Bitcoin Improvement Proposal)* : proposition d'amélioration du protocole Bitcoin] 16 , 34 , 65 , 66 , 68 , 112 et 113). La procédure a été codifiée dans le BIP9. » – V. également, github.com > bips > bip-0016.mediawiki, https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki.

évoque l'âge hobbien du cyberespace[2060], contrairement à Thomas Hobbes, John Locke considère qu'aucun gouvernement légitime ne saurait être absolu[2061]. La raison d'être de la technologie *blockchain* est d'incarner ce consentement mutuel commun à Thomas Hobbes et à John Locke, qui permet aux Hommes de quitter un état de nature non viable, d'oppression et de domination, tout en leur laissant le soin de fixer en amont les règles de vie en société[2062], et finalement de devenir cette nouvelle entité de confiance qui pourrait protéger les « netziens », c'est-à-dire les citoyens du Net, autant que les guider[2063]. Or, loin de la théorie de l'autorité absolue, John Locke propose justement l'institution d'un gouvernement fondé sur la règle de la majorité auquel, l'Homme, sous condition, se soumet et consent à abandonner une partie de ses droits[2064]. De plus, la légitimité du corps politique en place découle, selon lui, du « *trust* », c'est-à-dire du consentement du peuple, autrement dit de la confiance de la communauté qui lui est attribuée[2065].

Selon Jean-Jacques Rousseau, « l'obéissance à la loi qu'on s'est prescrite est liberté ». L'Homme doit toutefois veiller, d'une part, à instaurer une égalité juridique entre les Hommes et, d'autre part, à ne pas s'abandonner à un gouvernement qui ne serait autre que le fruit d'un rapport de force déguisé, mais peut toutefois aliéner ses droits à condition que le contrat préserve la liberté de chacun. Le modèle de John Locke consent ainsi que, dans l'hypothèse où « le gouvernement ne respecte pas les lois naturelles […], les hommes [puissent] opposer leur droit de résistance à l'oppression »[2066]. Force est de constater que, dans son fonctionnement, la *blockchain* publique tend à respecter ces principes empruntés aux théories du contrat social et, *a fortiori*, à reproduire les conditions propices à l'obtention du consentement mutuel nécessaire à l'institution d'une confiance algorithmique.

Les nouvelles formes de *blockchains* apparues ces dernières années se sont révélées très différentes dans leur fonctionnement. Ces divergences laissent suggérer que ces principes ne seraient dès lors plus observés, ce qui laisserait entière la question de l'objectif de ces nouveaux protocoles si ce n'est de pouvoir mettre fin à l'oppression et à

[2060] MACKINNON (Rebecca), *Consent of the Networked: The Worldwide Struggle for Internet Freedom*, ed. Basic Books, 2012, cité dans : GUILHAUDIS (Élise), art. cit., *loc. cit.*
[2061] TERESTCHENKO (Michel), *Enjeux de philosophie politique moderne : les violences de l'abstraction*, éd. PUF, 1992, pp. 64-65.
[2062] GUILHAUDIS (Élise), art. cit., *loc. cit*.
[2063] Pour plus de détails sur le sujet, v., MACKINNON (Rebecca), *Consent of the Networked: The Worldwide Struggle for Internet Freedom, op. cit.*
[2064] *Id.*
[2065] *Id.*
[2066] V., *lemondepolitique.fr*, Cours > Politique > Philosophie politique > Déclin de l'absolutisme > John Locke.

la domination de l'état de nature. Il est essentiel, pour répondre à ces questions, de parvenir à définir les concepts qui seront utilisés.

B. Blockchains privatisées

294. Un réseau *blockchain* local, fermé et maîtrisé : la *blockchain* « privée ». Les règles de fonctionnement d'une *blockchain* dite « privée » sont fondamentalement différentes de celles de la *blockchain* originelle. Si la *blockchain* publique était Internet[2067], la *blockchain* privée serait Intranet[2068]. Ainsi, tel un réseau local entièrement fermé et centralisé[2069], la version privée de la chaîne de blocs est intégralement régie par un seul et unique administrateur, déterminé, qui fixe les règles de fonctionnement[2070] et délivre les autorisations d'accès au cas par cas[2071]. Son autorité s'étend au contrôle des droits de lecture, d'écriture, de modification, et même de validation du registre[2072].

En règle générale, les nœuds sont également contrôlés par un seul et même acteur. Or, celui qui maîtrise les nœuds d'une *blockchain* maîtrise la validation du contenu des inscriptions et leur enregistrement. Cet acteur est par conséquent l'unique administrateur du système. De cette manière, il apparaît admissible de considérer que le tiers de confiance refait son apparition, non à travers l'algorithme en principe neutre et immuable du protocole, mais par le biais de la gouvernance centralisée de la *blockchain* privée, laquelle rompt définitivement avec la philosophie du réseau P2P des *blockchains* traditionnelles. Plus encore, dès lors que l'administrateur de la chaîne privée dispose, *via* son contrôle absolu des inscriptions, de la faculté de modifier n'importe quel bloc ou opération inscrit(e) sur la *blockchain*, se pose un problème de fiabilité de nature à remettre en question l'objectif initialement poursuivi par la technologie.

Finalement, le seul intérêt de cette utilisation semble résider dans l'association d'outils d'optimisation des procédures internes de réseaux locaux, à l'instar des réseaux de groupes de sociétés ou de services appartenant à une même entreprise, et de mécanismes de défense contre les risques opérationnels. Selon une auteure, les *blockchains* « privées » ne constituent qu' « un outil d'enregistrement immédiat et [de]

[2067] Attention toutefois, Internet est un réseau centralisé. La *blockchain* constitue un réseau entièrement décentralisé, en principe. Le parallèle effectué porte donc davantage sur l'idée d'ouverture du réseau plutôt que sur la question de la centralisation/décentralisation.
[2068] GUILHAUDIS (Élise), art. cit., p. 2.
[2069] BEAUDEMOULIN (Nathalie) *et al*., « Les enjeux de la Blockchain pour la Banque de France et l'Autorité de Contrôle prudentiel et de Résolution (ACPR) », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 31.
[2070] BERBAIN (Côme), art. cit., p. 6.
[2071] LE TROCQUER (Anne-Hélène), « Blockchain, gouvernance d'entreprise et infrastructures de marchés », art. cit., *loc. cit*.
[2072] GUILHAUDIS (Élise), art. cit., *loc. cit.*

partage d'informations et de transactions »[2073]. Instrument des organismes privés pour leurs systèmes B2B et, éventuellement, B2C, la version privée de la technologie consiste en une base de données traditionnelle, dotée de fonctionnalités de sécurisation par cryptographie[2074]. Insuffisamment conciliante pour être implémentée à grande échelle, cette solution apparaît éloignée de l'idée originelle de Satoshi Nakamoto, de sorte qu'il pourrait être raisonnable d'interroger la qualification de « *blockchain* » la concernant.

295. Entre vraie et fausse *blockchain*[2075] : la *blockchain* « de consortium », un réseau *blockchain* partiellement ouvert, flexible et maîtrisable. À mi-chemin entre *blockchain* publique et *blockchain* « privée », est née une *blockchain* hybride, qui consiste en un protocole dont les règles d'ouverture et de fonctionnement sont déterminées par une personne ou un groupe de personnes. De la rédaction de son protocole dépendra finalement son degré d'ouverture et d'autonomie.

Le plus souvent, une ou plusieurs personnes ou organisations régulent la *blockchain* de consortium et fixe dès sa conception les droits de lecture, d'écriture, et de modification des blocs de la chaîne[2076]. Appelée également « *permissioned blockchain* »[2077], celle-ci est dite « ouverte en accès, mais fermée en écriture »[2078]. En fonction des règles mises en œuvre, sa nature partiellement décentralisée[2079] pourra prendre la forme d'une administration centralisée ou d'une gouvernance plurielle, plus ou moins équilibrée[2080]. D'ailleurs, la modification du protocole est en principe possible et s'exécutera selon un consensus fondé sur un système d'attribution de voix prédéfini. En définitive, le caractère majoritairement public ou privé d'une *blockchain* hybride n'est pas fixé et sa détermination relèvera d'un examen au cas par cas des règles que renferme son algorithme.

Malgré tout, l'intérêt de cette configuration est de pouvoir profiter de l'ensemble des avantages délivrés par la *blockchain* publique, notamment en matière de sécurité et de collaboration, tout en aménageant la possibilité pour ses administrateurs d'inclure des fonctionnalités de contrôle, d'identification des utilisateurs et éventuellement

---

[2073] BEAUDEMOULIN (Nathalie) *et al*., art. cit., *loc. cit.*
[2074] *Id*., p. 31.
[2075] GUILHAUDIS (Élise), art. cit., p. 2 ; Rapp. AN n° 1092, rapp. Sénat n° 584, 20 juin 2018, Comprendre les blockchains : fonctionnement et enjeux de ces nouvelles technologies, présenté par Valéria FAURE-MUNTIAN, Claude DE GANAY, et Ronan LE GLEUT, au nom de l'office parlementaire d'évaluation des choix scientifiques et technologiques.
[2076] FÉNÉRON PLISSON (Claire), art. cit., p. 21.
[2077] FLORI (Jean-Pierre), art. cit., p. 98.
[2078] DEVILLIER (Nathalie), art. cit., p. 1037.
[2079] LE TROCQUER (Anne-Hélène), « Blockchain, gouvernance d'entreprise et infrastructures de marchés », art. cit., *loc. cit*.
[2080] BEAUDEMOULIN (Nathalie) *et al*., art. cit., *loc. cit.*

d'adaptation des paramètres en fonction du cas d'utilisation[2081]. Par exemple, les administrateurs d'une *blockchain* de consortium peuvent interdire l'accès au protocole à certains acteurs tels que des concurrents, ou au contraire en ouvrir l'accès mais limiter la lecture pour offrir un service consommateurs sous la forme d'une architecture B2C[2082]. Les cas d'utilisation sont, en l'état de l'art, multiples. Plus de 200 institutions financières mondiales ont pu ainsi se réunir pour créer le « C*onsortium R3* » en optant pour cette forme de *blockchain*. Selon elles, l'avantage de la *blockchain* hybride est d'avoir « un acteur neutre qui est là pour aiguiller tout le monde » tout en gardant la maîtrise de sa gouvernance[2083]. Pour imposer une identification effective à ses utilisateurs, la *blockchain* financière *Ripple* utilise également ce mode de gouvernance. Ouvert en accès, son protocole, à la différence de *Bitcoin*, permet toutefois la publicité des informations de transactions, mais pas des informations de paiement[2084].

296. Privatisation et inévitable réinstauration d'une organisation hiérarchique. La mutation de la *blockchain* publique a eu pour effet de réédifier la logique hiérarchique des sociétés centralisées. Même exercé de manière multiple sous la forme de consensus, le contrôle par une ou des autorités centralisatrices du pouvoir de décision fait naître, à nouveau, ce tiers de confiance, cet intermédiaire que la *blockchain* originelle s'emploie à surpasser[2085]. Toutefois, la *blockchain* publique pourrait quant à elle condamner son propre déploiement si elle persiste à poursuivre un idéal d'autonomie inconditionnelle et à ne pas rapidement prendre la mesure de l'importance d'instaurer un minimum de gouvernance.

Alors que l'utilité de la *blockchain* « privée » interroge et que la *blockchain* publique semble condamnée à demeurer limitée voire à sacrifier ses promesses d'égalité, d'intégrité et de fiabilité au profit d'une recentralisation du pouvoir, il convient d'évaluer les conséquences de ces utilisations divergentes de la technologie.

[2081] GUILHAUDIS (Élise), art. cit., *loc. cit.* – BERBAIN (Côme), art. cit., p. 6.
[2082] FÉNÉRON PLISSON (Claire), art. cit., *loc. cit*.
[2083] DALIBARD (Frédéric), cité dans PERREAU (Charlie), « R3, le consortium blockchain qui divise les banques », *Journal du Net* [en ligne], 18 juill. 2017, https://www.journaldunet.com/economie/finance/1196309-r3-le-consortium-blockchain-qui-divise-les-banques/.
[2084] BERBAIN (Côme), art. cit., p. 7.
[2085] BEAUDEMOULIN (Nathalie) *et al*., art. cit., *loc. cit*.

§ 2. Analyse des conséquences de la privatisation des *blockchains* par des entités centralisées : contrôle et déséquilibres

297. Une *blockchain* est, par nature, un réseau décentralisé et distribué, tendant vers l'autonomie. Par conséquent, lorsque de nouvelles formes de *blockchains* émergent de la pratique et que leur mise en œuvre mène à réduire, voire à faire disparaître, ces caractéristiques originelles pour instaurer une gouvernance contrôlant son développement, des questions se posent. D'ailleurs, l'analogie qui semble s'établir entre le développement actuel de la *blockchain* et le développement qu'a connu Internet ces dernières années[2086] tend à démontrer que l'innovation ne parvient somme toute pas à résister à la privatisation progressive du web[2087]. Toutefois, au-delà d'identifier la manière dont la technologie est, malgré sa philosophie, elle aussi progressivement appréhendée par d'influentes entreprises, il importera d'évaluer, d'une manière générale, l'impact de la privatisation imposée à la technologie. Cette évaluation permettra notamment de soulever une double difficulté tenant, d'une part, dans la création de monopoles économiques (A) et, d'autre part, dans la création de modèles d'administration centralisée (B).

A. La création de monopoles économiques

298. Dessein commun, avenir commun ? S'inspirant de l'idéologie originelle d'Internet et du cyberespace selon laquelle « *no borders, no banks* » (« ni frontières, ni banques »)[2088], l'écosystème *blockchain* met en avant des aspirations libérales avec l'objectif de parvenir à se détacher de l'emprise des tiers de confiance traditionnels et corrompus[2089], mais également d'abolir les pratiques monopolistiques voire oligopolistiques[2090]. Les utilisateurs d'Internet ont, à de multiples reprises, manifesté une certaine préférence pour une organisation reposant sur le réseau plutôt que « l'organisation pyramidale » classique, comme en témoignent la création du web ainsi que, plus tard, le déploiement des plateformes *Uber*, *Airbnb* ou encore *BlaBlaCar*[2091].

[2086] *Id.*
[2087] SMYRNAIOS (Nikos), *Les GAFAM contre l'internet*, éd. Ina, 2017, pp. 7-9.
[2088] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 6.
[2089] *Ibid.*, pp. 6-7.
[2090] BARSAN (Iris M.), « Blockchain - Blockchain et propriété intellectuelle », *Comm. com. électr*. 2020, n° 4, étude 7, n° 13.
[2091] MERINDOL (Valérie), « Les entreprises de la nouvelle économie sont-elles vraiment plus efficaces ? », *The Conversation* [en ligne], 4 sept. 2017, https://theconversation.com/les-entreprises-de-la-nouvelle-economie-sont-elles-vraiment-plus-efficaces-78977. – V. également, OST (François), VAN DE KERCHOVE (Michel), « De la pyramide au réseau ? Pour une théorie dialectique du droit », *RID comp*. 2003, n° 55-3, pp. 730-742.

Conscients que le réseau n'a pas encore réussi à s'imposer face à la pyramide du pouvoir établie au sein de ces sociétés, les différents initiateurs de la *blockchain* ambitionnent d'instituer un nouveau modèle de confiance[2092].

Développé grâce à l'association d'un protocole décentralisé, d'une « approche communautaire » avec une gouvernance, et *a fortiori* une confiance placée dans la multitude, et d'une volonté de « [dépasser] les individualités »[2093], le modèle des *blockchains* s'efforce de mettre en place un cercle vertueux créateur de confiance. Cette association permet de construire une forme de lien social capable de remplacer tout modèle d'autorité centralisée[2094], si bien que tout porte à croire que ce réseau de blocs aurait pu réussir à instituer une véritable confiance algorithmique tel que le réseau Internet l'avait envisagé[2095].

En effet, détourné de sa finalité initiale d'un « Internet totalement libre et dérégulé », se passant des tiers de confiance[2096], il a été pour cette même raison entièrement privatisé[2097]. Au dire de Nikos Smyrnaio, « l'Internet originel n'a pas été conçu pour un usage commercial »[2098]. Pourtant il est devenu ce qui constitue sûrement à l'heure actuelle le plus important marché oligopolistique du début du siècle[2099]. En conséquence, son développement décentralisé a été immobilisé afin d'en faire un « espace réintermédié », réglementé, payant, sous la gouvernance exclusive des quelques acteurs du secteur[2100]. Or, face au soudain engouement des mêmes acteurs qui ont privatisé le web[2101], nombre d'auteurs craignent que la *blockchain* puisse également être réduite à un usage purement commercial[2102].

[2092] BARRAUD (Boris), « Les blockchains et le droit », art. cit., *loc. cit.*
[2093] *Id.*
[2094] Pour plus de précisions sur le sujet, v. notamment, RIFKIN (Jeremy), *La troisième révolution industrielle : Comment le pouvoir latéral va transformer l'énergie, l'économie et le monde*, éd. Les liens qui libèrent, 2012.
[2095] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 7.
[2096] CARRÉ (Marion), LASRY (Julia), MECHERRA (Salima), HOANG (Huyen), « La blockchain va-t-elle tuer les tiers de confiance ? », *ZDNet* [en ligne], 15 mars 2018, https://www.zdnet.fr/blogs/social-media-club/la-blockchain-va-t-elle-tuer-les-tiers-de-confiance-39865540.htm.
[2097] CHAFFIN (Zeliha), « Paris dénonce une "privatisation" de la gouvernance d'Internet », *Le Monde* [en ligne], 24 mars 2016, https://www.lemonde.fr/economie/article/2016/03/24/icann-paris-denonce-une privatisation-de-la-gouvernance-d-internet_4889567_3234.html. – SMYRNAIOS (Nikos), *op. cit*., pp. 7-9.
[2098] *Id.*
[2099] SMYRNAIOS (Nikos), *op. cit.*, pp. 10-12.
[2100] BARRAUD (Boris), « Les blockchains et le droit », art. cit., *loc. cit.*
[2101] V. notamment, BLOCK (Raphaël), « La blockchain, le nouvel eldorado des entreprises », *Les Echos* [en ligne], 17 mars 2018, https://www.lesechos.fr/07/03/2018/lesechos.fr/0301351756204_la-blockchain--le-nouvel-eldorado-des-entreprises.htm. – CUNY (Delphine), « "La Blockchain, c'est la quatrième révolution industrielle !" », *La Tribune* [en ligne], 15 mai 2018, https://www.latribune.fr/entreprises-finance/banques-finance/la-blockchain-c-est-la-quatrieme-revolution-industrielle-777445.html.
[2102] BARRAUD (Boris), « Les blockchains et le droit », art. cit., *loc. cit*. – BERBAIN (Côme), art. cit., *loc. cit*.

299. L'appropriation d'un bien commun. La concurrence dans le domaine ne cesse de croître, de sorte que certains évoquent une « course au monopole »[2103]. Persuadés que « *winer takes all* » (« le premier remporte tout le marché »), les acteurs économiques cherchent à devenir la référence en la matière[2104]. Véritable enjeu markéting[2105], cette concurrence prend la forme d'une explosion des déploiements de nouvelles *blockchains*. Seulement, afin de garder un contrôle souvent exclusif sur le protocole, les acteurs économiques développent essentiellement des *blockchains* « privées », avec les caractéristiques fondamentalement divergentes qui leur sont attachées[2106]. Dans cette quête de la création d'une *blockchain* entièrement maîtrisable, le risque est à terme d'annihiler la liberté et les principes directeurs de partage et en particulier d'*open source* qui avaient été érigés au sein de la technologie *blockchain*. Une auteure souligne que « l'aspiration profonde des créateurs de cet écosystème était justement d'en faire bénéficier le plus grand nombre et non de cloisonner cet environnement par des monopoles et droits d'exploitation qui excluent forcément un certain nombre d'acteurs »[2107]. Il apparaît toutefois que les investissements parfois colossaux en la matière parviennent à justifier la brevetabilité de la *blockchain*[2108].

300. L'appropriation d'un bien commun : par la propriété intellectuelle. Volontairement *open source*, la technologie *blockchain* de Satoshi Nakamoto est destinée à être copiée, diffusée, et même modifiée, améliorée et intégrée à d'autres systèmes informatiques selon les besoins de ses utilisateurs, ce qui n'aurait pas été le cas si elle avait été un logiciel propriétaire[2109]. Un auteur constate d'ailleurs que les logiciels *open source* devraient, en principe, tomber dans la catégorie du domaine public, d'autant plus que la *blockchain* de Satoshi Nakamoto est spécifiquement couverte par une licence *open*-source américaine (la licence MIT), constituée par un document d'une demi-page qui indique que le protocole est « *AS-IS* » (« tel quel ») protégé[2110]. Si personne ne peut empêcher l'accès au code source d'un logiciel *open source*, autrement dit le fermer pour

[2103] BERBAIN (Côme), art. cit., *loc. cit.*
[2104] « Le vainqueur prend tout », « tout » étant le marché économique.
[2105] Rapp. Sénat n° 584, préc.
[2106] BARRAUD (Boris), « Les blockchains et le droit », art. cit., *loc. cit.*
[2107] BARSAN (Iris), « Blockchain - Blockchain et propriété intellectuelle », art. cit., n° 11.
[2108] *Ibid.*, n° 13.
[2109] *Id.* – V. également, FITZGIBBON (Magali), « Analyses outillées de la propriété intellectuelle des logiciels et traçabilité des composants tiers », *RLDI* 2014/3, n° 102, pp. 150 et s. ; SPEARMAN (Kelli), « Protecting Blockchain Investments in a Patent Troll World », *Journal of Intellectual Property Law*, Vol. 6, Issue 1, Article 7, pp. 182-183.
[2110] SPEARMAN (Kelli), « Protecting Blockchain Investments in a Patent Troll World », art. cit., p. 183.

se l'approprier, il n'empêche que certaines exclusivités juridiques peuvent, ponctuellement et partiellement, être consenties.

En effet, comme le souligne Iris Barsan, bien que fondée sur des algorithmes ne pouvant, en France et en Europe, ni faire l'objet d'une protection par le biais du droit d'auteur (directive 2009/24/CE du 23 avril 2009 concernant la protection juridique des programmes d'ordinateur[2111], considérant n° 11)[2112], ni assurer l'exclusivité de son exploitation par le biais d'un brevet (CPI, art. L. 611-10, Convention sur la délivrance de brevets européens[2113], art. 52[2114]), la *blockchain* peut être indirectement appropriée, d'une part, dès lors que l'algorithme est intégré à un logiciel protégeable (CPI, art. L. 112-2, 13°) et, d'autre part, s'il présente « une contribution technique nouvelle et non évidente » à une invention brevetable[2115]. L'Office européen des brevets (OEB) a, d'ailleurs, déjà consenti à protéger un algorithme à ce titre[2116]. Des entreprises tentent actuellement, sur tous les continents et notamment en Chine et aux Etats-Unis, de déposer des brevets leur permettant de garantir leur exclusivité sur des éléments du protocole[2117]. La plupart des brevets déposés en matière de *blockchain* relèvent d'une manière générale d'améliorations des protocoles de crypto-monnaies, mais pas seulement puisque certaines entreprises particulièrement innovantes ont pu protéger de nouvelles fonctionnalités[2118].

[2111] Dir. n° 2009/24/CE du Parlement européen et du Conseil, 23 avr. 2009, concernant la protection juridique des programmes d'ordinateur (version codifiée) (Texte présentant de l'intérêt pour l'EEE), *JOUE* L 111, 5 mai 2009, pp. 16-22. Le considérant n° 11 de la directive précise que « seule l'expression d'un programme d'ordinateur est protégée et [...] les idées et les principes qui sont à la base des différents éléments d'un programme, y compris ceux qui sont à la base de ses interfaces, ne sont pas protégés par le droit d'auteur en vertu de la présente directive. En accord avec ce principe du droit d'auteur, les idées et principes qui sont à la base de la logique, des algorithmes et des langages de programmation ne sont pas protégés en vertu de la présente directive ».

[2112] V. notamment, CARON (Christophe), *Droit d'auteur et droits voisins*, éd. LexisNexis, 6e édition, 2019, n° 178.

[2113] Conv., 5 oct. 1973, sur la délivrance de brevets européens (Convention sur le brevet européen, CBE) telle que révisée par l'acte portant révision de l'article 63 de la CBE du 17 décembre 1991 et l'acte portant révision de la CBE du 29 novembre 2000.

[2114] Sur les similitudes entre le protocole *blockchain* et le programme informatique, *supra* n° 19.

[2115] BARSAN (Iris), « Blockchain - Blockchain et propriété intellectuelle », art. cit., n° 14.

[2116] L'auteure cite pour exemple un recours (OEB, 21 avr. 2004, T 0258/03, Auction method c/ HITACHI) contre une décision ayant rejeté la demande d'un brevet européen déposé par la société Hitachi, Ltd. alors même que la méthode utilisée faisait appel à des moyens techniques constituant une invention au sens de l'art. 52 (1) de la CBE. – Pour plus de précisions, v., BARSAN (Iris), « Blockchain - Blockchain et propriété intellectuelle », art. cit., *loc. cit*.

[2117] V. en ce sens notamment, D. (Etienne), « Mastercard : Un brevet pour relier la crypto-monnaie à la monnaie-fiat », *Cryptonaute* [en ligne], 18 juill. 2018, https://cryptonaute.fr/mastercard-brevet-compte-crypto-monnaie-fiat-fiduciaire/ ; SHOME (Arnab), « Bank of America Now Holds Patent for Cryptocurrency Exchange System », *Finance Magnates* [online], 1st Dec. 2017, https://www.financemagnates.com/cryptocurrency/news/bank-america-now-holds-patent-cryptocurrency-exchange-system/. – KAYE (Byron), WAGSTAFF (Jeremy), « L'"inventeur" du bitcoin multiplie les dépôts de brevets », *Challenges* [en ligne], 20 juin 2016, https://www.challenges.fr/high-tech/l-inventeur-du-bitcoin-multiplie-les-depots-de-brevets_17159.

[2118] BARSAN (Iris), « Blockchain - Blockchain et propriété intellectuelle », art. cit., n° 14 ; KRAJEWSKI (Trevor), LETTIERE (Rich), « Blockchain and Intellectual Property », *Les Nouvelles – Journal of the Licensing Executives Society*, Vol. LIV No. 1, 24 Mar. 2019, pp. 2-3, https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3316992_code2574456.pdf?abstractid=3316992&mirid=1&type=2.

Il en va ainsi de l'entreprise *Intuit* qui a réussi à obtenir un brevet pour son concept d'envoi de *bitcoins* par SMS[2119].

Comme le constate une auteure, « parfois, pouvoir exclure les concurrents d'une découverte peut présenter un intérêt », notamment pour la collectivité, qui peut alors bénéficier des investissements en recherches et développements, sans que cette diffusion ne puisse porter préjudice au détenteur du brevet, lequel conserve le monopole d'exploitation[2120]. Seulement, la *blockchain* était originellement une technologie ouverte, transparente et mise à la disposition de chacun[2121]. Si bien qu'octroyer l'exclusivité de son utilisation pourrait, à l'instar des protocoles Internet, non seulement définitivement freiner le déploiement futur de *blockchains* publiques, mais également faire de la *blockchain* une technologie privée conditionnant toute utilisation future du protocole au paiement d'un droit. Plus encore, fermer le protocole reviendrait à déstabiliser le marché, voire créer une économie inégalitaire fondée sur la détention de droits exclusifs. Une société qui aura bénéficié, gratuitement, des avantages et spécificités de la technologie *open source* pourra ensuite faire supporter aux autres sociétés des coûts de licence importants que son monopole rendra, de surcroît, difficilement négociables[2122], si bien que certains auteurs annoncent l'imminence d'une véritable « guerre des brevets »[2123]. À l'heure actuelle, le protocole de la *blockchain* ferait l'objet de 2 048 brevets en Chine, 1 234 aux États-Unis, et 340 en Europe[2124]. Ces chiffres, au-delà de confirmer les craintes exposées, révèlent par ailleurs, selon Iris Barsan, un risque important pour la croissance des entreprises européennes vis-à-vis des concurrents chinois et américains, un risque qui devra toutefois faire l'objet d'un examen approfondi eu égard à l' « équilibre délicat à trouver entre la protection et la liberté »[2125].

Par ailleurs, un autre type de monopole tend, par son installation progressive, à soulever nombre de difficultés.

301. L'appropriation d'un bien commun : par l'achat de la puissance de calcul. Le cœur disruptif de *Bitcoin* est lui aussi actuellement convoité par de puissantes

[2119] P. (Stanislas), « L'entreprise Intuit obtient un brevet pour l'envoi de Bitcoin par SMS », *Cryptonaute* [en ligne], 13 août 2018, https://cryptonaute.fr/intuit-brevet-envoi-bitcoin-par-sms/.
[2120] BARSAN (Iris), « Blockchain - Blockchain et propriété intellectuelle », art. cit., n° 14.
[2121] EPO, « Talking about a new revolution: blockchain. Conference report », The Hague, 4 Dec. 2018, non publié [en ligne], p. 10, www.epo.org/learning-events/events/conferences/2018/blockchain2018.html.
[2122] *Id.*
[2123] *Id.* ; KRAJEWSKI (Trevor), LETTIERE (Rich), art. cit. p. 3.
[2124] MÉNIÈRE (Yann), « The emerging blockchain patent landscape », *in* EPO Conference, « Patenting Blockchain », The Hague, 4 Dec. 2018, non publié [en ligne], https://www.epo.org/news-events/news/2019/20190314.html.
[2125] BARSAN (Iris), « Blockchain - Blockchain et propriété intellectuelle », art. cit., n° 15.

entreprises financières. En effet, l'auto-régulation des mineurs permise par le processus du « *mining* », fonctionnalité du protocole fondée sur la confiance, est gravement menacée par une société, l'entreprise britannique gHash.io[2126]. Ce groupe constitue, en réalité, un « *mining pool* », c'est-à-dire qu'il concentre un nombre important de mineurs de la chaîne, et donc de capacités de calculs, dans le but de s'assurer la victoire à, presque, chaque phase de vérification de *Bitcoin* et ainsi remporter les récompenses. *A priori*, bien que le jeu ne paraisse pas tout à fait équitable ni équilibré, rien n'interdit dans le protocole que des mineurs se regroupent pour associer leur force de travail. Seulement, au-delà des gains résultant des récompenses associées au travail fourni, cette configuration conduit gHash.io à progressivement acquérir la majorité de la puissance de calcul globale du protocole[2127]. Cette question sera développée amplement à la suite de l'étude[2128], mais en tout état de cause, détenir plus de 51 % de cette puissance permettrait à *gHash.io* de prendre le contrôle exclusif de la chaîne.

Comme le souligne Pierre Porthaux, « la concentration et l'augmentation de la force de travail font partie des dérives qui n'ont pas été anticipées par Sakoshi Nakamoto (qui affirmait "un CPU, un vote") »[2129]. À nouveau, l'utilisation faite de la technologie en contradiction avec les principes posés initialement, en particulier l'utilisation par des entreprises dont le seul but est de faire du chiffre d'affaires[2130], conduit progressivement à remettre en question la fiabilité du système.

Nombre d'acteurs économiques semblent appréhender la technologie de la chaîne de blocs davantage comme un danger à moyen-long terme au sens où les plateformes de type *Airbnb* et *Uber* pourraient effectivement être, du moins en partie, remplacées[2131]. Néanmoins, cette perception les mène à absorber l'intégralité du marché, « quitte à trahir l'état d'esprit initial de la [...] *blockchain* »[2132], comme pour Internet dès ses premières années[2133].

D'ailleurs, force est de constater que la mutation du protocole initial a fait des *blockchains* de type « privées » ou « de consortium » des technologies à la gouvernance

---

[2126] BERBAIN (Côme), art. cit., p. 4.
[2127] *Id.*
[2128] *Infra* n°s 310 et s.
[2129] Rapp. Sénat n° 584, préc.
[2130] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 7.
[2131] *Ibid.*, note n° 16 : « Par exemple, *Ujo Music* propose un service visant à rendre aux artistes la pleine propriété de leurs productions. Cela pourrait mettre à mal les plates-formes qui cannibalisent une partie de la valeur créée. Pour ce qui est du transport par automobile, des projets tels que *La Zooz* ou *Arcade City* ont pour finalité de donner lieu à des formes d'*Uber* sans *Uber* et, donc, sans prélèvement de commissions en échange de la confiance garantie. »
[2132] DOUVILLE (Thibault), VERBIEST (Thibault), « Blockchain et tiers de confiance : incompatibilité ou complémentarité ? », *D.* 2018, n° 5, p. 1144.
[2133] CARRÉ (Marion), LASRY (Julia), MECHERRA (Salima), HOANG (Huyen), « La blockchain va-t-elle tuer les tiers de confiance ? », art. cit.

plus flexible. Les acteurs économiques ne comptent pas seulement envahir le marché économique, mais envisagent de contrôler l'intégralité du protocole de Satoshi Nakamoto par le biais de ces nouveaux modèles d'administration.

B. La création de modèles d'administration centralisée

302. Les avantages de l'administration centralisée ou partiellement centralisée : une application du droit objectif facilitée. Dans le domaine, sous diverses formes, la privatisation de la *blockchain* peut présenter un certain intérêt. En effet, alors que l'identification efficace des divers participants pouvait parfois soulever des difficultés en matière de *blockchain* publique[2134], cette problématique ne se pose pas en ce qui concerne les *blockchains* « privée » et hybride. En effet, le caractère fermé ou éventuellement partiellement ouvert entraîne une identification systématique de chacun des utilisateurs au moment où ils envoient une requête demandant l'autorisation d'accéder au système[2135]. Au-delà de l'identification, l'ensemble des questions relatives à l'application et à l'applicabilité du droit positif envisagées jusqu'ici[2136] n'ont pas, non plus, lieu d'être. Il en va ainsi notamment des règles en matière de données personnelles et de droit à l'oubli auxquelles les protocoles « privés » et hybrides pourront, sans nul doute, se conformer.

303. Les avantages de l'administration centralisée ou partiellement centralisée : un système de prise de décision allégé. Par ailleurs, si l'application de règles de gouvernance centralisatrices conduisent à rassembler chacun des pouvoirs originellement partagés entre les membres de la communauté en une source unique de pouvoir, la prise de décision sur les *blockchains* en est assurément simplifiée. Or il apparaît qu'en termes de réformes structurelles, les *blockchains* traditionnelles souffrent parfois des lenteurs ou des difficultés à atteindre un consensus. Il en va ainsi de celle de *Bitcoin*[2137] qui, pour des raisons de scalabilité[2138] et de continuation de la chaîne, nécessiterait des modifications

[2134] Sur les difficultés d'identification en matière de *blockchain* publique, *supra* n° 114.
[2135] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 18.
[2136] Sur les incohérences entre la technologie *blockchain* et le droit objectif, *supra* n°s 182 et s.
[2137] PHUC (Morgan), « Bitcoin - La guerre des blocs », *BitConseil* [en ligne], 25 mars 2017, https://bitconseil.fr/bitcoin-guerre-blocs/.
[2138] Ou « *scalability* », désigne, selon la définition donnée par Wikipedia.fr [https://fr.wikipedia.org/wiki/Scalability] elle-même tirée du Grand Dictionnaire terminologique de l'Office québécois de la langue française [http://gdt.oqlf.gouv.qc.ca/Resultat.aspx], « la capacité d'un produit à s'adapter à un changement d'ordre de grandeur de la demande (montée en charge), en particulier sa capacité à maintenir ses fonctionnalités et ses performances en cas de forte demande ». De plus, « selon René J. Chevance, le mot anglais *scalability*, formé sur l'adjectif scalable dérivé du verbe *to scale* ("changer d'échelle"), "n'a pas d'équivalent communément admis en français" [v.,CHEVANCE (René J.), « Serveurs multiprocesseurs et SGBD parallélisés », *Techniques Ingénieur* [en ligne], n° H2068 v1, 2000, p. 4, https://www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9/bases-de-

de son protocole afin d'intégrer une nouvelle limite de transactions pouvant être inscrites sur un bloc. Cependant, à défaut de réussir à concilier l'ensemble des utilisateurs sur un nombre de transactions, la communauté et donc le protocole restent bloqués sur ce point[2139]. Lorsqu'un consensus est difficilement atteignable, force est de reconnaître que le contexte collaboratif démultiplie nécessairement les difficultés alors qu'une gouvernance édictant des règles autoritaires, claires et précises n'aurait à supporter quant à elle aucun contretemps[2140].

Toutefois, la facilité offerte par ces nouvelles formes de *blockchains* doit être évaluée à la lumière des compromissions auxquelles il faudrait, en contrepartie, inévitablement s'accommoder.

304. Sacrifier l'égalité et la sécurité pour le contrôle ou le contrôlable ? La volonté du code informatique est avant tout celle de son codeur. En règle générale, le développeur d'une chaîne de blocs « privée » ou de consortium intègre directement dans le protocole un corpus de règles de fonctionnement, dont il s'assure le respect par les utilisateurs en les liant par un contrat au moment où ceux-ci s'identifient pour accéder au contenu mis à leur disposition[2141]. En définitive, puisque l'ouverture du protocole est, dans ces types de chaînes, sinon absente, du moins partielle, la gouvernance exercée par le gestionnaire est considérable[2142] et marque, d'une manière ou d'une autre, un retour des mécanismes de centralisation du pouvoir à l'instar des tiers de confiance tant critiqués[2143].

En plus du pouvoir, la logique pyramidale adoptée par les *blockchains* privatisées les entraîne à procéder à un déplacement de la redistribution de la valeur créée initialement par les multiples acteurs travaillant pour la *blockchain*, vers l'intermédiaire central[2144]. La centralisation d'Internet a par exemple eu pour conséquence de créer des sociétés oligopoles, à l'instar de Google, de Facebook, de Amazon et d'autres puissants acteurs économiques du secteur, qui sont parvenues à imposer leur mode de fonctionnement à travers le monde[2145]. D'ailleurs, force est de reconnaître que les algorithmes développés par ces sociétés ont une telle emprise sur les individus qu'ils sont

---

donnees-42309210/serveurs-multiprocesseurs-et-sgbd-parallelises-h2068/]. Les traductions utilisées sont ; extension graduelle, évolutivité, facteur d'échelle, extensibilité, passage à l'échelle, ou capacité à monter en charge ».

[2139] PHUC (Morgan), art. cit.

[2140] BARRAUD (Boris), « Les blockchains et le droit », art. cit., *loc. cit.*

[2141] *Id*.

[2142] *Id.*

[2143] HELLEU (Guillaume), MASURE (Anthony), « Total Record. Les protocoles blockchain face au post-capitalisme », *Multitudes* 2018/2, n° 71, p. 77.

[2144] BARRAUD (Boris), « Les blockchains et le droit », art. cit., p. 7.

[2145] SMYRNAIOS (Nikos), *op. cit.*, pp. 10-12.

capables désormais d'interférer, en général, dans leurs vies personnelle et professionnelle et, en particulier, dans leurs pratiques de consommateurs. Selon Boris Barraud, ils constituent finalement « la source essentielle de normativité qui a notamment droit de vie et de mort sur de nombreuses entreprises »[2146]. La centralisation de la *blockchain* risque à terme de poser également un problème de confiance eu égard à la perte d'objectivité du protocole. En effet, selon Satoshi Nakamoto, l'enjeu réside dans la règle de la distributivité, incarnée le plus souvent par des protocoles « *Proof of Work* », qui constitue une des règles indispensables au fonctionnement de tout protocole basé sur un modèle-type *blockchain*. Il résulte de cette règle qu'aucun utilisateur malveillant ne pourra ajouter, modifier, ou supprimer des éléments de la *blockchain* dès lors qu'elle sera elle-même appliquée et respectée. Or, dans un système centralisé, de surcroît dépourvu de mineurs se partageant la charge de valider et d'inscrire les informations dans les blocs de la chaîne, tout porte à croire qu'un participant soit contraint, à un moment donné, de s'auto-proclamer arbitre avec la mission de valider lui-même les blocs[2147]. La mise en œuvre de cette solution posera nécessairement un problème d'impartialité et donc de sécurité. La CNIL a d'ailleurs soulevé le problème et recommande, notamment en ce qui concerne les *blockchains* de consensus, « d'évaluer, en fonction de l'éventuelle divergence ou convergence des intérêts des acteurs participants, un minimum de mineurs permettant d'assurer l'absence de coalition permettant de contrôler plus de 50 % des pouvoirs sur la chaîne »[2148].

305. Une utilité amoindrie ? Au niveau de la gestion interentreprises par exemple, la technologie *blockchain* traditionnelle ne semble présenter que peu d'utilité. À moins de dépasser les applications informatiques déjà existantes dans le domaine de la comptabilité, des ressources humaines et d'autres systèmes de planification des ressources de l'entreprise, l'utilisation de la chaîne publique, bien que parfaitement envisageable, se révèlerait cependant particulièrement inopportune en raison des nombreuses démarches et besoins en investissement tant financier qu'humain et de l'inutile complication des procédures qu'elle occasionnerait.

[2146] BARRAUD (Boris), « Les blockchains et le droit », art. cit., *loc. cit*. – V. également, « Goggle Maps réveille le marché de la cartographie en passant au payant pour les pros », *Capital* [en ligne], 20 juill. 2018, https://www.capital.fr/entreprises-marches/google-maps-reveille-le-marche-de-la-cartographie-en-passant-au-payant-pour-les-pros1299172.
[2147] Rapp. Sénat n° 584, préc.
[2148] CNIL, « Blockchain : Premiers éléments d'analyse de la CNIL », CNIL [en ligne], sept. 2018, p. 11, https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf.

En revanche, la flexibilité du protocole d'une *blockchain* de type « privée » ou de consortium pourrait éventuellement permettre de dépasser les fonctionnalités des bases de données traditionnelles en fournissant à l'entreprise une sécurité accrue[2149]. Bien que la privatisation du protocole apparaisse en effet comme étant le seul moyen de permettre aux entreprises d'utiliser la *blockchain* efficacement, d'une manière générale, le fait que la gestion du registre de la *blockchain* ne soit attribuée qu'à un nombre limité d'utilisateurs mène, malgré tout, à interroger son réel intérêt[2150]. En effet, même en termes de rapidité et de capacités techniques, les *blockchains* privatisées ne semblent présenter qu'une modeste utilité par rapport aux solutions existantes, qu'il s'agisse d'ailleurs de l'implanter au sein d'une entreprise ou dans d'autres secteurs[2151]. Simon Polrot constate que, dans la pratique, « beaucoup de projets de *blockchains* privées assez ambitieux se sont finalement rabattus vers les simples usages d'horodatage et d'ordonnancement »[2152].

Par ailleurs, même en matière d'horodatage et d'ordonnancement, qui constituent les spécificités principales de la *blockchain*, l'intérêt des chaînes centralisées est discutable. En effet, dans le fonctionnement du protocole traditionnel, c'est parce que la fonction de production des blocs fait l'objet d'une distribution et que la vérification requiert un consensus entre les multiples participants que les inscriptions sont réputées immuables. Autrement dit, par une gestion décentralisée, la technologie créée une « vérité partagée » capable de garantir l'infaillibilité de son système d'horodatage[2153]. *A contrario*, la mise en œuvre du contrôle des inscriptions par l'entité centralisée ou centralisatrice des *blockchains* « privées » et de consortium laisse entière la question de leur immuabilité. Simon Polrot soulève à juste titre la question de la valeur, et indirectement, de l'intérêt d'un acte notarié enregistré au sein d'un système privé[2154]. Finalement, l'apport de ces mutations semble relativement mitigé en termes de traçabilité.

306. Brider la recherche et l'innovation collective ? De la même façon, la privatisation de la technologie ne lui permettra pas de poursuivre son projet *open source* qui encourageait jusqu'ici l'innovation, autant que la productivité et l'efficacité des membres et ce, dans un schéma de coopération libre et ouverte. Le risque est, qu'à terme,

[2149] LEE (David), CHUEN (Kuo), DENG (Robert H.), *Handbook of Blockchain, Digital Finance, and Inclusion: vol. 2:ChinaTech, Mobile Security, and Distributed Ledger*, ed. Academic Press, 2017, pp. 156-157.
[2150] WÜST (Karl), GERVAIS (Arthur), « Do you need à blockchain ? », *in* 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, 20-22 Jun. 2018, *IEEE* [online], 8 Nov. 2018, https://eprint.iacr.org/2017/375.pdf ; DE THÉSUT DUFOURNAUD (Sylvie), art. cit.
[2151] Rapp. Sénat n° 584, préc.
[2152] *Id.*
[2153] *Id.*
[2154] *Id.*

les projets *blockchains* auto-régulés et auto-gérés ne puissent être développés ni déployés[2155].

307. Dans sa théorie du contrat social, John Locke met en avant l'importance de la division des pouvoirs pour éviter les abus d'un corps politique dominant[2156]. Au-delà du contexte notamment politique qu'il expose à travers sa conception de la démocratie libérale, cette théorie selon laquelle les pouvoirs ne doivent pas, dans un système, être concentrés entre les mains d'une seule entité semble faire échos aux multiples difficultés relevées de l'utilisation des *blockchains* privatisées. La mise en œuvre d'une gouvernance au sein d'une technologie comme celle de la *blockchain* se révèle finalement délicate. D'une part, l'auto-régulation actuelle a montré un certain nombre de limites à travers la difficile légitimation de la gestion du détournement de *TheDAO*[2157] et, d'autre part, la régulation centralisée apparaît réduire substantiellement l'intérêt de la technologie, et lui faire perdre son caractère innovant le cas échéant. Une gouvernance fondée sur une logique collaborative, à condition toutefois qu'elle s'adapte et impose dès sa conception une gouvernance plus marquée afin, à la fois, de rendre légitime et de conditionner l'intervention du développeur, pourrait permettre ce qui s'apparenterait à une forme de partage des pouvoirs. Toutefois, il n'empêche que chacun des protocoles envisagés engendre des problématiques sensiblement différentes les unes des autres qui devront être examinées au cas par cas afin d'établir si les exigences légales du secteur d'implantation sont respectées[2158]. En théorie, il apparaît que n'importe quelle forme de gouvernance devra malgré tout être une source d'autorité et de finalité juridique[2159].

Néanmoins la pratique complique le respect de cette exigence pourtant nécessaire à son essor. En effet, si une simple faille dans une application d'*Ethereum* a pu soulever des doutes quant à la fiabilité du protocole, il semble raisonnable de s'inquiéter des conséquences en termes de confiance s'il s'avérait que la *blockchain* présente, en pratique, des vulnérabilités résultant de son propre mode de fonctionnement et que certains pourraient choisir d'utiliser à mauvais escient.

[2155] *Id.*
[2156] TERESTCHENKO (Michel), *op. cit.*, *loc. cit*.
[2157] Pour plus de précisions sur *TheDAO*, *supra* n^{os} 270 et s.
[2158] BEAUDEMOULIN (Nathalie) *et al*., art. cit., pp. 31-32.
[2159] COLLOMB (Alexis), SOK (Clara), LEGER (Lucas), « Technologie des registres distribués : quel impact sur les infrastructures financières ? », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 27.

Chapitre 2. Les vulnérabilités fonctionnelles

308. Comme le rappelle Ricardo Perez-Marco, la *blockchain* constitue « un réseau automatique qui crée de la confiance entre personnes qui ne peuvent pas se faire confiance »[2160]. Ce réseau doit donc veiller à être suffisamment sécurisé pour instaurer le climat de confiance nécessaire à des relations, notamment conventionnelles, stables et durables. Il doit d'autant plus s'en assurer qu'il aspire à substituer aux tiers de confiance actuels une « version transactionnelle des réseaux de pair à pair »[2161]. Seulement, il s'avère que cette distributivité, et la décentralisation qui l'établit, suggèrent qu'une multitude d'individus puisse intervenir sur la chaîne, y compris ceux animés d'intentions malveillantes. Mais, qu'en est-il si le danger peut également découler de la présence de l'Homme dans le fonctionnement de la technologie ? Sous diverses formes et par le biais de différentes interventions, l'Homme contribue à rendre vulnérable la technologie et constitue finalement un risque pour son intégrité. Plus encore, ce contexte semble révéler que la technologie demeure dépendante de l'Homme, et plus particulièrement de son comportement et *a fortiori* de sa propre fiabilité.

Il n'est dès lors guère étonnant que la technologie se retrouve compromise par une pluralité de risques d'attaques (Section 1), ni d'ailleurs que son fonctionnement soit finalement limité par la présence imposée des Oracles (Section 2).

Section 1. Une technologie compromise par une pluralité de risques d'attaques

309. La technologie initiale des *blockchains* est fondée sur la combinaison de deux théories mathématiques, à savoir, la théorie des réseaux informatiques, mobilisant le potentiel des architectures pair à pair et les techniques de cryptographie, et la théorie des jeux, qui se traduit par une incitation des mineurs à sécuriser le réseau[2162]. En effet, un auteur constate que le protocole *Bitcoin* constitue « le seul jeu où l'on a intérêt à jouer dans les règles », car la compétition créée au sein du réseau conduit à ce que « celui qui ne joue pas dans les règles va non seulement ne pas gagner d'argent mais aussi en perdre

[2160] Rapp. AN n° 1092, rapp. Sénat n° 584, 20 juin 2018, Comprendre les blockchains : fonctionnement et enjeux de ces nouvelles technologies, présenté par Valéria FAURE-MUNTIAN, Claude DE GANAY, et Ronan LE GLEUT, au nom de l'office parlementaire d'évaluation des choix scientifiques et technologiques.
[2161] *Id*.
[2162] *Id*.

(en dépensant de l'énergie en vain) »[2163]. Finalement, l'ensemble de ces paramètres compose le facteur de confiance du système, suggérant dès lors qu'une simple modification de l'un d'eux est susceptible de déstabiliser l'intégralité du réseau[2164]. Néanmoins, les règles posées au sein de la communauté n'empêchent pas certains utilisateurs de les enfreindre, ou du moins de les contourner pour attaquer le système. Son propre fonctionnement permet ainsi à des utilisateurs de prendre son contrôle, sinon d'y faire régner l'insécurité. Un état des lieux s'avère nécessaire afin de comprendre ces attaques et mieux les anticiper voire, éventuellement, les solutionner.

Il s'agira, d'une part, d'examiner la dangerosité des prises de pouvoir des attaques à 51 % permises par une faille au sein du principe de consensus décentralisé régissant les *blockchains* publiques (§ 1) et, d'autre part, d'évaluer la vulnérabilité des utilisateurs aux nouvelles méthodes de vols et, *a fortiori*, l'importance des failles dans la cybersécurité du protocole distribué (§ 2).

§ 1. Une faille au sein du principe de consensus décentralisé : les dangereuses prises de pouvoir des attaques à 51 %

310. En règle générale, les *blockchains* publiques faisant appel au *mining* fonctionnent sur la base de nœuds calculant en continu des empreintes *SHA256* afin de valider les blocs un à un[2165]. L'objectif étant qu'une majorité, définie à 51 % des mineurs, valide et inscrive définitivement chaque opération. L'immuabilité et la fiabilité du système émanent de ce consensus décentralisé. Seulement, comme le souligne Pierre Porthaux, « la concentration et l'augmentation de la force de travail font partie des dérives qui n'ont pas été anticipées par Satoshi Nakamoto (qui affirmait "un CPU, un vote") »[2166]. Il convient dès lors d'analyser ces comportements de concentration du minage (A), mais également de dresser un état des lieux, non seulement de leurs conséquences, mais également des solutions actuellement en projet pour y remédier (B).

A. Analyse des comportements de concentration du minage

311. Un protocole soumis à la puissance des processeurs : quand l'investissement en *hardware* l'emporte sur l'importance du *software*. L'activité de minage consiste en

[2163] *Id.*
[2164] *Id.*
[2165] *Supra* n° 134.
[2166] Rapp. AN n° 1092, rapp. Sénat n° 584, préc.

la résolution d'un problème de mathématiques au sein d'un modèle de réseau P2P[2167]. En pratique, ce calcul consiste à tester, une à une, différentes valeurs jusqu'à obtenir un *hash* répondant à la difficulté posée par le protocole[2168]. Par le biais de son ordinateur, lequel constitue un des nœuds du réseau (*node*), chaque mineur peut participer à la course organisée par le protocole qui, s'il la remporte, lui permettra de sceller sa propre version du bloc sur la chaîne, et en parallèle d'être rétribué pour le travail de son nœud[2169]. L'apport de ces principes de fonctionnement est considérable en matière de sécurité puisqu'ils scellent, par leur application, l'inscription d'un document ou d'une transaction *blockchain* entre deux utilisateurs, et *a fortiori* celle d'un acte entre deux parties, de manière définitive et immuable[2170]. L'extrême complexité du problème de mathématiques proposé aux mineurs assure la sûreté du mécanisme. En permettant aux nœuds de rivaliser entre eux, de manière subsidiaire le protocole a fait de la puissance de calcul un paramètre aussi important que la distributivité ou la preuve de travail. Seulement, à mesure que la difficulté des calculs requis pour valider les blocs a augmenté, les mineurs ont cherché des processeurs plus rapides et plus performants. La *blockchain* publique, et en particulier la chaîne du *Bitcoin*, a ainsi progressivement été envahie de nœuds disposant de processeurs « ASICs » (*Application-Specific Integrated Circuits*)[2171]. Ces processeurs spécialement conçus pour le minage de crypto-monnaies sont des circuits intégrés[2172] capables de dépasser les processeurs et processeurs graphiques (GPU) habituellement utilisés par les mineurs, à la fois en termes de rapidité, d'efficacité mais également en

[2167] *Supra* n°s 95 ; 142 et s.
[2168] Pour une définition détaillée, *supra* n° 145. – V. également, FLORI (Jean-Pierre), « Sécurité et insécurité de la blockchain et des smart contracts », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 98 : « Le problème mathématique repose sur une fonction de hachage, à savoir une fonction qui prend une séquence de lettres et de chiffres x de longueur arbitraire, et en tire une autre y de longueur fixe. La propriété des fonctions de hachage est qu'il est relativement facile de calculer y à partir de x, mais impossible de retrouver x à partir de y, de même qu'il est difficile de factoriser un grand nombre, mais facile de vérifier qu'une factorisation est correcte. Le problème mathématique est alors le suivant : étant donné l'entête du bloc le plus récent x, il faut trouver un nombre n (dit valeur de circonstance) tel que le hachage y de la séquence (x, n) satisfasse une certaine condition : par exemple les vingt-cinq premiers caractères doivent être des zéros. Comme il n'est pas possible d'aller à l'envers et de calculer n, la seule méthode consiste à essayer des nombres n les uns après les autres, jusqu'à ce que l'on trouve un y qui réponde à la condition. » – Autrement expliqué, v., VELDE (François R.), « Bitcoin pour remplacer les devises », *Rev. éco. fin*. 2015/4 (2016), n° 120, p. 105 : « Étant donné le hache H(Bi-1) du bloc précédent de la blockchain, ainsi que les données à intégrer au nouveau bloc Bi (une liste Li de transactions à valider dans le cadre de *bitcoin*), il s'agit essentiellement de trouver un préfixe Ni, tel que le nouveau bloc Bi=(Ni, H(Bi-1), Li) constitue de la concaténation de ces éléments satisfasse la condition que le hache H(Bi) commence par i bits nuls. ».
[2169] Notamment *supra* n° 146.
[2170] Notamment *supra* n° 145.
[2171] BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », *github* [liens de publication originaux supprimés] [online], Nov. 2013, https://github.com/ethereum/wiki/wiki/White-Paper.
[2172] *Id*.

termes de facilité d'utilisation[2173]. Bien que l'investissement demeure conséquent[2174], les ASICs sont vendus à des prix de plus en plus abordables, ce qui permet de démocratiser progressivement l'activité du minage de crypto-monnaies, du moins jusqu'à la prochaine version de processeurs[2175]. Néanmoins, des milliers de dollars sont aujourd'hui nécessaires à n'importe qui voudrait miner de manière efficace.

Comme Vitalik Buterin le souligne concernant *Bitcoin*, la course à la validation des blocs n'est plus la « *decentralized and egalitarian quest* » (« course décentralisée et égalitaire ») qu'avait instituée Satoshi Nakamoto, mais une course à la performance, à la puissance de calcul et, finalement, à la prise de pouvoir[2176].

312. L'union fait la puissance de calcul : la concentration des nœuds en *pools* de minage (*Mining Pools*). Le *mining* semble de moins en moins accessible eu égard aux complexités techniques, matérielles et financières qu'il engendre. Une fois astreints à l'achat de matériels spécialisés, les mineurs doivent se soumettre aux besoins en alimentation électrique que ces machines et équipements de plus en plus performants requièrent. Plus ils sont rapides, plus ils consomment, si bien qu'il apparaîtrait que « le minage du *Bitcoin* consomme désormais plus d'électricité que 159 pays »[2177]. Seulement, tandis que certaines villes augmentent spécifiquement le prix du kilowatt/heure pour les mineurs[2178], d'autres légifèrent pour interdire le *mining*[2179]. S'éloignant progressivement

---

[2173] VINOT (Alexandre), « ASIC résistance, une fausse bonne idée ? », *Bitcoin.fr* [en ligne], 14 mai 2018, https://bitcoin.fr/asic-resistance-une-fausse-bonne-idee/.

[2174] L'achat d'un ASIC demande entre 200 et 3 000 dollars selon la puissance de *hash* désirée. Le prix des ASICs les plus perfectionnés a parfois pu atteindre 15 000 dollars. Pour plus d'informations sur le sujet, v. notamment, TUWINER (Jordan), « Meilleurs rigs et matériels ASIC de minage », *Buy Bitcoin Worldwide* [en ligne], 13 juill. 2017, https://www.buybitcoinworldwide.com/fr/mineurs-de-bitcoins/ ; « Les confessions d'un mineur de bitcoin », *Bitcoin.fr* [en ligne], 26 juin 2013, https://bitcoin.fr/les-confessions-d-un-mineur-de-bitcoin/.

[2175] PAVEL (Ilarion), « La blockchain : Les défis de son implémentation », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 22.

[2176] BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », préc.

[2177] « Le minage du Bitcoin consomme désormais plus d'électricité que 159 pays », *Crypto-France* [en ligne], 18 déc. 2017, https://www.crypto-france.com/le-minage-du-bitcoin-consomme-desormais-plus-delectricite-que-159-pays/ : « Les transactions *Bitcoin* nécessitent désormais tellement d'énergie que l'électricité utilisée par une seule transaction pourrait assurer l'approvisionnement énergétique d'un foyer pendant près d'un mois, d'après une étude effectuée par la banque néerlandaise ING [http://uk.businessinsider.com/electricity-required-for-single-bitcoin-trade-could-power-a-house-for-a-month-2017-10]. »

[2178] SERVET (Alistair), « Québec : les mineurs de cryptomonnaies paieront l'électricité 2 fois plus cher », *Clubic* [en ligne], 21 juill. 2018, https://www.clubic.com/antivirus-securite-informatique/cryptage-cryptographie/crypto-monnaie/actualite-844646-quebec-mineurs-cryptomonnaies-paieront-electricite-2-cher.html.

[2179] ALVAREZ (Bruno), « Une ville interdit le minage de bitcoins », *L'édition du soir* [en ligne], 16 mars 2018, https://www.ouest-france.fr/leditiondusoir/data/21541/reader/reader.html#!preferred/1/package/21541/pub/30961/page/6 : « La ville de Plattsburgh, située dans l'État de New York, a constaté que le minage de *bitcoins* consomme environ 10 % de son offre en électricité. Conséquence : ce jeudi soir, le conseil

de l' « *egalitarian quest* » qu'elle était à ses débuts, la *blockchain* conduit ses mineurs à user d'inventivité afin de rénover leurs méthodes et moyens pour miner. Deux formes de centralisation ont principalement émergé de ces pratiques, dont les conséquences ne sont pas sans soulever de multiples difficultés.

313. L'union *via* le regroupement des mineurs entre eux : vers la fin de l' « *egalitarian quest* » des *blockchains*. D'une part, nombre de mineurs ont décidé de procéder à des regroupements en « *pools* » *via* un serveur central[2180] afin de mutualiser leurs puissances de calcul respectives[2181]. Souvent contractuellement organisés par des entreprises de minage de crypto-monnaies, à l'instar de la société britannique gHash.io[2182], ces *pools* permettent aux mineurs de mettre en commun leur puissance de calcul lors des étapes de vérification et de validation des blocs de la chaîne afin, s'ils en sortent vainqueurs, de partager la récompense (*block reward*) au prorata de leur participation. Toutefois il apparaît qu'aux termes des contrats unissant les mineurs à l'entreprise de minage ou, d'une manière générale, au responsable du serveur central, ce dernier opère une emprise indirecte sur l'intégralité de la puissance de calcul réunie[2183]. Or, s'il parvenait à recueillir la majorité de la puissance totale de minage, ce pouvoir lui permettrait de prendre l'entier contrôle du protocole[2184]. Tel est le danger rencontré avec la société gHash.io, laquelle, par son autorité croissante exercée sur la chaîne, menace la « liberté virtuelle » que permettait jusqu'ici *Bitcoin*[2185]. Considérée par l'entreprise comme étant une « conséquence naturelle » de l'effet « *Mining Pools* »[2186], la possibilité pour gHash.io de remporter l'intégralité des récompenses et *a fortiori* de prendre le contrôle exclusif de la chaîne du *Bitcoin* a toutefois pour effet d'inquiéter les utilisateurs, ce qui, indubitablement, génère un sentiment d'insécurité.

314. L'union *via* la création d'usines de nœuds : vers la fin de la décentralisation de la *blockchain* ? D'autre part, avec un budget nettement supérieur à beaucoup d'autres entreprises, des sociétés ont décidé de centraliser entièrement le processus de minage, et

municipal a voté, à l'unanimité, un moratoire de 18 mois interdisant l'exploitation minière de *bitcoins* dans la ville. Une première aux États-Unis. »

[2180] FLORI (Jean-Pierre), art. cit., p. 99.

[2181] GUILHAUDIS (Élise), « Comprendre la blockchain à travers l'étude d'un cas pratique : le covoiturage "Blockcar" », *RLDI* 2017/12, nº 143, p. 5.

[2182] BEAUDEMOULIN (Nathalie) *et al*., « Les enjeux de la Blockchain pour la Banque de France et l'Autorité de Contrôle prudentiel et de Résolution (ACPR) », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 31.

[2183] FLORI (Jean-Pierre), art. cit., p. 99.

[2184] *Id.*

[2185] BEAUDEMOULIN (Nathalie) *et al*., art. cit., *loc. cit*.

[2186] *Id*.

ont pour cela bâti, dans des pays comme la Chine[2187] et l'Inde[2188], des bâtiments exclusivement composés de processeurs minant continuellement. Le choix des pays d'implantation est stratégique puisque, d'une part, l'électricité est souvent relativement bon marché et, d'autre part, l'approvisionnement en processeurs, en particulier en processeurs ASICs, est facilitée car la plupart des fournisseurs sont eux-mêmes implantés dans ces pays[2189].

Dans son *White Paper Ethereum* publié en 2013, Vitalik Buterin avait constaté que 50 % de la puissance de calcul de *Bitcoin* étaient détenus par trois usines de minage chinoises[2190]. À l'heure actuelle, 81% de la puissance de l'ensemble des *mining pools* sont localisés en Chine, détenus par diverses entreprises telles que BTC.com, Antpool, et viaBTC[2191]. Témoignant de l'importance croissante que ces usines de nœuds prennent sur le réseau, ces chiffres semblent se heurter aux principes originels de sécurité, de transparence, de neutralité, de décentralisation, d'intégrité, de fiabilité, et finalement de confiance qu'incarnait la technologie *blockchain*. Certains auteurs vont jusqu'à imaginer que le gouvernement chinois pourrait, par opportunité ou en fonction des motivations politiques, volontairement décider de ne plus assurer l'approvisionnement en électricité des usines de minage non-chinoises présentes sur le territoire[2192].

315. En tout état de cause, cet usage concentré de la technologie est susceptible de constituer un frein à l'institution d'une confiance algorithmique. La décentralisation et la distributivité de la technologie permettent de garantir l'immuabilité des inscriptions de n'importe quelle chaîne et, d'une manière générale, sa fiabilité. Contrôlée de l'intérieur, elle ne présenterait dès lors plus aucun intérêt. Pour déployer davantage, ou du moins maintenir la technologie dans les entreprises et chez les particuliers, il est donc important de connaître les conséquences d'une prise de pouvoir sur le réseau.

B. Conséquences de la concentration et solutions en projet

316. Les effets d'une prise de pouvoir à 51 % sur une *blockchain*. Placée sous le contrôle exclusif d'un utilisateur ou d'un *pool*, une *blockchain* ne pourrait plus assurer

[2187] MEKKI (Mustapha), « Les mystères de la blockchain », *D.* 2017, n° 37, pp. 2160 et s., n° 4.
[2188] TUWINER (Jordan), « *Pools* de *mining* de *bitcoins* », *Buy Bitcoin Worldwide* [en ligne], 25 avr. 2018, https://www.buybitcoinworldwide.com/fr/minage/pools/.
[2189] FLORI (Jean-Pierre), art. cit., p. 99.
[2190] BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », préc.
[2191] TUWINER (Jordan), préc.
[2192] GUILHAUDIS (Élise), art. cit., p. 5.

l'immuabilité de ses inscriptions, si bien qu'une telle puissance permettrait à son détenteur de modifier, de supprimer ou de forcer l'inscription de ses propres transactions, mais pas uniquement. À l'instar du fonctionnement d'une chaîne privatisée[2193], non seulement l'attaquant majoritaire serait en mesure de contrôler l'accès au protocole en gérant les droits et autorisations de lecture et d'écriture, mais il pourrait également s'assurait la mainmise sur l'ensemble du registre, et donc sur l'ensemble des transactions inscrites ou à inscrire[2194].

Avec un tel pouvoir, l'attaquant pourrait, par exemple, intercepter une opération entre le moment où la demande par l'utilisateur a été envoyée sur le réseau et le moment où l'inscription a été effectivement inscrite dans un bloc, afin de l'invalider, de la détourner à son profit ou au profit de l'utilisateur de son choix, de modifier son montant, puis de forcer sa validation[2195].

Un attaquant majoritaire pourrait tout aussi facilement créer un phénomène de « double dépense » (*double-spending problem*) à son avantage, par le biais d'un *fork*[2196]. Ainsi, celui qui a le contrôle de la chaîne de blocs peut, par exemple, initier une transaction en échange d'un produit quelconque, entrer en la possession de ce produit, puis diviser la *blockchain* en utilisant la méthode du *fork*[2197]. En invalidant ensuite sa propre inscription au sein de la chaîne issue du *fork*, la transaction est définitivement supprimée et le mineur majoritaire peut réutiliser le montant de la transaction annulée pour en inscrire une autre sur cette chaîne – *double-spending*. Or, en vertu de l'art. 2276, al. 1er, du C. civ., « en fait de meubles, la possession vaut titre ».

Souvent utilisée en dehors de la *blockchain*, l' « attaque par déni de service » (*DoS attack*, *Denial of Service attack*) a pour effet de rendre indisponible un service auprès de ses utilisateurs. Dans le secteur des *blockchains*, une telle attaque repose sur l'envoi simultané d'une multitudes de transactions de faible valeur entravant les nœuds du réseau et provoquant l'arrêt, plus ou moins continu, du protocole. Par le biais des *pools* de minage, quelle que soit la forme qu'ils prennent, cette attaque bénéficie de la multiplicité des nœuds de sorte qu'elle constitue une « attaque par déni de service distribuée » (*DDoS attack*, *Distributed Denial of Service attack*). Profondément perturbantes, éventuellement paralysantes, ces attaques, lorsqu'elles sont menées par des utilisateurs non-majoritaires, ne permettent pas la maîtrise matérielle du protocole, mais restent malgré tout très

[2193] Définition de la *blockchain* « privée », *infra* n° 294 ; pour une analyse des impacts d'une administration centralisée, *supra* n°s 302-307.
[2194] PAVEL (Ilarion), art. cit., p. 22.
[2195] GUILHAUDIS (Élise), art. cit., p. 5.
[2196] Sur le phénomène de double-dépense, *supra* n° 6.
[2197] PLEYNET (Jean-Baptiste), « Le minage expliqué aux non-initiés », *Medium* [en ligne], 16 juin 2017, https://medium.com/@JB_Pleynet/le-minage-expliqu%C3%A9-aux-non-initi%C3%A9s-b511b5a33117.

intrusives. Comme en témoigne l'attaque par déni de service distribuée de plusieurs plateformes d'échanges en 2015, laquelle avait créé un dysfonctionnement de l'intégralité du réseau de *Bitcoin*[2198], elles ont pour effet de mettre en péril la stabilité du système attaqué. Le danger est plus grand lorsque ce procédé est utilisé par un attaquant majoritaire. En effet, fort de son pouvoir sur la chaîne et aussi anonyme que le réseau le lui permet, il peut dès lors intercepter des transactions ou opérations spécifiques, et suspendre leur validation de telle sorte qu'elles ne soient jamais validées ni intégrées à un bloc[2199]. L'opération resterait ainsi dans la liste d'attente (*memory pool*) aussi longtemps que le mineur garderait son emprise sur la *blockchain*. Dans cette hypothèse, la partie à un contrat qui n'aurait pas attendu la validation du bloc pour respecter son propre engagement ne recevrait alors jamais la contrepartie de son exécution. Elle ne serait d'ailleurs pas non plus fondée à engager la responsabilité contractuelle de son cocontractant puisque l'opération, de surcroît s'agissant d'un *smart contract*, n'aurait jamais été inscrite sur la chaîne. Sur un autre plan, l'attaquant majoritaire pourrait également viser un utilisateur particulier, et paralyser son nœud, continuellement[2200]. Au-delà de l'intérêt purement financier, ce procédé constitue un moyen simple et efficace de perturber le réseau, ce qui n'est pas sans soulever de multiples difficultés et en particulier juridiques. Gravement compromise, la confiance pourrait également décroître rapidement et créer un phénomène d'abandon de la technologie[2201].

En pratique, ce type d'attaques est rarement mené à l'encontre d'importantes *blockchains* telles que *Bitcoin* et *Ethereum*, et cible plutôt la « petite crypto-monnaie alternative » qui ne requiert pas une puissance de calcul élevée pour miner[2202]. Il en va ainsi, par exemple, de *Krypton*, *Shift*[2203], *BitcoinGold*[2204], *Verge* ou encore *ZenCash*[2205], dont les protocoles ont eu à essuyer quelques-unes de ces attaques. Toutefois, le risque existe et il convient de le prendre en considération, notamment en interrogeant le traitement pénal de ces méthodes.

[2198] « Attaque massive du réseau », *bitcoin.fr* [en ligne], 12 févr. 2014, https://bitcoin.fr/attaque-massive-sur-le-reseau-bitcoin/.
[2199] PAVEL (Ilarion), art. cit., *loc. cit.*
[2200] *Id.*
[2201] *Id.*
[2202] FLORI (Jean-Pierre), art. cit., p. 99.
[2203] REDMAN (Jamie), « Small Ethereum Clones Getting Attacked by Mysterious "51 Crew" », *Bitcoin.com* [online], 4 Sept. 2016, https://news.bitcoin.com/ethereum-clones-susceptible-51-attacks/.
[2204] KALLENBORN (Gilbert), « Un pirate a volé 18 millions de dollars en prenant le contrôle d'une blockchain », *01.net* [en ligne], 28 mai 2018, https://www.01net.com/actualites/un-pirate-a-vole-18-millions-de-dollars-en-prenant-le-controle-d-une-blockchain-1458134.html.
[2205] R. (Rémy), « Attaques 51 % : ZenCash (ZEN) s'ajoute à la liste des victimes », *Journal du Coin* [en ligne], 4 juin 2018, https://journalducoin.com/blockchain/attaques-51-zencash-zen-sajoute-a-la-liste-des-victimes/.

317. L'attaque à 51 % sous l'angle du droit pénal. Assimilables à des « atteintes aux systèmes de traitement automatisé de données », il apparaît que ces attaques pourraient entrer dans le champ d'application des art. 323-1 à 323-5 du C. pén. Ces textes présentent une liste exhaustive des atteintes pouvant faire l'objet d'un traitement pénal. Il s'agit notamment des hypothèses de « suppression ou […] modification de données contenues dans le système, [d'] altération du fonctionnement de ce système » (C. pén., art. 323-1, al. 2), du fait « d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données » (C. pén., art. 323-2, al. 1er), « d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient » (C. pén., art. 323-3, al. 1er), et enfin de « [participer] à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions [précitées] » (C. pén., art. 323-4). En ce qui concerne la participation à une organisation constitutive d'association de malfaiteurs, le Code pénal précise que peut être retenue la responsabilité pénale des personnes morales pour le compte de laquelle l'atteinte a été commise (C. pén., art. 323-6), si bien que les entreprises mettant à disposition un serveur central pourraient également encourir les sanctions pénales prévues. A ainsi été condamné un individu « se réclamant de la mouvance *Anonymous* » aux visas notamment des art. 323-1 (altération du fonctionnement), 323-2 (entrave au fonctionnement) et 323-4 du C. pén. (entente établie en vue d'une atteinte), « pour sa participation à une attaque de déni de service distribué contre le site EDF »[2206].

Si le comportement malveillant d'un mineur majoritaire semble ainsi susceptible de faire l'objet d'une sanction pénale, rien n'est moins certain quant à la simple emprise directement ou indirectement exercée sur l'intégralité de la puissance de calcul d'une *blockchain*. Le fait de prendre le contrôle et d'être susceptible de se servir à mauvais escient de ce pouvoir ne semble effectivement pas constituer une atteinte aux systèmes de traitement automatisé de données, y compris au sens de l'art. 323-1 du C. pén. qui qualifie d'atteinte « le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données ». Pour caractériser l'élément intentionnel de l'infraction commise par l'individu « se réclamant de la mouvance *Anonymous* » et le condamner à six mois de prison avec sursis et à 29 000 € de dommages-intérêt, le TGI de Paris a retenu que la personne coupable était consciente de profiter d'un accès non autorisé au système de traitement automatisé de données et « à l'insu des victimes ». Or, en matière de *blockchain*, une telle concentration n'est pas, à

[2206] TGI Paris, 13e ch. corr. 1, 28 sept. 2016.

l'origine, « frauduleuse » puisque le protocole fait certes obstacle à cette éventualité *via* les principes de distributivité et de décentralisation, mais il ne l'interdit pas explicitement. Les attaques à 51 % ne sont pas constitutives en elle-même d'une infraction au sens de ces textes et nécessiterait, pour être qualifiée ainsi, d'un comportement supplémentaire visant à porter atteinte de manière active au système, d'autant que la sanction préventive n'existe pas.

De la même manière, le fait « d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument » pour commettre une atteinte (C. pén., art. 323-3-1), à l'instar des processeurs ASICs, ne peut, en matière de *blockchain*, constituer un acte de préparation à une atteinte. La pratique a en effet rendu légitime la détention et l'utilisation d'un matériel spécialisé pour le *mining*, de sorte que même les approvisionnements massifs en processeurs effectués par les usines de minage ne semblent pas pouvoir être condamnés, isolément du moins, qu'ils soient ou non destinés ou susceptibles de servir à commettre une infraction.

D'une manière générale, outre la caractérisation des éléments matériels et intentionnels de l'infraction, il apparaît que la qualification des « systèmes de traitement automatisé de données » présente un caractère suffisamment perméable pour s'appliquer en matière de *blockchains*. Il s'avère en effet que la définition de ces systèmes n'a jamais été véritablement[2207] précisée, ni par le législateur ni par la doctrine, et que la jurisprudence comprend volontairement cette notion de manière assez extensive[2208], l'intérêt étant évidemment de permettre au texte répressif de s'adapter aux évolutions de la technique informatique[2209]. En raison de son coût et de ses répercussions économiques,

[2207] Le Sénat avait tenté d'en donner une définition lors de l'élaboration du Nouveau Code pénal, v., Rapp. Sénat n° 3, 2 oct. 1987, au nom de la commission des Lois constitutionnelles, de Législation, du Suffrage universel, du Règlement et d'Administration générale sur la proposition de loi adoptée par l'Assemblée nationale, relative à la fraude informatique, p. 52, https://www.senat.fr/rap/1987-1988/i1987_1988_0003.pdf : « Ensemble composé d'une ou plusieurs unités de traitement automatisé de mémoire, de logiciel, de données, et d'organes d'entrée sortie et de liaisons qui concourent à un résultat déterminé, cet ensemble étant protégé par un dispositif de sécurité ».

[2208] Une auteure constate d'ailleurs qu'elle « recouvre aussi bien une puce électronique de carte de paiement, de téléphone mobile, un site internet, une base de données, ou un autocommutateur téléphonique électronique » [QUEMENER (Myriam), *Le droit face à la disruption numérique : Adaptation des droits classiques - Émergence de nouveaux droits*, éd. Gualino, Hors collection, 2018, p. 98]. – V. également, DEVERGRANNE (Thiébaut), *La propriété informatique*, sous la direction de Jérôme Huet, Paris : Université Panthéon-Assas (Paris II) [en ligne], 2007, pp. 33-34, https://www.donneespersonnelles.fr/these-thiebaut-devergranne.pdf.

[2209] GASSIN (Raymond), « Fraude informatique », *Rép. pén. Dalloz*, v° Fraude informatique, 1995, n° 70 : « l'énumération des éléments de l'ensemble, [...] si longue soit-elle, ne doit pas être considérée comme exhaustive, mais seulement comme exemplative ; les manifestations concrètes de l'informatique sont, en effet, si diverses et ses progrès techniques si rapides qu'une énumération close risquerait d'être vite dépassée ». Le rapport du Sénat [v. : Rapp. Sénat n° 3, préc., p. 52] laissait d'ailleurs lui-même apparaître une telle volonté : « Il ne saurait être question d'énoncer en une liste exhaustive les éléments qui peuvent le composer et qui sont parcourus par le fluide qu'est l'information. Doivent seulement être retenus ceux de ses éléments qui en constituent les caractéristiques essentielles et dont il est vraisemblable qu'ils subsisteront dans l'évolution actuellement prévisible de l'informatique ».

l'appréhension par le droit pénal de ces différentes hypothèses d'attaques serait susceptible d'avoir un effet dissuasif important au sein des *blockchains*.

Il apparaît de plus que l'UE, dans une volonté de renforcer la répression pénale contre la fraude et la contrefaçon des moyens de paiement autres que les espèces[2210], encourage vivement les États membres à sanctionner pénalement « le fait d'effectuer ou de faire effectuer un transfert d'argent, de valeur monétaire ou de monnaie virtuelle, causant ainsi de manière illicite à autrui une perte de propriété dans le but de procurer un gain illégal à l'auteur de l'infraction ou à un tiers » et ce, en « empêchant ou perturbant le fonctionnement d'un système informatique » ou en « introduisant, altérant, effaçant, transmettant ou supprimant des données informatiques, sans en avoir le droit »[2211].

318. Perspectives d'évolution des protocoles : pour une *blockchain* résistante aux prises de pouvoir. Face au danger que représentent ces concentrations de la puissance de minage, des solutions de nature à mettre fin ou à pallier leurs effets actuels ont été proposées[2212]. L'objectif premier de ces recherches est de faire obstacle à toute forme de concentration de mineurs.

En l'état de l'art, la version *Homestead* d'*Ethereum* exploite un système de *Proof of Work* (PoW, preuve de travail)[2213] spécifique nommé « *Ethash* », qui lui permet d'accélérer les processus de vérification et de confirmation des blocs originellement utilisés par le protocole *Bitcoin* et, en principe, de contourner l'utilisation d'ASICs et la concentration des mineurs en *pools*. De plus, le protocole *Ethereum* est programmé pour ajuster automatiquement, et même « dynamiquement », la difficulté du problème de mathématiques lié au processus de vérification de bloc aux puissances de calcul présentes sur le réseau[2214]. Plus encore, *Ethash* fait appel à deux propriétés, à savoir le *memory hardness* et GHOST (*Greedy Heaviest Observed SubTree*). D'une part, le *memory hardness* oblige les mineurs, en parallèle des opérations de vérification nécessitant de la puissance de calcul, à rechercher des données au sein d'un fichier stocké en mémoire, ce qui ne dépend dès lors plus des ASICs dont les performances techniques sont limitées à

[2210] Dir. (UE) n° 2019/713 du Parlement européen et du Conseil, 17 avr. 2019, concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces et remplaçant la décision-cadre 2001/413/JAI du Conseil, *JOUE* L 123/18, 10 mai 2019. – V. également, LASSERRE CAPDEVILLE (Jérôme), « L'avenir de la répression pénale contre certaines fraudes aux instruments de paiement. La transposition de la directive (UE) 2019/713 du 17 avril 2019 », *RD bancaire et fin*. 2021, n° 1, dossier 6, n°s 29-30.
[2211] Dir. (UE) n° 2019/713, art. 6, respectivement a) et b).
[2212] BEAUDEMOULIN (Nathalie) *et a*l., art. cit., p. 31. – V. également, FLORI (Jean-Pierre), art. cit., p. 99.
[2213] Définition *supra* n° 145.
[2214] GALAS (Godefroy), « Analyse et comparaison des mécanismes de consensus dans la blockchain », *Medium* (en ligne), 15 mai 2018, https://medium.com/@godefroy.galas/analyse-et-comparaison-des-m%C3%A9canismes-de-consensus-dans-la-blockchain-f91aee511ea3.

l'exécution des instructions de minage[2215]. D'autre part, GHOST contraint les mineurs à inscrire, au sein de l'en-tête de chaque nouveau bloc en cours de validation, les en-têtes des blocs « orphelins » ou, dans le langage du protocole, « *uncles* » (« oncles »)[2216]. De cette manière, aucune chaîne alternative ne peut, en principe, être valablement créée. Ensemble, ces deux propriétés permettent de réduire les risques de centralisation des puissances de minage et, accessoirement, de ne pas gaspiller le travail fourni par les mineurs. En moyenne, un bloc est créé toutes les quatorze secondes, ce qui rend *de facto* difficile toute modification de la chaîne existante mais également la création d'une chaîne illégitime.

Pour accroître la sécurité du protocole, la Fondation *Ethereum* travaille actuellement sur le déploiement d'une version utilisant, non plus la *Proof of Work*, mais la *Proof of Stake* (PoS), qui correspond à la preuve d'enjeu[2217]. Le principe de ce protocole est d'obliger chaque mineur à calculer et à vérifier des opérations prises au hasard dans la liste d'attente de la chaîne. De cette manière, plus aucun mineur n'aurait accès à la totalité des transactions à inscrire, et chacun n'aurait qu'à renvoyer le résultat qu'il a obtenu[2218].

Autre alternative à la PoW classique notamment en cours de développement chez BitTorrent, la « *Proof of Space* » s'appuierait sur l'espace disque plutôt que sur la puissance de calcul en tant que ressource principale pour le *mining*[2219].

[2215] *Id.* : « le mécanisme *Ethereum* ne demande pas seulement d'effectuer rapidement des calculs, mais également d'aller chercher des données dans un fichier stocké en mémoire qui s'appelle le DAG (*Directed Acyclic Graph* […]), fichier qui est régénéré tous les 30 000 blocs (5 jours) et dont la taille augmente progressivement au fil du temps. Le matériel de type ASIC étant, à l'heure actuelle, incapable de réaliser de nombreuses "petites" opérations de recherche en mémoire en parallèle, l'algorithme de minage *Ethereum* est donc ASIC-résistant ».

[2216] V., Annexe n° 11. Schéma d'un *fork* d'une *blockchain*, p. 443.

[2217] Pour plus de précisions sur le sujet, v., BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », préc. ; ZUNDEL (Jean), POLROT (Simon), MASSERON (Alexis), « Qu'est-ce que la preuve d'enjeu / Proof-of-Stake ? – FAQ par V. Buterin – Traduction française », *Ethereum France* [en ligne], 3 janv. 2017, https://www.ethereumfrance.com/quest-ce-que-la-preuve-denjeu-proof-of-stake-faq-par-v-buterin-traduction-francaise/ : « Le mécanisme de la preuve d'enjeu peut être décrit comme un "minage virtuel". Là où la preuve de travail prévient efficacement les attaques *Sybil* en se fondant sur la rareté et le coût du matériel informatique, la preuve d'enjeu repose sur la crypto-monnaie de la *blockchain* elle-même. Avec la preuve de travail, un participant peut investir 1 000 dollars dans un ordinateur de minage, le brancher, commencer à participer au réseau en produisant des blocs et recevoir une récompense. Avec la preuve d'enjeu, le même participant investit 1 000 dollars en achetant directement la crypto-monnaie de la *blockchain* puis met en dépôt ces crypto-monnaies en utilisant le mécanisme de preuve d'enjeu, qui va ensuite (pseudo-)aléatoirement assigner à ce participant le droit de produire des blocs et de recevoir une récompense. » ; BLOKDYK (Gerardus), *Proof-of-stake: The One Essential Checklist*, ed. CreateSpace Independent Publishing Platform, 2018.

[2218] BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », préc.

[2219] ROSE O'LEARY (Rachel), « Proof of Space: BitTorrent Creator Publishes Eco-Friendly Mining Paper », *CoinDesk* [online], 19 Sept. 2017, https://www.coindesk.com/proof-of-space-bittorrent-creator-publishes-eco-friendly-mining-paper/.

319. Une évolution des pratiques et des objectifs de piratage. Le plein essor de la *blockchain* est conditionné à sa capacité à endiguer les attaques et à corriger ses propres vulnérabilités. La confiance en la technologie ne peut être maintenue si cette dernière ne peut être fiable. Les projets proposant de corriger la faiblesse des principes de décentralisation et de distributivité implantés dans le protocole originel n'en sont qu'à leurs balbutiements si bien qu'aucun n'a encore été introduit dans les *blockchains* actuelles. Mais ils n'en sont pas moins encourageants du point de vue de la protection contre les différentes formes de concentration de mineurs. Toutefois, la pratique révèle que les utilisateurs restent encore très vulnérables aux cyberattaques, d'autant que nombre d'entre elles les visent directement.

§ 2. Des failles dans la cybersécurité du protocole distribué : la vulnérabilité des utilisateurs aux nouvelles méthodes de vols

320. En 2017, plusieurs sites Internet ont été publiquement dénoncés pour avoir usé de la confiance de leurs internautes, et de leur puissance de calcul, afin d'augmenter leur propre puissance de minage sur les *blockchains*[2220]. Pour cela, ils avaient inséré un *script* sur leur site mettant automatiquement à contribution les processeurs des visiteurs à leur insu[2221]. Il en allait ainsi, par exemple, du site *coin-have.com* qui conduisait l'internaute, sans son consentement et le plus souvent sans qu'il s'en aperçoive, à miner pour son administrateur. D'autres sites Internet ont été poursuivis et condamnés à une amende allant jusqu'à 60 000 € sur le fondement de l'art. 323-1 du C. pén. pour avoir installé des enregistreurs de frappe/touche (*keylogger*), capables d'enregistrer les caractères saisis, effectuer des captures d'écran ou encore dresser des listes des actions des utilisateurs, à

[2220] MARTINON (Jacques), « Phénomènes criminels célèbres ou exotiques dans le champ des crypto-actifs », *D. IP/IT* 2019, n° 10.

[2221] LESAGE (Nelly), « De plus en plus de sites minent des crypto monnaies à votre insu quand vous les consultez », *Numerama* [en ligne], 13 oct. 2017, https://www.numerama.com/tech/297685-de-plus-en-plus-de-sites-minent-des-crypto-monnaies-a-votre-insu-quand-vous-les-consultez.html : « Une étude menée par *Adguard* vient de souligner à quel point cette manipulation est devenue monnaie courante. Selon les observations du blog, le minage de crypto monnaie concernerait plus de 500 millions d'internautes, dont l'activité en ligne est exploitée à leur insu. [...] "Nous avons trouvé 220 sites qui lancent un processus de minage lorsqu'un utilisateur ouvre leur page principale, avec une audience agrégée de 500 millions de personnes. Ces gens vivent dans le monde entier ; il y a des sites avec des utilisateurs depuis les États-Unis, la Chine, l'Amérique du sud, l'Europe, la Russie, l'Inde, l'Iran… et la liste continue", précise *Adguard* sur son site. [...] Le blog ajoute que ce chiffre est plutôt impressionnant, compte tenu de la jeune existence de *Coinhive*. En effet, le service a été lancé il y a à peine plus d'un mois, le 14 septembre 2017. [...] Pour la plupart, les sites incriminés se trouvent dans une "zone grise" du net, selon les termes employés par *Adguard* : il s'agit principalement de sites permettant de pirater des fichiers vidéo, de *Torrent Trackers* ou de sites à caractère pornographique. »

l'insu de ces derniers, pour intercepter leurs codes d'accès[2222]. Objet de convoitises, les crypto-monnaies, utilisée originellement comme des récompenses pour le minage, rendent vulnérables les citoyens du web, mais aussi et surtout leurs détenteurs, qui sont la cible d'attaques de plus en plus diverses. Tantôt détournant les propres règles de la *blockchain*, tantôt procédant par piratage des comptes et *wallets*, ces mineurs usent d'impressionnants artifices afin de parvenir à leurs fins. En définitive, tant les risques de *forks* (A) que d'attaques de clés (B) sont susceptibles de porter atteinte à la réputation de la technologie et ainsi mettre en péril son intégrité. D'autant que ces attaques, initialement initiées dans l'objectif de subtiliser les crypto-monnaies détenues au sein des *wallets*, pourraient poser nombre de difficultés si elles parvenaient à intercepter des informations identifiantes, voire l'identité d'utilisateurs.

A. Le risque des forks

321. Alliance des *forks* et de la règle de la chaîne la plus longue. Le risque de *fork*, ou fourche, intervient dans l'intervalle de temps séparant l'émission d'un bloc valide par un nœud et le moment où ce bloc est reçu pour mise à jour de sa version de la chaîne par un autre nœud du réseau. En règle générale, cette durée constitue le « temps de latence » ou « temps de propagation » qui compose toute *blockchain*[2223]. D'un protocole à un autre, ce temps varie entre 12[2224] et 20 secondes[2225]. Puisque les nœuds ne reçoivent pas le bloc en même temps, certains continuent de vérifier leur propre bloc pendant que d'autres ajoutent le bloc vérifié à leur chaîne, si bien qu'ils sont susceptibles de ne pas détenir exactement la même copie de la *blockchain*[2226]. En effet, ce laps de temps peut parfois permettre à deux blocs, *A* et *A'*, d'être simultanément validés et reçus[2227]. Schématiquement, les deux blocs circulent sur le réseau et chaque mineur va continuer à valider les prochains blocs à partir du bloc validé qu'il a reçu, autrement dit, soit à partir de *A*, soit à partir de *A'*[2228]. Cette configuration a pour conséquence de créer un *fork* involontaire[2229].

[2222] V., par exemple, Cass. Crim., 16 janv. 2018, n° 16-87.168.
[2223] *Id.*
[2224] *Id.*
[2225] Rapp. AN n° 1092, rapp. Sénat n° 584, préc.
[2226] MARIN-DAGANNAUD (Gautier), « Comprendre la blockchain Ethereum – Article 1 : Bitcoin, première implémentation de la blockchain (2/2) », *Ethereum France* [en ligne], 13 juin 2016, https://www.ethereum-france.com/comprendre-la-blockchain-ethereum-article-1-bitcoin-premiere-implementation-de-la-blockchain-22/.
[2227] Rapp. AN n° 1092, rapp. Sénat n° 584, préc.
[2228] PLEYNET (Jean-Baptiste), préc.
[2229] V., Annexe n° 11. Schéma d'un *fork* d'une *blockchain*, p. 443.

Pour arrêter ce processus dangereux pour le fonctionnement de la *blockchain*, celle-ci a pour instruction d'attendre qu'un certain nombre de blocs soient validés, et de ne conserver que la chaîne la plus longue, c'est-à-dire la plus longue en termes de blocs[2230]. Il s'agit ici d'une règle de *consensus* permettant à la chaîne d'être automatiquement stabilisée[2231]. Seulement, l'application effective de cette règle conduit à supprimer définitivement l'intégralité des blocs de la chaîne la plus courte[2232]. En d'autres termes, les opérations inscrites dans les blocs validés directement après le bloc qui a créé le *fork* en *A* et *A'* ont une chance sur deux d'être supprimées.

322. Un *bug* possible dans le code : l'accident « *value overflow* » de *Bitcoin*. Ce type d'évènement n'est malgré tout pas commun sur les chaînes, puisqu'en règle générale les développeurs et/ou la communauté mettent en place des systèmes permettant d'éviter, sinon de prévenir ou de corriger, ces défauts. Cependant, le risque n'est pas pour autant écarté, en témoigne l'accident « *value overflow* » subi par le réseau en 2010, au cours duquel le protocole avait validé, par erreur, une transaction créant 184 milliards de *bitcoins*[2233]. Il s'est avéré que le protocole ne supportait pas les transactions aussi importantes, ce qui a révélé un *bug* au niveau de l'algorithme de vérification des transactions[2234]. Certains utilisateurs avaient profité de ce *bug* dans la capacité maximale des transactions pour initier des opérations erronées[2235]. La communauté avait alors installé un correctif afin de plafonner les montants des transactions ultérieures, cependant, cinq heures s'étaient écoulées et certains nœuds, non corrigés, ont continué de miner la chaîne initiale[2236]. La règle de la chaîne la plus longue a fini par imposer la nouvelle version corrigée de la chaîne, ce qui a permis d'annuler les transactions frauduleuses, mais a également provoqué la suppression de toutes les transactions contenues dans les blocs de la chaîne non corrigée. À raison d'un bloc inscrit par tranche de dix minutes, et, en moyenne, de 1 500 transactions par bloc[2237], près de 45 000 opérations ont donc été supprimées.

[2230] ANTONOPOULOS (Andreas M.), *Mastering Bitcoin*, ed. O'Reilly, 2nd edition, 2017, p. 174.
[2231] FLORI (Jean-Pierre), art. cit., p. 99.
[2232] Rapp. AN n° 1092, rapp. Sénat n° 584, préc.
[2233] *Id.*
[2234] *Id.*
[2235] *Id.*
[2236] *Id.*
[2237] V., blockchain.com, Explorer > Block Details > Average Transactions Per Block (valeur calculée sur les trois dernières années écoulées).

323. Une attaque accessible à 30 % de force de calcul. Semblable à l'une des possibilités de « *double-spend attack* » de l'attaque à 51 %, sans les 51 % de puissance de calcul[2238], cette entreprise n'est pas assurée de réussir et a même davantage de chances d'échouer[2239], mais le risque existe et doit malgré tout être appréhendé. Ainsi est-il possible qu'un mineur détenant 30 % de la puissance de minage sur une chaîne, tente une attaque et réussisse à imposer un bloc concurrent (*A'*) au bloc valide (*A*) contenant par exemple une version modifiée de sa transaction initiale et éventuellement une double dépense. Dans ces circonstances, la chaîne étant immédiatement divisée (*fork*), les autres mineurs du réseau reçoivent à part quasiment égale le bloc *A* et le bloc *A'* qu'ils vont continuer à miner sur leurs chaînes respectives. Le mineur peut récupérer la double mise en la rassemblant dans une même chaîne et en fonction de sa longueur, la règle de la chaîne la plus longue déterminera automatiquement la version qui sera adoptée en tant que chaîne principale[2240]. Si la chaîne modifiée remplace la version initiale, la modification est alors définitivement validée[2241]. En dehors de la recherche de la double dépense ou de l'altération d'une opération, un auteur évoque la possibilité de censure d'une transaction que le mineur ne voulait pas publique[2242]. Comme le constate Gautier Marin-Dagannaud, « la règle de la chaîne la plus longue est bien pratique pour stabiliser la chaîne de blocs et garantir son unicité, mais elle ouvre aussi la porte à une nouvelle forme de *double-spend attack* »[2243], présentant dès lors le même type de risques pour les utilisateurs qu'une attaque à 51 %.

324. Un risque à relativiser pour les contractants. S'agissant des parties ayant conclu un contrat sur la chaîne, éventuellement par le biais d'un *smart contract*, le problème de ce type d'attaque réside dans la création de « blocs orphelins » susceptibles d'être supprimés de la chaîne[2244]. Outre les conséquences précitées en matière d'attaque majoritaire[2245], ces dérives du protocole posent d'importantes questions juridiques. Par exemple, si une partie à un contrat prévoyant des pénalités de retard exigibles le jour

[2238] BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », art. cit.
[2239] MARIN-DAGANNAUD (Gautier), « Comprendre la blockchain Ethereum – Article 1 : Bitcoin, première implémentation de la blockchain (2/2) », art. cit.
[2240] Cette règle n'aurait pas eu à jouer au cours d'une attaque à 51 % puisque l'attaquant aurait pu directement valider ses blocs et créer une chaîne plus longue.
[2241] PAVEL (Ilarion), art. cit., p. 22.
[2242] FLORI (Jean-Pierre), art. cit., p. 100.
[2243] MARIN-DAGANNAUD (Gautier), « Comprendre la blockchain Ethereum – Article 1 : Bitcoin, première implémentation de la blockchain (2/2) », art. cit.
[2244] PAVEL (Ilarion), art. cit., p. 21 ; V. également, Annexe n° 11. Schéma d'un *fork* d'une *blockchain*, p. 443.
[2245] *Supra* n° 316.

suivant la date de règlement dans le cas où les sommes dues sont réglées après cette date, a initié un paiement qui, en raison d'un *fork*, est voué à être supprimé car inscrit dans le bloc de la chaîne la plus courte, engagerait-elle sa responsabilité contractuelle ? D'autant que la preuve de sa transaction ne serait plus inscrite de manière immuable sur la *blockchain*. Hormis la nécessité à nouveau d'anticiper dans un *smart contract* toutes les difficultés pouvant survenir au cours de la relation contractuelle[2246], la technologie doit renforcer la sécurité de son protocole. *Quid* d'un mineur-cocontractant, animé d'intentions malveillantes, qui tenterait par le biais de cette attaque d'apporter des modifications unilatérales à son engagement ? Ilarion Pavel souligne d'ailleurs que « plus un réseau présente des phénomènes de fourche, et plus il est vulnérable aux attaques »[2247].

C'est ainsi que Vitalik Buterin a muni, dès sa conception, son protocole de la propriété GHOST (*Greedy Heaviest Observed SubTree*)[2248]. En obligeant les mineurs à inscrire, au sein de l'en-tête de chaque nouveau bloc en cours de validation, les en-têtes des blocs « orphelins » ou, dans le langage du protocole, « *uncles* » (« oncles »), aucune chaîne alternative ne peut, en principe, se substituer à la chaîne principale, et aucun bloc ne peut être laissé dans l'oubli. Cette implémentation est source de sécurité, en particulier en matière de *smart contracts*, lesquels s'exécutent le plus souvent par le biais de la *blockchain Ethereum*.

Par ailleurs, il convient d'évoquer la probabilité d'une telle attaque, non vis-à-vis de son organisation technique, mais en termes de rapport coût/avantage[2249]. En effet, cette attaque, parfaitement envisageable, se révèle cependant particulièrement inopportune en raison des nombreuses incertitudes entourant sa réalisation et de l'importance de l'investissement qu'elle requiert dès lors que moins de 51 % du *hash rate* sont détenus.

Il n'empêche que, dans le risque d'une telle éventualité, il apparaît raisonnable d'attendre quelques blocs avant de considérer une transaction comme étant définitive[2250].

325. L'évolution des pratiques de piratage ont également mené les *hackers* à explorer de nouvelles techniques leur permettant de prendre possession des identifiants et bi-clés des utilisateurs de *blockchains*. Ces vols, initialement initiés dans l'objectif de subtiliser les crypto-monnaies détenues au sein des *wallets*, pourraient poser nombre de difficultés

[2246] Sur la question, *supra* n°s 225-226.
[2247] PAVEL (Ilarion), art. cit., *loc. cit.*
[2248] Pour plus d'informations sur le sujet, v., BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », préc.
[2249] ANTONOPOULOS (Andreas M.), *op. cit.*, p. 173.
[2250] MARIN-DAGANNAUD (Gautier), « Comprendre la blockchain Ethereum – Article 1 : Bitcoin, première implémentation de la blockchain (2/2) », art. cit.

si ces derniers contenaient des informations identifiantes, voire l'identité de leurs utilisateurs.

B. Le risque des attaques de clés

326. Une situation irrémédiable : l'importance des clés cryptographiques au sein du réseau des *blockchains*. Un portefeuille numérique, ou *wallet*, constitue une forme de compte bancaire pour crypto-monnaies. En règle générale, le protocole *Bitcoin* permet aux utilisateurs de recourir à deux types de portefeuilles, à savoir les portefeuilles *software* notamment proposés par les plateformes de *trading* de crypto-monnaies, et les portefeuilles *hardware*. Tandis que les *software wallets* sont, le plus souvent, connectés à Internet (*online wallet*) et sont par conséquents accessibles par le biais d'un ordinateur ou d'un smartphone, les *hardware wallets*, parce qu'ils consistent en un appareil spécifiquement destiné à la gestion de crypto-monnaies, ne peuvent stocker celles-ci qu' « à froid », c'est-à-dire en dehors de toute connexion Internet (*offline wallet*, ou *cold wallet*)[2251]. Quel que soit son type, un portefeuille, au moment de sa création, génère une graine de récupération (*root seed*)[2252] à partir de laquelle est créé un couple de clés (bi-clés) composé, d'une part, de la clé publique destinée à réceptionner les transactions et informations transmises sur le réseau et, d'autre part, de la clé privée associée, employée pour déchiffrer les informations reçues[2253]. Il s'avère qu'en pratique les utilisateurs ne divulguent jamais ces clés. En effet, dès lors qu'un utilisateur s'apprête à initier une transaction, il va demander à son portefeuille de dériver un nouveau bi-clés « enfant » du couple de clés « parent ». Les adresses publiques dérivées seront donc utilisées en tant qu'adresses de réception, tandis que les clés privées associées permettront, individuellement, d'accéder aux crypto-monnaies transférées à chacune des adresses, et que la clé privée « parent » permettra d'accéder à celles contenues dans toutes les adresses. Finalement, il apparaît que la plupart des utilisateurs ne saisissent pas non plus

---

[2251] « Comment choisir et créer un portefeuille de crypto-monnaies », *Coin24* [en ligne], https://coin24.fr/dictionnaire/portefeuilles-wallets/

[2252] Cette séquence, constituée de douze à vingt-quatre mots en anglais aléatoirement déterminés par l'algorithme, est fournie sous la forme d'une *seed phrase*, qui est une phrase mnémonique, ou mnémotechnique facilitant sa mémorisation. Nombre de phrases mnémoniques ont été inventées, par exemple, le « *Piem* », qui constitue un mélange de « *Pi* » et de « *poem* », permet, *via* le nombre de lettres contenu dans chaque mot, de mémoriser les huit premières décimales de Pi : « *May I have a large container of coffee beans ?* » (π = 3,14159265). – V., « Comment choisir et créer un portefeuille de crypto-monnaies », art. cit. ; « Bitcoin wallet », *BTC Direct* [en ligne], https://btcdirect.eu/fr-fr/bitcoin-wallet.

[2253] Pour une définition générale de la cryptographie asymétrique, *supra* n° 99. – V. également, Annexe n° 6. Schéma exposant la provenance des bi-clés, p. 438. – V. également, Maguayo, « Update bip-0032.mediawiki », *GitHub* [online], 25 Oct. 2018, https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki#Specification_Key_.

leur clé privée pour transférer ou récupérer des *bitcoins*, ils doivent uniquement définir un code PIN verrouillant l'accès au portefeuille, lequel prend la forme d'un « trousseau de clés » automatique[2254].

Cependant, qu'adviendrait-il si une clé privée, voire la clé privée « parent » d'un utilisateur, était subtilisée ? À l'instar des hypothèses de « perte » de clés privées, qui s'élèvent d'ailleurs actuellement à 20 % des unités de crypto-monnaies disponibles, soit l'équivalent de presque 3,8 millions de *bitcoins*[2255], le vol d'une clé privée équivaut à la disparition définitive de l'intégralité des crypto-monnaies disponibles à l'adresse ou aux adresses générées par la clé[2256]. En effet, « une clé privée permet d'accéder, de gérer, de dépenser la crypto-monnaie détenue à l'adresse associée. Quiconque la détient dispose des bitcoins »[2257]. Or, de multiples dangers guettent ces clés, tels que des virus, des messages électroniques « douteux », des fichiers attachés dans les e-mails, des sites web « suspects »[2258]… Il est important, en la matière, de prendre certaines précautions, telles qu'utiliser plusieurs *wallets* afin de réduire les conséquences de potentielles attaques qui toucheraient directement les plateformes de portefeuilles de crypto-monnaies[2259], ou utiliser plusieurs clés privées voire privilégier les systèmes de multi-signatures[2260]. Mais ces précautions ne suffisent pas toujours.

327. Profil de risque des *online wallets*. Au cours de son inscription sur le protocole *Bitcoin*, le nouvel utilisateur peut choisir d'être un « client complet », ce qui suggère qu'il télécharge l'intégralité de la chaîne, ou de faire appel à des portefeuilles en ligne qui proposent des « services client web ». Cependant, il s'avère que ces plateformes de

---

[2254] *Id.*

[2255] HELLEU (Guillaume), MASURE (Anthony), « Total Record. Les protocoles blockchain face au post-capitalisme », *Multitudes* 2018/2, n° 71, p. 74.

[2256] PAVEL (Ilarion), art. cit., p. 23.

[2257] BLONDEAU (Alison), « Le juge civil face au secret entourant le système de clé privée sur blockchain », *in* NEVEJANS (Nathalie) (dir.), *Données et technologies numériques. Approches juridique, scientifique et éthique*, éd. mare & martin, coll. Droit & Science politique, 2021, p. 157.

[2258] Pour plus de détails sur le sujet, v. le site, https://cryptoast.fr/comment-securiser-et-stocker-crypto-monnaies/.

[2259] LE GUEN (Olivier), « Questions à Olivier Le Guen sur la perquisition et la saisie des crypto-actifs », *D. IP/IT* 2019, n° 10, p. 541.

[2260] PAVEL (Ilarion), art. cit., *loc. cit.* : « Dans un monde ou les cyberattaques sont de plus en plus fréquentes, il faut renforcer les mesures de cybersécurité habituelles : mettre à jour les logiciels et les antivirus, ne pas répondre aux messages électroniques douteux ou ne pas cliquer sur les fichiers attaches, éviter de naviguer sur des sites web suspects, ne pas télécharger des fichiers provenant de sources non vérifiées. Il est conseillé d'éviter les bourses de change ou les portefeuilles en ligne fournissant des services client web, car ils n'offrent pas encore suffisamment de garanties de sécurité pour entreposer l'argent : il est préférable d'être "client complet" afin de disposer de l'ensemble de la *blockchain*. Il est aussi recommandé d'utiliser plusieurs portefeuilles, d'effectuer les transactions de faibles montants à partir d'un terminal mobile (client léger), moins sécurisé, d'effectuer celles de montants élevés à partir d'un ordinateur fixe (client complet). Le fait d'utiliser des transactions multi-signatures à partir de plusieurs clés privées réparties sur plusieurs supports différents (ordinateur de bureau, smartphone) augmente également la sécurité. »

trading de crypto-monnaies constituent les principaux objectifs des attaques des pirates de *blockchains*[2261] alors même qu'en l'état de l'art, elles ne bénéficient pas d'une protection suffisante[2262]. Nombre de ces plateformes, par manque de sécurité, exposent directement leurs utilisateurs. Il en va ainsi de *Mtgox*, volée de 650 000 dollars en *bitcoins* en 2017[2263], ou encore de *MyEtherWallet* qui, à la suite d'une attaque ayant été exécutée par une adresse IP basée en Russie *via* une extension de *Google Chrome*, a perdu plus de 365 000 dollars en *ethers* en 2018[2264]. Seulement, lorsque le *wallet* n'est plus en état de restituer tant les clés que le montant volé en crypto-monnaies, les utilisateurs spoliés ne disposent d'aucun recours[2265].

328. Des attaques de bibliothèques de *wallets* : les « *side channel attacks* ». Il est possible de subtiliser des informations telles que des bi-clés au sein de systèmes de génération de clés privées de type DSA/ECDSA, comme en témoigne la publication de NCC Group qui l'a découverte en 2018[2266]. En pratique, cette attaque est permise par une faille existante au sein de certaines bibliothèques des *wallets* qui ne pratiquent pas le calcul des clés de façon constante[2267]. Au cours de la génération d'une nouvelle clé privée, les bibliothèques stockent temporairement en mémoire cache des informations sur l'utilisateur, telles que son activité, sa consommation, son temps de réponse, etc. L'objectif de l'attaquant est alors de se connecter au canal auxiliaire à partir de la même machine que l'utilisateur victime, par exemple *via* le *cloud*, et de profiter de cette brève ouverture pour récupérer une ou plusieurs clés privées, ainsi que les informations associées[2268]. Cette attaque par canal auxiliaire (*side channel attack*) a été identifiée sur la base d'une faiblesse d'un modèle de *wallet* déjà corrigée en 2015.

[2261] MARTINON (Jacques), art. cit. : « Entre 2017 et 2018, le groupe Lazarus, réputé proche de la Corée du Nord, serait responsable du vol de 571 millions de dollars sur un total de 882 millions de dollars de crypto-actifs dérobés sur des plateformes d'échange, soit près de 65 % de la somme totale au niveau mondial. »
[2262] FLORI (Jean-Pierre), art. cit., p. 100.
[2263] AÏT-KACIMI (Nessim), « Mtgox : le mystère des 650.000 bitcoins évaporés », *Les Echos* [en ligne], 19 juill. 2017, https://www.lesechos.fr/19/07/2017/lesechos.fr/030454291283_mtgox---le-mystere-des-650-000-bitcoins-evapores.htm.
[2264] « MyEtherWallet: le gestionnaire de cryptomonnaies victime d'une attaque », *Les Numériques* [en ligne], 11 juill. 2018, https://www.lesnumeriques.com/vie-du-net/myetherwallet-gestionnaire-cryptomonnaies-victime-attaque-n76047.html.
[2265] FLORI (Jean-Pierre), art. cit., p. 100.
[2266] GUITTARD (Grégory), « Une faille de sécurité frappant la génération de clés cryptographiques », *Le Journal du Coin* [en ligne], 18 juin 2018, https://journalducoin.com/blockchain/faille-de-securite-contenue-frappant-les-signatures-cryptographiques-mais-pas-vos-chers-hardware-wallets/.
[2267] Pour la liste de ces bibliothèques, v., KEEGAN (Ryan), « Return of the Hidden Number Problem », *NCC Group Whitepaper* [online], 13 Jun. 2018, p. 12, https://medium.com/r/?url=https%3A%2F%2Fwww.nccgroup.trust%2Fglobalassets%2Four-research%2Fus%2Fwhitepapers%2F2018%2Frohnp-return-of-the-hidden-number-problem.pdf.
[2268] Pour plus de précisions sur le procédé d'attaque, v., *Ibid*., pp. 3-9.

En effet, la communauté avait découvert une faille permettant de récupérer la clé privée qui donne accès aux *bitcoins* stockés sur TREZOR, un *hardware wallet*, en utilisant des canaux secondaires tels que les fluctuations de puissance, les radiations électromagnétiques ou similaires, qui peuvent être reproduites par le biais d'un oscilloscope[2269]. Schématiquement, l'attaque consistait à mesurer la consommation d'énergie du portefeuille TREZOR afin de détecter les phases d'exécution du code et de génération de bi-clés, en copier l'empreinte en bits, et tester plusieurs empreintes différentes afin de déterminer celle qui correspond et reconstituer la clé privée de 128 bits. En réaction à ces résultats, une protection par code PIN a été ajoutée pour le calcul des clés publiques. D'autres travaux ont par la suite confirmé ce type de vulnérabilités au sein notamment de la librairie *iOs CoreBitcoin*[2270].

329. Des attaques par tromperie : le « *typo-squatting* » et l'attaque homographe IDN. Le *typo-squatting*, autre méthode de vol de bi-clés, consiste à dupliquer un site web en inversant ou modifiant un ou plusieurs caractères de son nom de domaine de sorte qu'il ait la même apparence, mais permette de récupérer des informations telles que les identifiants de *wallet*, code PIN, ou même clé privée d'utilisateurs. Par exemple, il peut s'agir de reproduire le site MyEtherWallet.com, et de remplacer les « l » par la lettre majuscule « I », à savoir « MyEtherWaIIet.com ». En réalité, les cas de *typo-squatting* reposent sur des « erreurs typographiques naturelles couramment commises lors de la saisie manuelle d'une URL », telles que confondre « l » et « I », mais également « 0 » et « O », « i » et « j » du fait de leur similitudes, en particulier en fonction de la police de caractères utilisée, ou de leurs emplacements sur le clavier[2271].

Reposant sur les mêmes objectifs, l'attaque homographe IDN utilise quant à elle les similitudes entre les systèmes d'écriture des jeux de caractères ASCII afin d'obtenir un hyperlien visuellement indiscernable[2272]. Il en va ainsi des lettres latines « e » et « a », assimilables aux lettres cyrilliques « e » et « a », mais également de la lettre « O » qui n'a pas reçu le même code ASCII en grec, latin et cyrillique et qui, pourtant, est visuellement identique dans chacun d'eux.

[2269] HOENICKE (Jochen), « Extracting the Private Key from a TREZOR... with a 70 $ Oscilloscope », *Jochen-Hoenicke.de* [online], 1st Nov. 2018, https://jochen-hoenicke.de/crypto/trezor-power-analysis/. Pour ls discussions sur *Reddit*, v., https://www.reddit.com/r/Bitcoin/comments/2s2iym/trezor_vs_ledger_wallet/cnlldv2/.

[2270] Pour plus de précisions sur les vulnérabilités découvertes en 2016 au sein de la librairie *iOs CoreBitcoin*, v., GENKIN (Daniel), PACHMANOV (Lev), PIPMAN (Itamar), TROMER (Eran), YAROM (Yuval), « ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels », [online], 18 Aug. 2016, https://eprint.iacr.org/2016/230.pdf.

[2271] Wikipedia, v° Attaque homographe IDN, https://fr.qaz.wiki/wiki/IDN_homograph_attack.

[2272] *Id.*

L'utilisateur, ainsi trompé, navigue sur le site dupliqué et saisi ses identifiants de *wallet*, son code PIN, une clé privée, … qui sont automatiquement redirigés vers l'attaquant.

330. Des attaques utilisant les réseaux de communication traditionnels : le « *SIM hijacking* ». Il est désormais possible de détourner des cartes SIM afin de dérober des millions de dollars en *bitcoins* mais également en autres crypto-monnaies. Techniques du « *SIM hijacking* » ou du « *swap SIM* »[2273], l'idée est de voler les numéros de téléphones de personnes détenant des crypto-monnaies en transférant dans une nouvelle carte SIM les données contenues dans la carte SIM de la personne, et d'exiger ensuite le paiement d'une rançon en crypto-monnaies[2274]. Les utilisateurs visés sont plus particulièrement des personnes travaillant directement dans le monde de la crypto-monnaie. En juillet 2018, un homme de 20 ans a été arrêté par la police de Californie, soupçonné de faire partie d'un groupe qui a ainsi volé 5 millions de dollars à plus de quarante victimes[2275]. L'enquête qui a suivi la mise en accusation par Michael Terpin, fondateur des plateformes *Transform Group* et *BitAngels*, de la société de télécommunications américaine AT & T à la suite d'un vol de 23 millions de dollars[2276], a révélé que cette dernière avait connaissance des arnaques développées sur son réseau sans toutefois protéger les numéros et identifiants de ses clients[2277].

331. Fraude et escroqueries : les « *giveaways* » et « systèmes de Ponzi ». Les *crypto-hackers* usent également de méthodes d'escroquerie consistant à proposer, et même promettre aux utilisateurs des placements financiers intéressants[2278]. Ils reçoivent les

[2273] BUNTINX (JP), « SIM Hijacking Nets Criminal $5 Million by Targeting Cryptocurrency Users », *Libe Bitcoins News* [online], 1st Aug. 2018, https://www.livebitcoinnews.com/sim-hijacking-nets-criminal-5-million-by-targeting-cryptocurrency-users/ ; « Détournement de cartes SIM : un investisseur poursuit un opérateur en justice après s'être fait voler 23 millions de dollars de crypto-monnaies », *Crypto-France* [en ligne], 15 août 2018, https://www.crypto-france.com/sim-hijacking-poursuite-at-t-vol-crypto-monnaies/.
[2274] LIAO (Shannon), « Customer sues AT&T for negligence over SIM hijacking that led to millions in lost cryptocurrency », *The Verge* [online], 15 Aug. 2015, https://www.theverge.com/2018/8/15/17695132/att-sued-over-lost-cryptocurrency-sim-swap-theft.
[2275] « Détournement de cartes SIM : un investisseur poursuit un opérateur en justice après s'être fait voler 23 millions de dollars de crypto-monnaies », préc.
[2276] TERPIN (Michael), « Cryptocurrency Entrepreneur and Investor Michael Terpin Sues "Too Big to Care" AT&T for Permitting $23.8 Million Theft in "SIM Swap" Scam by Authorized Agent », *West* [online], 15 Aug. 2015, http://globenewswire.com/news-release/2018/08/15/1552594/0/en/Cryptocurrency-Entrepreneur-and-Investor-Michael-Terpin-Sues-Too-Big-to-Care-AT-T-for-Permitting-23-8-Million-Theft-in-SIM-Swap-Scam-by-Authorized-Agent.html.
[2277] Pour plus de précisions sur le sujet, v. notamment, FRANCESCHI-BICCHIERAI (Lorenzo), « Bitcoin Investor Sues AT&T After Losing $23 Million In SIM Swap Hack », *MotherHead* [online], 15 Aug. 2015, https://motherboard.vice.com/en_us/article/pawwkz/bitcoin-investor-sues-att-23-million-sim-swap-hack.
[2278] *Id*. – V. également, « Kaspersky : 2,3 millions de dollars de crypto-monnaies dérobés au cours du 2ème trimestre » (version française), *Crypto-France* [en ligne], 15 août 2018, https://www.crypto-france.com/vol-2-3-millions-dollars-crypto-monnaies-deuxieme-trimestre-2018/ : « Au cours du deuxième

fonds, les transfère sur des adresses personnelles, puis ne les retournent jamais[2279]. Appelée « *giveaways* »[2280], cette méthode a ainsi permis à des attaquants de subtiliser 2,3 millions de dollars en crypto-monnaies à nombre d'utilisateurs peu avertis[2281]. Vantant un rendement de 10 % annuel, les escroqueries dîtes « de type Ponzi »[2282] ont également causé plus de 4 milliards de dollars de préjudices à des millions d'investisseurs de crypto-actifs *via BitConnect* ou encore *OneCoin*[2283]. Ces fraudes constituent des montages financiers élaborés sur une chaîne d'emprunt, consistant à rémunérer les investissements des épargnants actuels avec les sommes investies par les nouveaux épargnants.

332. Il existe nombre d'autres attaques, telles que les attaques de signatures, les contrefaçons, les attaques à messages, les attaques par force brute[2284], ou encore les boucles conditionnelles et les corruptions accidentelles[2285]… En outre, il apparaît raisonnable de considérer qu'aucune infrastructure de gestion de clés n'est véritablement inviolable. Ces risques d'intrusions malveillantes mettent en exergue les faiblesses inhérentes de la technologie, laquelle semble éprouver des difficultés à sécuriser ses utilisateurs dès lors que ces derniers utilisent des services tiers à la *blockchain*. Sa décentralisation semble de surcroît directement exposer ces derniers, qui deviennent à leur tour vulnérables. Ces multiples risques résultant des actions de certains individus ne proviennent cependant pas que d'attaques informatiques. En effet, l'éventuelle présence de l'Homme au sein du fonctionnement des *blockchains* par le biais des Oracles pose également un problème de fiabilité au sens où elle remet directement en question l'efficacité de l'interaction entre la *blockchain* et le monde réel.

---

trimestre, les internautes brésiliens ont été victimes de 15,51 % de ces attaques. Le pays est suivi par la Chine et la Géorgie (14,44 % chacune), puis par le Kirghizstan (13,6 %) et la Russie (13,27 %). »

[2279] *Id.*

[2280] VERGELIS (Maria), DEMIDOVA (Nadezhda), SHCHERBAKOVA (Tatyana), « Spam and phishing in Q2 2018 », *SecureList-KasperskyLab* [online], Aug.14, 2018, https://securelist.com/spam-and-phishing-in-q2-2018/87368/.

[2281] BAYDAKOVA (Anna), « Kaspersky: Cryptocurrency Scammers Stole $2.3 Million in Q2 », *CoinDesk* [online], 15 Aug. 2018, https://www.coindesk.com/kaspersky-cryptocurrency-scammers-stole-2-3-million-in-q2/.

[2282] Ce type d'escroqueries tire son nom de Charles Ponzi, escroc américain des années 1920 qui a mis en place un tel système de cavalerie à Boston, escroquant plus de 40 000 personnes pour 15 millions de dollars [v., notamment, ZUCKOFF (Mitchell), *Ponzi's Scheme: The True Story of a Financial Legend. Random House*, ed. Random House Trade Paperbacks, 2006].

[2283] V. notamment, MARTINON (Jacques), art. cit.

[2284] Pour plus de précisions sur ces diverses attaques, v. notamment, FOUQUE (Pierre-Alain), *op. cit.*, pp. 15-17.

[2285] Pour plus de précisions, v., LORRE (Pierre-Marie), « Blockchain : évolution ou révolution pour les contrats en France ? », Courbevoie : Institut Léonard de Vinci [en ligne], 2016, pp. 48-49, https://www.forumatena.org/files/livresblancs/LORE_BLOCKCHAIN_CONTRATS-FA.pdf.

Section 2. Un fonctionnement limité par la présence imposée des Oracles

333. À la fois source d'autonomie et de méfiance, les Oracles semblent limiter le fonctionnement de la technologie *blockchain* autant que compromettre son intégrité, son efficacité, et finalement son utilité. Originellement instituée pour permettre à des parties à un contrat de pouvoir se faire confiance à travers elle, la *blockchain* risque pourtant sa réputation et la confiance algorithmique qu'elle œuvre à édifier en permettant à des entités extérieures de réinjecter en son cœur la faillibilité humaine contre laquelle elle lutte. Alors que semble pour le moment s'imposer l'idée que le tiers de confiance est malgré tout un relais indispensable pour la *blockchain*, comme le souligne Mustapha Mekki, « les moyens sont nombreux et les technologies doivent pouvoir s'adapter afin que l'intervention d'un Oracle ne soit pas le cheval de Troie de la *blockchain* »[2286].

À cet effet il conviendra d'apprécier la fiabilité de ces yeux extérieurs à la *blockchain* (§ 1), lesquels opèrent un déplacement de la confiance initialement donnée à la technologie par les utilisateurs (§ 2)… à moins que la technologie ne parvienne effectivement à s'adapter.

§ 1. Fiabilité des yeux extérieurs à la *blockchain*

334. Dans son acception la plus commune, l'oracle est une personne qui pratique la divination. Du latin *orare* qui signifie parler, le mot « oracle » désigne la réponse d'une divinité donnée aux Hommes par l'intermédiaire de la personne, femme ou homme, qui la consulte [2287]. De tels intermédiaires ont ainsi permis de consulter les dieux dans la Grèce antique, faisant de Delphes la capitale de la divination grecque. Au-delà de l'aspect religieux et des sciences occultes, il apparaît que l'Oracle adopté par la *blockchain* interroge quant à lui la réalité du monde extérieur à celle-ci, pour ensuite lui transmettre ses réponses. Il s'agira d'abord de revenir sur cette notion appliquée à la technologie pour présenter le fonctionnement de ces systèmes d'Oracle, lesquels se proposent d'incarner un outil de recherche instantanée d'informations au service de la *blockchain* (A), avant d'examiner leur fiabilité en évaluant notamment les risques de centralisation et en étudiant la question de la responsabilité (B).

[2286] MEKKI (Mustapha), « Le smart contract, objet du droit (Partie 2) », *D. IP/IT* 2019, n° 1, p. 27.
[2287] CNRTL [en ligne], v° Oracle, https://www.cnrtl.fr/definition/oracle.

335. Définition. Tout au long de son exécution, un *smart contract* a besoin d'informations provenant du monde réel afin de déclencher une action prédéfinie dans la chaîne de blocs. En pratique, il s'agit pour le *smart contract*, par exemple, d'obtenir une information concernant le suivi d'un colis sur un site de livraison (« Le colis *X* est en cours de livraison ; a été livré »), ou de se procurer le cours des devises afin de déterminer le taux de change entre deux devises (« Le cours actuel de l'euro est de… ; le cours actuel du dollar américain est de… ; le rapport d'échange entre EUR/USD est de… »). Les questions « Quelle température fait-il ? », « À quelle heure l'avion a-t-il décollé/atterri ? », sont finalement susceptibles de se poser à la *blockchain* lorsque celle-ci met en œuvre des *smart contracts* alors même que, comme le constate Simon Polrot, « la *blockchain* est, […] par construction, aveugle au monde extérieur »[2288]. Pour pouvoir recourir à des données externes en temps réel, la *blockchain* peut actuellement procéder de deux manières. D'une part, si les informations que requière le *smart contract* sont inscrites sur la chaîne, cette dernière pourra effectuer une vérification en interne sans exiger d'instruction spécifique[2289]. Il en va ainsi, par exemple, pour établir la balance des paiements d'une adresse de transaction[2290]. D'autre part, si les informations recherchées émanent d'une source externe, la *blockchain* devra faire appel à un service extérieur capable de lui fournir[2291]. Néanmoins, dès lors que la technologie utilise une source externe et qu'elle intègre une donnée y figurant directement dans un bloc de la chaîne, le contenu de ce bloc est dépendant de ce service extérieur. Ainsi, si le service est suspendu, temporairement voire définitivement, le *hash* du bloc contenant la donnée récupérée, rendu techniquement inaltérable[2292], est automatiquement impacté[2293]. Modifié, son contenu ne serait plus valide, de même que son *hash* ainsi que tous les *hashs* des blocs qui le suivent, ce qui décrédibiliserait la chaîne entière.

Afin d'éviter ce cercle vicieux, la Fondation Ethereum a doublé son protocole d'un système nommé « Oracle », capable de solliciter des données externes[2294]. L'Oracle est ce point de contact entre la chaîne de blocs et le monde extérieur, réel, dans lequel

[2288] POLROT (Simon), « Les Oracles, lien entre la blockchain et le monde », *Ethereum France* [en ligne], 13 sept. 2016, https://www.ethereum-france.com/les-oracles-lien-entre-la-blockchain-et-le-monde/.
[2289] *Supra* n° 68.
[2290] Pour une définition de la balance des paiement et les vérifications quant à la solvabilité des adresses d'un émetteur, *supra* n° 143.
[2291] GUILHAUDIS (Élise), art. cit., p. 5.
[2292] Pour plus de précisions sur le procédé et les conditions d'inaltérabilité du *hash*, *supra* n°s 104-105, 145.
[2293] POLROT (Simon), « Les Oracles, lien entre la blockchain et le monde », art. cit.
[2294] BUTERIN (Vitalik), « Ethereum and Oracles », *Ethereum Blog* [online], 22 Jul. 2014, https://blog.ethereum.org/2014/07/22/ethereum-and-oracles/.

vivent ses utilisateurs[2295], de sorte qu'il est finalement raisonnable de considérer qu'il constitue ce que représentent les yeux pour l'Homme.

336. Définition technique et fonctionnement des Oracles d'*Ethereum*. Les développeurs ont fait usage des spécificités techniques du protocole d'*Ethereum* qui lui permettent notamment de coder des programmes simples comme complexes[2296], mais également de traduire et reformuler n'importe quel autre langage informatique[2297], et donc de pouvoir recourir à des données provenant de sources extérieures et en temps réel afin de déclencher une action prédéfinie dans la chaîne de blocs. Tel qu'il a été mentionné précédemment, Turing-complet et proche du langage *JavaScript*[2298], *Solidity* est également un langage de programmation de haut-niveau[2299]. Cette énième spécificité permet à la *blockchain* de supporter la mise en œuvre d'un système dynamique d'inscription d'actes auto-exécutants[2300] et donc de développer des applications adaptées à la logique « auto-application » requise par les *smart contracts* pour consolider des transactions, en particulier avec des appels d'Oracles[2301].

Concrètement, dès lors que les parties concluent un *smart contract*, les services d'un Oracle peuvent être souscrits. Incarné selon les cas par une personne physique ou par une machine, l'Oracle procède à des recherches et collecte les données dont les contrats auxquels il est rattaché ont besoin pour s'exécuter[2302]. En fonction des modalités d'exécution du contrat, l'Oracle intervient directement dans la *blockchain* pour saisir

---

[2295] LEGEAIS (Dominique), « Blockchain », *JCl. Sociétés Traité*, fasc. 2160, n° 54.
[2296] *Id.*
[2297] RODRIGUEZ (Philippe), *La révolution blockchain : Algorithmes ou institutions, à qui donnerez-vous votre confiance ?*, éd. Dunod, 2017, p. 143.
[2298] *JavaScript*, ou JS, est un langage de programmation dynamique complet qui permet d'intégrer une interactivité dynamique sur les sites web. Il s'agit, par exemple, des animations web, des jeux 2D ou 3D, ou encore de la fonction permettant de remplir les champs d'un formulaire à remplir en ligne en « un clic ». – Sur les particularismes de l'algorithme d'*Ethereum* par rapport à *Bitcoin*, *supra* n° 68.
[2299] D'abord proposé en août 2014 par Gavin Wood puis développé par l'équipe *Solidity* du projet *Ethereum* dirigé par Christian Reitwiessner. L'équipe était notamment composée de Gavin Wood, Christian Reitweissner, Alex Beregszaszi, Yoichi Hirai et bien encore d'autres collaborateurs d'*Ethereum*.
[2300] Vitalik Buterin précise à ce sujet que « le code EVM permet d'effectuer des boucles de deux manières. Premièrement, l'instruction *JUMP* permet au programme de revenir à un point précédent dans le code, tandis que l'instruction *JUMPI* permet d'effectuer un saut conditionnel, permettant des déclarations comme w*hile x < 27 : x = x * 2.* Deuxièmement, les contrats peuvent appeler d'autres contrats, permettant potentiellement une boucle à travers la récursivité. » [Trad. : Asseth, préc.], BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », préc.
[2301] Sur le sujet, v., KAROCYT, « Introduction aux Smart Contracts », *GitHub* [en ligne], 1er juin 2017, solidity-fr > docs > introduction-to-smart-contracts.rst, github.com ; PHUC (Morgan), « Caractéristiques de Solidity », *Bit Conseil* [en ligne], 22 août 2019, https://bitconseil.fr/solidity-langage-ethereum/.
[2302] GUILHAUDIS (Élise), art. cit., p. 5.

informatiquement la donnée demandée[2303], recueillie auprès d'une source préalablement fixée par les parties[2304], et l'intégrer à la programmation du *smart contract*[2305].

Les Oracles sont ainsi la matérialisation du service de confiance qui « adapte instantanément le *smart contract* à l'évolution des circonstances extérieures à la *blockchain* »[2306].

337. Des yeux protéiformes : un services de confiance à plusieurs visages. Il existe plusieurs formes d'Oracles. Alors que certains sont gérés par une ou plusieurs personnes physiques, d'autres consistent en des logiciels reliés à un serveur ou à une base de données[2307]. La mission de ces derniers est alors de rechercher la donnée requise directement sur Internet[2308]. Il peut s'agir de vérifier des informations météorologiques dans le cadre d'instructions telles que « Pleuvait-il le… dans la ville de… ? », des informations financières afin de déterminer « Quel est le taux de change EUR/ETH actuel ? », des informations de compagnies de transport pour permettre à un *smart contract* de savoir « À quelle heure l'avion… a décollé/atterri ? », ou encore des informations publiques d'ordre général telles que les résultats d'évènement sportifs, politiques[2309], … à condition toutefois que ladite donnée puisse être disponible en ligne.

338. L'exemple d'*Oraclize* : miser sur l'intégrité du processus. C'est sur ce concept que le service « *Oraclize* » a été développé[2310], ainsi que d'autres services d'Oracles similaires[2311]. Son fonctionnement est légèrement différent de celui que retient la communauté *Ethereum* dans sa définition de l'Oracle. En effet, *Oraclize* se fonde sur un nouvel algorithme d'audit et de preuve cryptographique, « *TLSNotary/pagesigner* »[2312], qui lui permet d'aller un cran plus loin et de certifier son travail. Cette fonction lui permet,

---

[2303] *Id.*

[2304] POLROT (Simon), « Les Oracles, lien entre la blockchain et le monde », art. cit. : « Par exemple, l'Oracle a entré à minuit, le 8 juillet 2016 à l'adresse 0x3615087316813abba… que la France a gagné 2-0 contre l'Allemagne à l'Euro. Lors de son exécution le 9 juillet, le *smart-contract* de pari qui fait appel à cette information en déduit que le parieur A a perdu car il avait envoyé une transaction pariant sur l'Allemagne, alors que B, qui avait envoyé une transaction pariant sur la France, a gagné et doit récupérer ses gains, qui lui sont automatiquement envoyés. »

[2305] GODEFROY (Lêmy), « La gouvernementalité des blockchains publiques », *D. IP/IT* 2019, n° 9, p. 497.

[2306] *Id.*

[2307] LEGEAIS (Dominique), *op. cit., loc. cit*.

[2308] RABESANDRATANA (Vanessa), BACCA (Nicolas), « L'Oracle hardware : la couche de confiance entre les blockchains et le monde physique », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 91.

[2309] POLROT (Simon), « Les Oracles, lien entre la blockchain et le monde », art. cit.

[2310] V. le site officiel, http://www.oraclize.it/.

[2311] POLROT (Simon), « Les Oracles, lien entre la blockchain et le monde », art. cit.

[2312] Pour plus d'informations sur le sujet, v. notamment, https://tlsnotary.org/ ; TLSnotary's White Paper, « TLSnotary - a mechanism for independently audited https sessions », TLSnotary [online], 10 Sept. 2014, https://tlsnotary.org/TLSNotary.pdf.

d'une part, de prouver que les informations inscrites au sein de la chaîne à un instant *t* correspondent à celles qui ont été effectivement fournies par le serveur de l'Oracle[2313] et, d'autre part, de distribuer cette preuve sur le web permanent, ce qui la rend disponible en permanence, y compris dans les cas où le système d'*Oraclize* serait momentanément inaccessible. Cette double performance a conduit les développeurs d'*Oraclize* à assurer que leur système est « *provably-honest* », ce qui pourrait être traduit par « certifié honnête ». Bientôt, les temps d'arrêts du système et l'intégrité des données collectées par les Oracles ne seront plus problématiques car ces derniers sont capables à la fois d'anticiper pour éviter toute latence préjudiciable aux parties, et d'empêcher qu'une donnée provenant de la source de données sélectionnée par les cocontractants puisse être modifiée avant son inscription sur la chaîne[2314]. Tel que le souligne finalement Simon Polrot, « ici, c'est la nécessité pour l'Oracle de conserver sa réputation à long terme qui garantit la fiabilité de ses prédictions »[2315].

339. L'exemple des assurances indicielles : la vérité paramétrée. Le concept des systèmes d'Oracles assistant l'exécution de *smart contracts* a également été adopté par des sociétés soucieuses de démontrer la fiabilité des services qu'elles proposent. C'est ainsi que la compagnie d'assurances Axa, après s'être intéressée à automatiser l'indemnisation en cas de retard d'avion *via Fizzy*[2316], s'est attachée à rendre plus intègre ses polices d'assurances vis-à-vis des professionnels des secteurs de l'agriculture, de l'agro-alimentaire, du tourisme et de la construction et du bâtiment.

Par le biais d'un système d'assurance indicielle, Axa propose désormais une couverture assurantielle capable de dédommager automatiquement et instantanément les assurés à hauteur des garanties souscrites. Les *smart contracts* conclus sur *Ethereum* fixent, par exemple, la couverture de l'assuré en cas de précipitations et, dès lors que celles-ci dépassent un certain palier prédéfini et vérifié par le biais d'un Oracle connecté aux bases de données de sites de services d'information météorologique officiels déterminés, l'indemnisation est directement versée au professionnel assuré[2317]. Le système est ainsi capable de contrôler des niveaux de précipitations ou de sécheresse, des

[2313] BERTANI (Thomas), « Understanding oracles », *Oraclize* [online], 18 Feb. 2016, https://blog.oraclize.it/understanding-oracles-99055c9c9f7b.
[2314] *Id.* – Pour un aperçu de l'application d'*Oraclize*, v., http://app.oraclize.it/service/monitor.
[2315] POLROT (Simon), « Les Oracles, lien entre la blockchain et le monde », art. cit.
[2316] BARBRY (Éric), « Smart contracts... Aspects juridiques ! », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 80. – Sur les assurances paramétriques utilisées pour optimiser l'exécution de contrats, *supra* n° 54.
[2317] THEVENIN (Laurent), « Météo : AXA se développe dans l'assurance indicielle », *Les Echos* [en ligne], 11 fév. 2015, https://www.lesechos.fr/11/02/2015/lesechos.fr/0204152662844_meteo---axa-se-developpe-dans-l-assurance-indicielle.htm.

intervalles de températures ou, d'une manière générale, tout évènement météorologique pouvant avoir un impact sur l'organisation de certains secteurs, et de couvrir les professionnels contre leur caractère aléatoire[2318].

340. L'exemple de *Augur* et *Gnosis* : l'existence d'une vérité décentralisée ? Les deux solutions précitées, parfaitement envisageables, peuvent se révéler cependant particulièrement difficiles à mettre en œuvre en raison de l'exigence de décentralisation de la *blockchain* et la difficulté de trouver un processus d'incitation suffisamment efficace pour attirer des mineurs. C'est pour remédier à cet inconvénient que, dans certains domaines limités toutefois, sont utilisés les marchés de prédiction tel *Augur* ou *Gnosis*. Or, par abus de langage ou par extrême élargissement de la notion, ces systèmes sont souvent assimilés à des Oracles[2319].

Fondé sur un système de consensus et sur la croyance en une forme de « sagesse collective », le marché prédictif laisse aux utilisateurs la possibilité de parier sur des évènements quelconques, et à partir des résultats de ces paris, le système déduit des tendances acceptées comme vérités[2320]. Un mécanisme de réputation et de « sanction » des mauvais parieurs, c'est-à-dire des utilisateurs dont le pari n'aurait pas respecté la vérité collective, est mis en place au sein du système afin d'inciter les participants à fournir la réponse correcte[2321].

Déjà utilisé par quelques *dApps* d'*Ethereum* et en phase de test sur d'autres[2322], ce système d'Oracle, proposant un service à la fois décentralisé et distribué, nécessitera néanmoins quelques développements supplémentaires avant d'être généralisé[2323].

[2318] Axa, « Assurance high-tech contre anomalies météorologiques », *Le Monde* [en ligne], 28 oct. 2015, https://www.lemonde.fr/ensemble-pour-l-environnement/article/2015/10/28/assurance-high-tech-contre-anomalies-meteorologiques_4798354_4797213.html.

[2319] BERTANI (Thomas), préc.

[2320] RABESANDRATANA (Vanessa), BACCA (Nicolas), art. cit., p. 91.

[2321] POLROT (Simon), « Les Oracles, lien entre la blockchain et le monde », art. cit.

[2322] *Id.* – V. notamment, l'Oracle décentralisé de la *start-up* Chainlink [https://chain.link/ ; NAZAROV (Sergey), « The missing link between blockchains and Enterprises », *World Economic Forum* [online], 15 Dec. 2020, https://www.weforum.org/agenda/2020/12/the-missing-link-between-blockchain-and-existing-systems/], et le projet de la *start-up* Razor Network d'une « Truly Decentralized Oracle Solution » [Ngetich (Dalmas), « Razor Network Raises $3.7 Million in Private Funding to Build "Truly Decentralized" Oracle Solution », *BTC Manager* [online], 4 Nov. 2020, https://btcmanager.com/razor-network-3-7-million-private-funding-decentralized-oracle-solution/#:~:text=Crypto%200%25%20Fee-,Razor%20Network%20Raises%20%243.7%20Million%20in%20Private,Build%20%E2%80%9CTruly%20Decentralized%E2%80%9D%20Oracle%20Solution&text=Decentralized%20Oracle%20platform%20Razor%20Network,seed%20and%20private%20sales%20round].

[2323] RABESANDRATANA (Vanessa), BACCA (Nicolas), art. cit., p. 91.

341. Hormis le cas des marchés prédictifs, il apparaît que le fonctionnement des Oracles soit principalement centralisé[2324]. Or, si la validité des blocs créés sur la base de données collectées par des Oracles dépend de l'existence et de la disponibilité des informations requises par les *smart contracts*, la fiabilité du contenu de ces blocs est tout autant dépendante de l'intégrité du service externe exploité. Tous ces usages sont susceptibles de constituer une nouvelle forme de manipulation ou, du moins, d'altération de la confiance dans la technologie.

B. Entre risques de centralisation et responsabilité(s)

342. En théorie : les conditions de la fiabilité. D'une manière générale, il paraît admissible de considérer que les utilisateurs se fient plus facilement à des ressources du web appartenant à une organisation reconnue comme étant fiable, sinon officielle, et davantage encore s'il s'agit d'un site d'une administration de l'État[2325]. Ainsi, les sites de la Banque de France, de Météo-France, de Légifrance, de l'Insee, ou encore du Tribunal de Commerce de Lille bénéficient pour chacun d'une forme de présomption d'intégrité, équivalente à une présomption simple, certes, mais qui peut permettre à l'Oracle qui l'a exploité d'emporter plus facilement la conviction de ses utilisateurs. La fiabilité est également assurée lorsque le contrat se fonde sur des critères neutres et vérifiables comme le cours des actions en bourse, l'indice de référence des loyers, ou encore des indices légaux fixés par loi de finance annuelle.

Quid cependant d'une demande portant sur la survenance d'un évènement récent, pas encore parfaitement défini, voire controversé, ou simplement subjectif. Tel que le soulignent Vanessa Rabesandratana et Nicolas Bacca, les évènements concrets, presque mécaniques, sont toujours susceptibles d'être contrôlés et confrontés *via* différentes sources de confiance, mais rien n'est moins sûr pour des évènements qui peuvent susciter des discussions, soulever des opinions divergentes et donc des vérités différentes[2326]. Ce constat mène à interroger l'importance du choix de la source exploitée par l'Oracle dans sa recherche de fiabilité.

343. En pratique : la question du choix de la source d'informations provenant du monde réel. Si l'information requise ne figure pas dans les données d'un site web appartenant à une organisation officielle, sinon à une organisation reconnue comme étant

[2324] GUILHAUDIS (Élise), art. cit., p. 5.
[2325] POLROT (Simon), « Les Oracles, lien entre la blockchain et le monde », art. cit.
[2326] *Id.*

fiable, la question se pose de savoir *comment* celle-ci pourra être recherchée. Des auteurs soulignent la complexité d'un tel choix, notamment lorsqu'il s'agit d'évaluer l'intégrité d'une source telle que le site de l'encyclopédie collective et universelle en ligne *Wikipedia*, connu pour ses divergences de versions[2327] et le manque de fiabilité de certains de ses contenus[2328], mais également de *Facebook*, *Le Monde*, *Twitter*, *Bitcoin.com*, *Mondial Relay*, etc. qui pourraient être utilement mobilisés mais dont la pertinence n'est pas garantie. Au-delà de la question du comment, il convient de déterminer les acteurs auxquels reviendrait éventuellement ce choix, lesquels disposeraient dès lors d'un pouvoir d'attester du taux de fiabilité d'un site web quelconque[2329].

L'Oracle pourrait ainsi choisir, en fonction de son algorithme, les sources qu'il considère fiables. D'après Simon Polrot, « *in fine*, le recours à un Oracle revient à introduire un tiers de confiance, au pouvoir aussi exorbitant que son équivalent mythologique : il décide seul de l'issue des *smart contracts*, qui sont par principe impossibles à arrêter… »[2330]. Mais si l'Oracle n'effectue pas de choix, l'aléa en résultant pourrait tout autant mettre en péril la stabilité et la réputation du système Oracle-*blockchain*. D'autant qu' « à l'inverse de son homologue de Delphes, il peut faillir »[2331].

344. Réagir face aux hypothèses de dysfonctionnement ou d'erreur : questions de responsabilité. En effet, puisque la centralisation réapparaît, accompagnée de l'ensemble de ses inconvénients, d'une manière plus ou moins claire à travers la notion d'Oracle[2332], il n'est pas déraisonnable de considérer que l'Oracle ne constitue pas un système qualifiable d'infaillible. Une auteure imagine ainsi le cas d'un dysfonctionnement au cours duquel un Oracle n'a pas transmis la donnée requise à la *blockchain*, à l'instar de l'utilisateur qui passe un contrat avec un auteur pour utiliser une de ses œuvres musicales dans le cadre de son activité professionnelle, qui s'est acquitté de la redevance déterminée au contrat, mais dont la cession de droit n'a pas été inscrite par l'Oracle[2333]. Il pourrait s'agir également d'un agriculteur qui n'a pas obtenu l'indemnisation prévue par son contrat en raison d'une absence de notification de la *blockchain* utilisée, ou encore un

[2327] Par exemple, il existe, entre les versions anglaise et française, des divergences concernant la définition de la *blockchain* elle-même. V. en ce sens, DELAHAYE (Jean-Paul), *Mathématiques et mystères*, éd. Belin, coll. Pour la science, 2016, p. 45.
[2328] RABESANDRATANA (Vanessa), BACCA (Nicolas), art. cit., p. 91.
[2329] LEE (David), CHUEN (Kuo), DENG (Robert H.), *Handbook of Blockchain, Digital Finance, and Inclusion: vol. 2:ChinaTech, Mobile Security, and Distributed Ledger*, ed. Academic Press, 2017, *op. cit.*, p. 157.
[2330] POLROT (Simon), « Les Oracles, lien entre la blockchain et le monde », art. cit.
[2331] *Id.*
[2332] GUILHAUDIS (Élise), art. cit., p. 5.
[2333] *Id.*

vendeur qui n'a pas reçu le prix automatiquement versé à la livraison du produit expédié pour la même raison. Hormis le cas où les parties ont anticipé le risque d'anomalies de fonctionnement du système[2334], le *smart contract* conclu ne pourrait dès lors pas s'exécuter et les sommes versées ne seraient pas retournées. En parallèle, existe la possibilité d'une erreur[2335] qui, volontaire ou involontaire, peut mener à ce qu'une donnée inexacte soit inscrite par l'Oracle dans la *blockchain*. Le danger consiste dans l'altération de la confiance dans la technologie. En cas de dysfonctionnement ou d'erreur, l'Oracle engagerait en principe sa responsabilité s'il s'agit d'un Oracle-personne physique, ou la responsabilité de son développeur dans l'hypothèse d'un logiciel relié à un serveur ou à une base de données[2336]. Toutefois, encore faut-il pouvoir déterminer si le dysfonctionnement provient de l'Oracle ou de la source exploitée. De la même manière, faut-il pouvoir établir l'origine de l'erreur, à savoir si elle résulte d'une erreur dans les données publiées par le site visité par l'Oracle, et/ou du choix du site source, ou si elle implique un défaut dans la recherche ou dans l'inscription effectuée sur la chaîne. Tous les Oracles ne sont pas aussi intransigeants dans leur fonctionnement qu'*Oraclize*[2337], le contexte d'une erreur ou d'un dysfonctionnement posera donc souvent un problème de preuve et, *a fortiori*, de sécurité juridique. De plus, la question se pose de la sécurité technique du système dans le cas où un individu, ou d'ailleurs le cocontractant, aurait un intérêt à transmettre une donnée erronée au *smart contract*[2338], si bien que l'intégrité de la technologie dépend de la sécurité du web dans sa globalité, et en particulier de la fiabilité de chaque source potentielle d'informations utilisables au sein d'un *smart contract*.

La mise en œuvre de ces systèmes n'est pas sans soulever de nombreuses difficultés. Celles-ci mènent d'ailleurs à se demander si une telle configuration pourrait conduire les développeurs d'une *blockchain* à essayer d'organiser leur irresponsabilité juridique en cas de *bug* informatique[2339]. Certains auteurs proposent ainsi de créer un « régime légal alourdissant [la] responsabilité [de l'Oracle] », lequel lui imposerait la souscription d'une assurance spéciale afin de pouvoir réparer un quelconque dysfonctionnement auprès des utilisateurs[2340].

[2334] Sur la notion d'anticipation contractuelle, *supra* n°s 225 et s.
[2335] GUILHAUDIS (Élise), art. cit., p. 5.
[2336] LEGEAIS (Dominique), *op. cit.*, *loc. cit*.
[2337] L'algorithme d'*Oraclize* est notamment garanti « *provably-honest* », *supra* n° 338.
[2338] POLROT (Simon), « Les Oracles, lien entre la blockchain et le monde », art. cit.
[2339] Sur les questions de responsabilité(s) décentralisée(s) en cas de dysfonctionnement de la technologie, *supra* n°s 258 et s.
[2340] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., n° 29.

345. Réagir face aux hypothèses de dysfonctionnement ou d'erreur : la solution de l'anticipation ? En dehors des questions de responsabilité, certains auteurs s'interrogent quant à la possibilité de recourir aux services d'un autre Oracle si un dysfonctionnement est détecté au cours de l'exécution du *smart contract,* ou éventuellement si l'information transmise par le premier ne satisfait pas l'une ou les deux parties[2341]. En principe, les parties au *smart contract* sont libres de déterminer les conditions de son exécution. Cependant, cette fonctionnalité suppose que l'information inscrite dans la *blockchain* par le premier Oracle soit modifiable et suggère que les circonstances ouvrant droit à cette seconde option soient prédéfinies afin que l'algorithme puisse les vérifier et s'adresser à l'autre Oracle le cas échéant. Cette solution, parfaitement envisageable, se révèle néanmoins particulièrement inopportune en raison des nombreux prérequis en termes d'anticipation, mais aussi et surtout de l'inutile complication de l'utilisation d'une technologie qui se voulait pourtant simplificatrice. En effet, en cas de désaccord entre les cocontractants concernant les données indiquées par les différents Oracles, leur faudra-t-il se tourner vers un mécanisme de résolution des conflits ?

346. Force est de constater que, dans ce contexte, la mise en œuvre d'un Oracle posera souvent un problème de confiance. D'une manière générale, le bilan est donc mitigé. L'utilisation des Oracles laisse apparaître de nouvelles problématiques juridiques. Bien que nous nous montrions encore prudents à leur égard, il est clair que l'évolution se fera dans le sens d'une dématérialisation accrue des relations contractuelles, si bien qu'il est important de prendre rapidement la mesure de leurs développements afin d'intégrer, dès leur conception, les mécanismes de sécurité à la fois technique et juridiques suffisants pour assurer et rassurer les utilisateurs. Ces dispositifs sont d'autant plus essentiels que les systèmes des Oracles prétendent opérer un déplacement de la confiance initialement déposée dans la technologie *blockchain*[2342] vers une nouvelle forme de tiers de confiance[2343]… dont il convient d'en déterminer les contours.

§ 2. Vers un déplacement de la confiance initiale

347. Il n'est plus tant question de savoir s'il est fait confiance en la technologie *blockchain* mais bien davantage s'il est fait confiance en trois éléments, à savoir, la

[2341] V. notamment, POLROT (Simon), « Les Oracles, lien entre la blockchain et le monde », art. cit.
[2342] GOSSA (Julien), « Les blockchains et smart contracts pour les juristes », *D. IP/IT* 2018, n° 7-8, p. 393.
[2343] *Id.* ; GUILHAUDIS (Élise), art. cit., p. 5 ; MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., *loc. cit.*

blockchain, le système d'Oracle utilisé, et la source centralisée auprès de laquelle ce dernier a pour instruction de se fournir en données[2344]. La détermination des contours de ce déplacement de la confiance est d'autant plus importante qu'à travers ce processus l'Homme devient à nouveau capable de manipuler la chaîne en contradiction avec la philosophie indépendante qu'elle a adoptée. Pourtant, s'arrêter à l'état de l'art et ne pas évoquer les possibilités futures de développement des Oracles conduirait à ne donner qu'une vision incomplète de la situation. S'il résulte actuellement de l'utilisation des Oracles une croissante ré-intermédiation et l'émergence de nouveaux tiers de confiance (A), il est cependant fort probable qu'à l'avenir, l'humain soit entièrement détaché de cette fonction grâce à l'intervention de l'univers des dispositifs électroniques dotés de capacités de perception de l'environnement et de communication et de l'IoT, éventuellement augmenté d'autres propriétés que proposent les nouvelles technologies telles que l'IA. En édifiant une passerelle entre les deux mondes, physique et virtuel, l'Oracle physique (B) pourrait ainsi permettre à la *blockchain* d'atteindre une forme d'autonomie fonctionnelle, si ce n'est définitivement remplacer ce besoin de confiance traditionnel entre les Hommes.

A. Entre ré-intermédiation et émergence de nouveaux tiers de confiance

348. La confiance des parties dans l'Oracle, condition de la confiance dans la technologie *blockchain*. Confrontée à ses propres limites[2345], la technologie *blockchain* a dû s'ouvrir au monde qui l'entourait afin d'acquérir un certain nombre d'informations que son fonctionnement exige. Actuellement incapable d'y procéder seule, son protocole a donc été associé à un système apte à solliciter des données externes[2346]. L'Oracle consiste donc en cette entité, humaine ou informatique, reliée à une ou plusieurs ressources du web, serveur et/ou base de données, qui créée un pont entre la *blockchain* et les informations du monde réel qu'elle requière pour s'exécuter. Cependant, son rôle le conduit à exercer une influence considérable sur le contrat et les parties, un « pouvoir aussi exorbitant que son équivalent mythologique » selon les dires de Simon Polrot[2347]. En effet, l'avenir du contrat, de son exécution à sa fin normale, dépendent finalement de la propre exécution de l'Oracle, et *a fortiori* de ses recherches et de l'intégrité des données

[2344] GOSSA (Julien), art. cit., *loc. cit.*
[2345] *Id.*
[2346] BUTERIN (Vitalik), « Ethereum and Oracles », *Ethereum Blog* [online], 22 Jul. 2014, https://blog.ethereum.org/2014/07/22/ethereum-and-oracles/.
[2347] POLROT (Simon), « Les Oracles, lien entre la blockchain et le monde », art. cit.

qu'il sélectionne. Or son rôle est d'autant plus important que le droit exige que les volontés des parties à un contrat soient respectées et ne peuvent souffrir aucune modification qu'elles n'auraient pas elles-mêmes décidées[2348]. Lorsqu'il a souscrit à un *smart contract*, le créancier a placé sa confiance non pas dans l'espoir que son débiteur s'exécute spontanément, conformément aux termes de leur contrat, mais il l'a placée dans la technologie *blockchain* et finalement dans le contrôle effectif de l'Oracle, logiciel ou humain. C'est cette vérification par une entité tierce qui l'a incité à avoir davantage confiance dans les qualités de la *blockchain*. Il en va ainsi de l'agriculteur dont les champs ont été endommagés par un orage de grêles qui se fie à la technologie *blockchain* et au caractère automatique du *smart contract* qu'il a conclu avec son assurance pour obtenir l'indemnisation qui lui est due. Or, pour cela, il a notamment confiance en l'Oracle puisque c'est finalement à lui de certifier auprès de la *blockchain* l'information qui aura pour conséquence de déclencher, ou non, son droit à obtenir une indemnisation pour le dommage qu'il a subi. De la même manière, si un contrat de distribution a été conclu sur la *blockchain* et que le prix des produits vendus a été fixé en fonction d'un indicateur économique tel qu'une clause d'indexation, les contractants se réfèreront à la fiabilité de l'Oracle pour fixer le prix exactement dû par chacun. Il apparaît donc que la confiance dans la technologie soit en effet dépendante de la confiance des parties dans l'Oracle.

C'est la raison pour laquelle se pose à nouveau les questions de fiabilité des données utilisées.

349. La double question du choix de la source d'informations provenant du monde réel et de la responsabilité : éléments de réponse. La fiabilité de ces données dépend de l'autorité de laquelle elles émanent autant que celle qui juge de cette intégrité, autrement dit l'Oracle. Certains auteurs, comme Julien Gossa, proposent de confier ce rôle de certificateur à des tiers disposant de compétences reconnues dans le domaine visé[2349]. Selon lui, dans le contexte d'une vente de photographies sur la *blockchain*, une agence de photographie spécialisée serait plus à même d'assurer les fonctions de vendeur[2350]. Elle endosserait alors les diverses responsabilités techniques et juridiques vis-à-vis du fournisseur de l'acheteur, tel un tiers de confiance. D'après d'autres auteurs, le rôle de l'Oracle devrait être tenu par des professionnels du droit[2351], à l'instar des

[2348] *Id.*
[2349] MEKKI (Mustapha), DORAL (Sylvian), STREIFF (Vivien), BOYER (Sacha), *in* « Dossier : Blockchain et métiers du droit : une force vive ou subversive ? », *D. IP/IT* 2020, n° 2, p. 86 ; GOSSA (Julien), art. cit., p. 393.
[2350] GOSSA (Julien), art. cit., *loc. cit.*
[2351] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., *loc. cit.*

notaires, des huissiers de justice ou des avocats, lesquels sont traditionnellement assujettis à des règles déontologiques ou d'éthique très strictes[2352], et pourraient dès lors assumer la responsabilité et exercer l'autorité qui y sont attachées. D'une manière générale, l'Oracle doit être « impartial et objectif »[2353]. À notre sens, il semble acceptable de faire intervenir des Oracles n'assurant pas forcément des fonctions juridiques ou spécialisées, appartenant éventuellement à la communauté d'une *blockchain*, à la condition que leur intégrité puisse être assurée en appliquant la solution au problème de mathématiques des généraux byzantins[2354]. En effet, à l'instar des *consensus based oracle* tels que *Augur*, la distribution du pouvoir de décision suggèrerait que l'information requise soit recherchée par plusieurs Oracles, que leurs réponses soient confrontées les unes aux autres, et que celle qui fait consensus soit accueillie comme reflétant la vérité qui sera ensuite intégrée à la *blockchain*.

En définitive, de ces Oracles semblent émerger des tiers de confiance « d'un genre nouveau »[2355], ou presque, puisque la plupart réuniraient les intermédiaires actuels, mais intervenant effectivement d'une toute autre manière[2356]. Une ré-intermédiation pourrait ainsi être engagée puisque, « finalement, l'on se rend compte que le rôle du tiers de confiance numérique existe »[2357] et permet de résoudre les quelques insécurités, en particulier juridiques, demeurant au sein de la chaîne[2358]. Bien que selon certains auteurs, cela signifie que « l'on aura toujours besoin d'un gardien de la véracité des données entrées dans le *smart contract* »[2359] et que ce gardien ne peut être qu'un humain[2360], ou du moins qu'un juriste, même intervenant indirectement dans ce processus pour être ce « gardien » des droits des utilisateurs[2361], la forme que peut effectivement prendre cette entité tierce prête à discussion.

[2352] MEKKI (Mustapha), DORAL (Sylvian), STREIFF (Vivien), BOYER (Sacha), *in* « Dossier : Blockchain et métiers du droit : une force vive ou subversive ? », art. cit.

[2353] MEKKI (Mustapha), « Le smart contract, objet du droit (Partie 2) », *D. IP/IT* 2019, n° 1, p. 27.

[2354] Pour une définition du problème de mathématiques des généraux byzantins, *supra* n° 98.

[2355] GUILHAUDIS (Élise), art. cit., p. 14.

[2356] COLLOMB (Alexis), SOK (Clara), LEGER (Lucas), « Technologie des registres distribués : quel impact sur les infrastructures financières ? », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 28 : « Il paraît naïf de penser que le développement de la technologie des registres distribues risque de faire disparaitre les intermédiaires financiers. Si l'on regarde le cas de la première des *blockchains*, celle du *bitcoin*, on constate que l'écosystème a favorise l'éclosion de nouveaux intermédiaires. »

[2357] MARRAUD DES GROTTES (Gaëlle), « Risques et opportunités de la blockchain pour les avocats », *Wolters Kluwer* [en ligne], 14 mai 2018, https://www.actualitesdudroit.fr/browse/techdroit/blockchain/12997/risques-et-opportunites-de-la-blockchain-pour-les-avocats.

[2358] GUILHAUDIS (Élise), art. cit., p. 14.

[2359] MARRAUD DES GROTTES (Gaëlle), « Risques et opportunités de la blockchain pour les avocats », art. cit.

[2360] ConsenSys, « A Visit to the Oracle », *Media ConsenSys* [online], 1st Jun. 2016, https://media.consensys.net/a-visit-to-the-oracle-de9097d38b2f.

[2361] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., *loc. cit.*

350. L'intervention humaine au sein de la *blockchain* absolument nécessaire ? Il existe des hypothèses où certaines informations ne peuvent pas être obtenues à partir de données purement publiques, ni même de faits observables par une communauté[2362]. Il en va ainsi, par exemple, de la remise d'un colis, du verrouillage effectif d'une porte, de la vitesse d'un véhicule, de la fin d'un contrat résultant de l'exécution normale du service commandé, tel que l'aboutissement d'un projet, la réception d'un ouvrage, ou la fin de la location d'un bien quelconque.

En principe, tout contractant devrait pouvoir se fier au système de l'Oracle, qu'il soit logiciel ou humain. Par exemple, dans le cadre d'une vente, d'une part, le créancier devrait avoir confiance en l'Oracle qui le prévient dès que sa commande est expédiée, ce qui déclenchera automatiquement son paiement le cas échéant et, d'autre part, le débiteur devrait avoir confiance dans le système de l'Oracle qui attesterait de la bonne ou mauvaise réception de la commande par le créancier. Cependant, dans des cas comme ceux évoqués, l'exigence de recherches approfondies, et même individualisées, suggérerait que l'Oracle doive en pratique se démultiplier afin de remplir sa mission. Ainsi, lors d'une vente, l'Oracle serait à la fois l'entité ayant expédié le produit, celle qui l'a réceptionné, et enfin celle qui l'a livré. Or, plus les sources se multiplient, plus la fiabilité du système diminue et plus la confiance est nécessaire.

Par ailleurs, quelle utilité de compliquer ainsi le processus si ce type de services procède actuellement de la même manière sans *smart contract* ni Oracle.

351. Évolution des besoins et nécessaire évolution des pratiques : l'exigence d'un Oracle plus proche de la réalité individuelle. Les contractants ont besoin de plus de concret[2363], d'un système qui puisse aller plus loin dans la vérification, qui puisse contrôler des évènements qui tiennent, selon les situations, à la personne du contactant ou à l'état d'une chose et ce, en temps réel[2364] et sans multiplier les intermédiaires de confiance. Nombre de *smart contracts* ont pour objet la réalisation de ventes de biens ou de services. Il est difficile pour un Oracle logiciel de collecter instantanément et, de plus, sur le web, des informations relatives à l'occupation d'une location saisonnière ou à l'état d'avancement d'un chantier. Dès lors que l'information est de l'ordre du privé, la transaction ne serait plus observée par l'Oracle. D'ailleurs, un logiciel ou même un

[2362] RABESANDRATANA (Vanessa), BACCA (Nicolas), art. cit., p. 91.
[2363] GOSSA (Julien), art. cit., p. 393.
[2364] GUILHAUDIS (Élise), art. cit., p. 14.

humain, ne peut, à distance, déterminer qui de l'expéditeur, du fournisseur, du transporteur, ou du destinataire n'a pas respecté ses engagements[2365].

Ce constat conduit certains auteurs à considérer l'Oracle comme étant l'actuel « talon d'Achile du *smart contract* »[2366]. Pourtant, force est de constater que si cet obstacle d' « orthogonalité »[2367] ne peut être résolu par l'Homme, du moins seul, il le pourra grâce à l'alliance entre la technologie *blockchain* et les objets du quotidien.

B. L'Oracle physique, passerelle entre les deux mondes

352. Définition et critères du concept d'Oracle physique. Pour permettre à un *smart contract* d'interagir de manière efficace et sécurisée avec le monde physique, il s'agirait de donner le rôle d'Oracle à un objet. Pour cela, le dispositif en question devrait non seulement disposer d'attributs fonctionnels lui permettant de capter des données, mais également être doté d'une capacité de communication.

Il est donc essentiel qu'ils disposent de capteurs[2368], c'est-à-dire « des organes sensoriels [leur] permettant de percevoir [leur] environnement »[2369], soit l'équivalent en robotique d'attributs consistant à « construire une représentation du monde physique à partir de données perçues »[2370] ou encore à « détecter et [à] enregistrer des signaux physiques »[2371] en fonction des informations nécessaires[2372]. La CNIL indique en effet que ces capteurs peuvent être d'origines variées et reliés entre eux afin de permettre à un dispositif ou équipement électronique de prélever et de rassembler en continu un ensemble de données physiques, provenant de son environnement proche[2373], à l'image de ce que sont les organes des sens chez l'homme. Un capteur peut, par exemple, mesurer

---

[2365] GOSSA (Julien), art. cit., *loc. cit.*
[2366] MEKKI (Mustapha), « Les mystères de la blockchain », art. cit., *loc. cit.*
[2367] RABESANDRATANA (Vanessa), BACCA (Nicolas), art. cit., p. 91 : « ces deux univers existent sur des plans qui ne se superposent jamais ».
[2368] Pour une définition plus détaillée des capteurs et des dispositifs électroniques dotés de capacités de perception de l'environnement, *supra* n° 64.
[2369] NEVEJANS (Nathalie), « Une introduction juridique à l'Objet Intelligent », communication au colloque « L'objet intelligent : normes, usages et responsabilités » de l'Institut d'électronique et des Systèmes (Université de Montpellier R 5214) et l'Unité Dynamiques du droit (Université de Montpellier R 5815) – Centre National de la Recherche Scientifique, Montpellier, Université de Montpellier, non publié, 6 nov. 2015.
[2370] « Le développement industriel futur de la robotique personnelle et de service en France », Ministère de l'économie [en ligne], p. 12, https://www.entreprises.gouv.fr/files/files/en-pratique/etudes-et-statistiques/dossiers-de-la-DGE/robotique.pdf.
[2371] « Éthique de la recherche en robotique. Rapport n° 1 de la CERNA, Commission de réflexion sur l'Éthique de la Recherche en sciences et technologies du Numérique d'Allistene », *CERNA* [en ligne], nov. 2014, p. 12, http://cerna-ethics-allistene.org/digitalAssets/38/38704_Avis_robotique_livret.pdf.
[2372] NEVEJANS (Nathalie), *Traité de droit et d'éthique de la robotique civile*, éd. LEH éditions, coll. Science, éthique et société, 2017, p. 120.
[2373] CNIL, *Rapport d'activité de 2015*, éd. La Documentation Française [en ligne], 2016, p. 84, https://www.cnil.fr/sites/default/files/atoms/files/cnil-36e_rapport_annuel_2015_0.pdf.

la température, la luminosité, la distance, les vibrations, le bruit, le son, ou encore la pollution[2374]. Nathalie Nevejans précise qu'en robotique il s'agit pour la machine « d'acquérir et d'interpréter les données sur son environnement ou sur elle-même » *via* des capteurs qui les transforment ensuite « en une information, le plus souvent un signal électrique, qui est alors utilisable »[2375]. Cette information peut effectivement être utilisée, mais pour qu'elle le soit par un *smart contract*, il faudra qu'elle puisse lui être communiquée. Pour cela, le dispositif électronique doit donc être doté de capacité de communication des données captées[2376].

En incluant dans l'exécution de la relation contractuelle des dispositifs électroniques, Oracles physiques, à la fois communicants et dotés de capacités de perception de leur environnement, le *smart contract* peut disposer d'informations supplémentaires sur son état d'exécution, en particulier d'informations concernant des faits matériels privés qui ne peuvent pas apparaître autrement qu'à travers l'objet et/ou la personne ciblée[2377].

353. Le rôle des capteurs : l'exemple dans le secteur de la gestion logistique. L'utilisation de ces capteurs devrait démultiplier les usages de la technologie *blockchain*, mais également ceux des *smart contracts*. Elle trouve une application particulière en matière de logistique, permettant par exemple d'assurer à l'entreprise cliente l'envoi de sa commande et de garantir en retour le fournisseur de la bonne réception de sa livraison par l'entreprise cliente. C'est sur ce concept qu'a été testé une application permettant de tracer, sans intervention humaine, l'affrètement de dix-sept tonnes d'amandes, de leur départ des vergers d'*Olam Ochards Australia* à Mildura dans l'État du Victoria en Australie, jusqu'à leur réception à Hambourg en Allemagne, en passant par les lignes ferroviaires et le port de Melbourne[2378]. De plus, pendant l'intégralité du voyage, le taux d'humidité et la température de la cargaison ont pu être surveillés et automatiquement régulés par le biais de capteurs connectés placés dans les containers d'amandes et directement reliés à la chaîne *Ethereum*[2379]. D'après Gerhard Ziems, directeur financier du transport ferroviaire *Pacific National* intervenu dans l'expérience, « ce projet est

[2374] BOUJAT (Gérard), ANAYA (Patrick), *Automatique industrielle en 20 fiches*, éd. Dunod, 2013, pp. 40-49.
[2375] NEVEJANS (Nathalie), *Traité de droit et d'éthique de la robotique civile*, *op. cit.*, pp. 119-120.
[2376] Pour une définition plus détaillée des capacités de communication et des dispositifs électroniques dotés de capacités de communication, *supra* n° 65.
[2377] RABESANDRATANA (Vanessa), BACCA (Nicolas), art. cit., p. 91.
[2378] « L'ABC aide à expédier des tonnes d'amandes 17 sur la blockchain », *Coin News Telegraph* [en ligne], 30 juill. 2018, https://fr.coinnewstelegraph.com/cba-helps-ship-17-tonnes-of-almonds-on-the-blockchain/.
[2379] NOTT (George), « 17 tonnes d'amandes tracées avec blockchain », *Le Monde Informatique* [en ligne], 31 juill. 2018, https://www.lemondeinformatique.fr/actualites/lire-17-tonnes-d-amandes-tracees-avec-blockchain-72462.html.

unique car il cherche à repenser la communication et le partage d'informations dans la gestion logistique. L'accès facilité à ces informations nous permet de mieux utiliser nos actifs et de fournir à nos clients de meilleurs services »[2380].

354. Le rôle des capteurs : l'exemple dans le secteur de l'assurance. Dans le domaine de l'assurance, certains imaginent déjà des *smart contracts* automobiles spécifiques, conclus à la demande ou à l'usage[2381], reliés à des dispositif électroniques de suivi embarqués dans le véhicule jouant le rôle d'Oracle et récompensant l'assuré pour son comportement exemplaire sur les routes[2382]. Les utilisations pourraient ainsi être démultipliées et être destinées, par exemple, à calculer la consommation en carbone d'un véhicule pour récompenser l'assuré émettant de faibles taux[2383]. Pour cela, il est essentiel que le système d'Oracle physique soit à la fois sécurisé et infalsifiable[2384]. Il pourra être constitué de capteurs permettant de collecter des données concernant la vitesse d'une automobile ou la qualité de gaz et de vapeurs qu'elle rejette, et être relié à des dispositifs sécurisés de lecture des données captées, à l'instar des projets de systèmes « *Oracles hardwares* » de la *start-up* Ledger[2385]. L'intégrité de ces dispositifs électroniques est assurée par le biais de deux éléments. D'une part, ils délivrent automatiquement une « *cryptographic attestation of the sensor reading* » (qui peut être traduit par une « attestation cryptographique du capteur ») afin de certifier de l'origine et de l'authenticité des données captées puis transmises. D'autre part, ils sont dotés d'une « *anti-tampering installation of the reader device* » (une « installation anti-falsification du capteur ») qui, en cas de tentative de falsification des données, de manipulation ou de de désactivation des capteurs, par exemple, déconnecte instantanément le ou les capteurs visés et envoie un message d'alerte immuable *via* la *blockchain*[2386].

[2380] Cité dans : *id.*

[2381] LELOUP (Laurent), « Assurance : Blockchain, entre opportunités et défis », *Blockchain Daily News* [en ligne], 28 mars 2014, https://www.eyrolles.com/Entreprise/Livre/blockchain-9782212566659/. – Pour plus d'informations sur le sujet, v. notamment, ADAM-KALFON (Pauline), DUBREUIL (Emmanuel), RICHARD (Marie-Line), « Blockchain, catalyseur de nouvelles approches en assurance », PwC [en ligne], mars 2017, https://www.pwc.fr/fr/assets/files/pdf/2017/03/blockchain-et-assurance/etude-blockchain-catalyseur-de-nouvelles-approches-en-assurance.pdf.

[2382] RABESANDRATANA (Vanessa), BACCA (Nicolas), art. cit., p. 92.

[2383] LARCHEVEQUE (Éric), « Hardware Pythias: bridging the Real World to the Blockchain », *Ledger* [online], 31 Aug. 2016, https://blog.ledger.co/2016/08/31/hardware-pythias-bridging-the-real-world-to-the-blockchain/#.7sxi7v3vw.

[2384] RABESANDRATANA (Vanessa), BACCA (Nicolas), art. cit., p. 92.

[2385] V. le site officiel, https://www.ledger.fr//

[2386] LARCHEVEQUE (Éric), préc. : « *Deployment of these oracles require provisioning of the system (master attestation keys and device identification keys), and establishing a strategy to supervise they correct initial installation (to make sure they are measuring what we want them to measure). Trust on the long term is guaranteed by anti-tampering features and private keys' protection through a Secure Element*. »

355. Une solution à venir. Matérialisant la passerelle entre *blockchain* et monde réel[2387], une fois déployés, ces systèmes pourraient contribuer à fournir à la technologie *blockchain* un moyen de se soustraire définitivement à l'intervention de l'Homme, tout en suscitant la confiance généralisée des utilisateurs[2388]. Pour cela, ils pourront compter sur le soutien de l'IoT, éventuellement augmenté d'autres propriétés que proposent les nouvelles technologies telles que celles de l'IA. En effet, comme le constate Nathalie Nevejans, « si l'objet communicant est, par la force des choses, nécessairement connecté, il ne l'est pas forcément à Internet »[2389]. Néanmoins, lorsqu'il l'est, ses attributs fonctionnels et les diverses informations qu'il capte sont mis au service d'un ensemble plus grand contribuant à créer un réseau d'objets capable de « faire le lien entre logiciel et objets »[2390], et ainsi d'optimiser la relation entre monde virtuel et monde physique. L'IoT désigne la connexion des objets à un réseau plus large, local ou Internet, sans requérir l'intervention de l'utilisateur[2391]. Plus encore, selon un auteur, la combinaison de solutions d'IA et du système des *smart contracts* pourrait étendre les capacités de la *blockchain* et lui permettre d'auditer les conventions de ses utilisateurs, tant en termes de conformité à l'instar des contrôles de *compliance* et RSE, qu'en termes de normativité[2392].

Alors même que les technologies liées à l'IA requièrent, pour être maîtrisées, de rester sous le contrôle de l'Homme[2393], force est de constater qu'en matière de *blockchains*, moins d'humain équivaut à plus de neutralité, et *a fortiori* à un accroissement de sa fiabilité. Avant de permettre à la technologie de franchir en toute autonomie cette frontière entre monde virtuel et monde réel qui lui échappe, l'interconnexion à opérer devra réussir à décoder les subtilités humaines et *a fortiori* juridiques. En effet, ce type de dispositif demandera un effort particulier en matière d'investissement, de R&D et de supervision au moment de son déploiement. Sa généralisation posera indubitablement des questions de responsabilité en cas de dysfonctionnement (mauvaise transmission, altération de données, conditions de captation difficiles ou impossibles, …), d'erreur ou de piratage, qui constitueront un nouveau champ d'investigation pour les juristes formés sur les notions techniques des

[2387] LARCHEVEQUE (Éric), préc.
[2388] *Id.*
[2389] NEVEJANS (Nathalie), « Une introduction juridique à l'Objet Intelligent », art. cit.
[2390] *Id.*
[2391] Pour une définition détaillée de l'IoT et de l'interconnexion entre Internet et objets, *supra* n° 66.
[2392] MEKKI (Mustapha), « *Blockchain* et métiers du droit en questions », *D. IP/IT* 2020, n° 2, p. 87.
[2393] Rapp. n° 464, 15 mars 2017, pour une intelligence artificielle maîtrisée, utile et démystifiée, déposé par Claude DE GANAY et Dominique GILLOT, au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques.

nouvelles technologies et exigera, en outre, une collaboration étroite entre juristes et programmeurs.

CONCLUSION GÉNÉRALE

356. Le contexte actuel contraint à se résigner ; l'objectif de disruption initial n'a pas encore été pleinement atteint par la technologie. En effet, les tiers traditionnels de confiance ne sont pas tous remplaçables. La technologie s'avère, en l'état actuel, à tout point de vue incapable d'égaler l'œuvre du notaire français ou l'autorité protectrice du juge étatique, par exemple. Selon les applications envisagées, la volonté de simplification des relations entre les Hommes semble tantôt élargir remarquablement le champ des possibilités, tantôt être réduite à une simple promesse. Par ailleurs, la philosophie qui sous-tend la technologie *blockchain* est, d'une manière générale, profondément imprégnée d'une difficile acceptation de l'État, de ses composantes, de ses fondements et de ses Lois. Seulement, en rejetant le droit, elle écarte également la sécurité juridique qu'il s'évertue à instituer. Toute technologie, de surcroît émergente, s'appliquant au domaine contractuel et dont le produit est censé matérialiser une « sphère de confiance » dans les relations entre les individus, ne peut se déployer pleinement si les parties n'ont pas la certitude de pouvoir s'y fier. Ainsi, pour qu'une véritable disruption soit opérée, la technologie doit-elle être capable d'instaurer une sécurité suffisante, s'apparentant à la sécurité juridique des Lois étatiques, capable de résoudre les récurrentes problématiques du domaine contractuel autant que les problèmes engendrés par ses propres spécificités. Plus encore, pour passer du déploiement à l'acceptation sociétale et à l'utilisation à grande échelle de la technologie, il appartient à ses concepteurs d'apporter aux utilisateurs une valeur ajoutée par rapport au système déjà existant. Autrement dit, il s'agit de leur fournir une valable raison d'abandonner un système, certes critiquable mais malgré tout efficace, en faveur d'une nouveauté dont l'avenir est incertain.

357. Bien qu'en l'état de l'art, la technologie ne peut se substituer à toutes les professions basées sur la confiance, soutenir qu'elle ne produit des effets juridiques somme toute limités semble excessif. Elle ouvre des opportunités inédites d'économie transparente, équitable et démocratique[2394]. S'il est indubitablement nécessaire de percevoir les dangers à travers l'engouement de l'innovation, il serait injuste de méconnaître son potentiel, tant découvert qu'à découvrir. Promettant la mise en place

[2394] GIRAUD (Thomas), « Vie culturelle - La *blockchain* est-elle l'avenir de la culture ? », *Vie culturelle JAC*, 2017, n° 51, p. 35.

d'une sécurité juridique accrue, le déploiement d'une *blockchain* exécutant automatiquement ou, à tout le moins, sollicitant automatiquement d'exécuter les termes d'un contrat prédéterminé s'est montré capable d'établir un suivi dans l'exécution de celui-ci, et plus encore lorsque la technologie devient à la fois un instrument et une garantie tantôt virtuelle tantôt physique de l'exécution du contrat par le biais de l'interconnexion des technologies. Or, cette assistance est de nature à renforcer l'efficacité de la force contractuelle donnée à l'engagement et à instaurer *ipso facto* un climat de confiance entre les parties dès la formation du contrat. En instaurant une confiance triangulaire entre les cocontractants et les algorithmes dans les transactions dites « consensuelles », et en facilitant la constitution, la conservation et la restitution intègre de preuves dans le domaine[2395], tout en proposant une nouvelle variété de signature électronique et, d'une manière plus générale, une réappropriation des données personnelles et la limitation du nombre d'intermédiaires, la technologie de la chaîne de blocs semble révéler des dispositions techniques et technologiques suffisantes pour pouvoir, à terme, s'imposer. En témoigne la démarche de réédification de la confiance sur Internet initiée par la Commission européenne, qui envisage de s'appuyer sur la technologie *blockchain* pour créer une identité décentralisée et sécurisée pour tous les citoyens européens[2396]. Un temps d'acceptation, et de formation, sera sans doute nécessaire à tout point de vue, tant les mutations générées seront considérables[2397]. Mais comme le souligne Boris Barraud, la *blockchain* n'est-elle pas « au même stade que le protocole TCP/IP, avant l'invention du *World Wide Web* »[2398] ?

358. S'il est essentiel de ne pas passer à côté de l'innovation, il n'empêche que celle-ci doit être perçue davantage comme un progrès plutôt qu'une éventuelle contrainte. Il convient alors de rester prudent vis-à-vis d'une technologie qui n'en est qu'à ses balbutiements[2399]. C'est notamment la raison pour laquelle il est indéniable que celle-ci ne pourra évoluer, ni hors du droit, ni d'ailleurs en marge des juristes. L'automaticité et la rigidité qui la caractérisent constituent parfois des obstacles à l'institution d'une

[2395] Notaires du Grand Paris, « Présentation de la BlockChain Notariale. Dossier de Presse », *Notaires du Grand Paris* [en ligne], 7 juill. 2020, p. 4, https://notairesdugrandparis.fr/sites/default/files/2020-07-07%20-%20DP%20-%20Pr%C3%A9sentation%20de%20la%20Blockchain%20Notariale%20VF2.pdf.
[2396] *Ibid.*, pp. 12 et s. ; AGOSTI (Pascal), « Identité numérique, eIDAS et blockchain...Vers un nouveau paradigme centré surl'utilisateur », *L'Usine Digitale* [en ligne], 26 mai 2020, https://www.usine-digitale.fr/article/identite-numerique-eidas-et-blockchain-vers-un-nouveau-paradigme-centre-sur-l-utilisateur.N968186.
[2397] LEGEAIS (Dominique), « Blockchain », *JCl. Sociétés Traité*, fasc. 2160, n° 14.
[2398] BARRAUD (Boris), « Les blockchains et le droit », *RLDI* 2018/4, n° 147, p. 49.
[2399] COLLOMB (Alexis), SOK (Clara), LEGER (Lucas), « Technologie des registres distribués : quel impact sur les infrastructures financières ? », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), p. 28.

confiance pleine et entière dans son algorithme, à moins pour ce dernier de renouer avec les pratiques relationnelles humaines. Pour cela, il doit commencer par reconnaître l'importance du rôle joué par l'Homme pour gérer les particularités humaines, à l'instar de tous les principes et subtilités que connaît et applique le droit pour protéger les contractants et qui font toute la différence dans l'univers juridique, puis évaluer les solutions et adapter ses comportements. Aussi la technologie devrait-elle accueillir l'assistance proposée par les actuels Oracles notamment humains, tout en s'efforçant de sécuriser techniquement la moindre de leurs interventions au sein de la chaîne, du moins le temps pour les Oracles physiques de faire leurs preuves. Une telle adaptation de la technologie sera également essentielle pour permettre à certains professionnels du droit, et en particulier les juges, d'intervenir pour offrir aux utilisateurs des garanties qui lui font défaut[2400]. En la matière, le juge, sous diverses qualifications, constitue en effet depuis longtemps le garant national de la sécurité juridique et du droit en tant que principal intermédiaire des parties et autorité décisionnelle. Si la technologie permettait au juge de retrouver l'essentiel de son autorité en la matière, ce dernier pourrait rééquilibrer le rapport de force contractuel actuellement imposé par le code.

359. L'adaptation de la technologie aux règles de droit est inévitable. Cependant, cette adaptation, pour être véritablement efficace, devra être réciproque. Un faux rapport de force instauré depuis l'origine de la *blockchain* survit entre eux alors même qu'ils partagent le même objectif, à savoir : offrir aux sujets de droit et aux justiciables une plus grande sécurité. Dans son *Discours des inégalités*, Jean-Jacques Rousseau décrivait déjà les conséquences de l'inertie face au changement en constatant que les Hommes étaient « devenus pauvres sans avoir rien perdu, simplement parce que tout changeait autour d'eux et qu'eux n'avaient point changé »[2401]. Originellement décentralisé et distribué, le protocole des *blockchains* publiques encourage l'auto-régulation *via* la neutralité de l'algorithme. Seulement, le dilemme posé par *TheDAO* a conduit la communauté à remettre en question son principe de neutralité pour favoriser la protection des utilisateurs. Or, l'histoire de l'innovation technologique témoigne de l'intérêt croissant pour le fait technique et des nombreuses tendances à l'appropriation des technologies afin d'en tirer un profit personnel[2402], si bien qu'une analogie semble s'établir entre le développement actuel de la *blockchain* et le développement qu'a connu Internet ces dernières années[2403].

[2400] MEKKI (Mustapha), « *Blockchain* et métiers du droit en questions », *D. IP/IT* 2020, n° 2, p. 87.
[2401] ROUSSEAU (Jean-Jacques), *Discours sur l'inégalité*, éd. Marc-Michel Rey, 1755. Pour une publication plus récente, v., ROUSSEAU (Jean-Jacques), *Œuvres complètes*, éd. Le Seuil, 1971, p. 228.
[2402] SMYRNAIOS (Nikos), *Les GAFAM contre l'internet*, éd. Ina, 2017, pp. 7-9.
[2403] *Id.*

Face au risque pour l'État de laisser à nouveau s'échapper un bien commun qui contribuera à créer, à terme, des monopoles économiques, la question se pose de savoir s'il ne serait pas mieux que ce soit le droit étatique qui se charge de lui donner un cadre, tout en garantissant de respecter ses principes et ses spécificités. Tel est le danger que représente, pour l'un, comme pour l'autre, un refus de s'adapter. La réflexion doit donc commencer dès aujourd'hui afin de bâtir, d'une part, l'équilibre nécessaire entre *blockchain* et droit[2404] et, d'autre part, la confiance que nécessitera la *blockchain* pour prendre sa place[2405]. L'Homme délègue l'exécution de son contrat social, mais c'est finalement en lui qu'il est demandé de faire confiance initialement. Ce dernier constat semble d'ailleurs raisonner en faveur d'un maintien des principes de décentralisation et de distributivité propres à la *blockchain* originelle, autrement dit publique, associée à un système de récompense, clé de l'incitation des mineurs et, au-delà, de la garantie de sa neutralité. En parallèle, la *blockchain* devrait laisser la place dans son code informatique, non seulement pour l'instauration de règles de fonctionnement conformes au droit, mais également de règles effectives et *by design* de gouvernance[2406]. En effet, lorsqu'une technologie vante ses qualités de « machine à créer de la confiance »[2407], les attentes sont nécessairement démultipliées, tout comme le risque de les décevoir. Lorsque la convoitise et les intentions malveillantes de certains individus mettent en péril la stabilité de la technologie, son protocole doit être capable de mobiliser et de faciliter l'application des règles protectrices en la matière, et ses développeurs de prendre des mesures pour endiguer les failles techniques et d'assumer, s'il y a lieu, leurs responsabilités vis-à-vis des utilisateurs, notamment en ce qui concerne les données à caractère personnel. Seulement, l'application du droit exige de pouvoir identifier le responsable, de sorte que le déploiement d'un mécanisme, propre, d'identification est clairement indispensable. Tels seront sûrement les prérequis juridiques nécessaires à l'essor de la confiance en la *blockchain*.

360. Néanmoins, il s'avère que les règles juridiques et techniques, même adaptées à sa spécificité, ne suffiront pas si en parallèle la technologie ne gagne pas en maturité[2408]. Seulement, pour qu'elle s'impose comme standard technologique, tel que Moody's,

[2404] HELLEU (Guillaume), MASURE (Anthony), « Total Record. Les protocoles blockchain face au post-capitalisme », *Multitudes* 2018/2, n° 71, p. 77.
[2405] ZOLINSKY (Célia), « Fintech – Blockchain et smart contracts : premiers regards sur une technologie disruptive », *RD bancaire et fin.* 2017, dossier 4, n° 22.
[2406] COLLOMB (Alexis), SOK (Clara), LEGER (Lucas), art. cit., p. 28.
[2407] « The promise of the blockchain: The trust machine », *The Economist* [online], 31 Oct. 2015, https://www.economist.com/leaders/2015/10/31/the-trust-machine.
[2408] ZOLINSKY (Célia), art. cit., *loc. cit.*

société d'analyse financière, le prévoit pour la fin d'année 2021[2409], il sera essentiel que l'innovation puisse se déployer et créer les circonstances propices au développement d'une confiance algorithmique. Comme pour tout modèle économique fondé sur des logiciels libres et ouverts, il semble pertinent « de ne pas intervenir trop en amont et de laisser les entreprises innover, tout en auditant les ressources du droit positif »[2410]. Si la technologie a besoin d'évoluer pour pouvoir espérer dépasser les obstacles psychologiques de la confiance et véritablement égaler les qualités attendues des tiers de confiance actuels tout en assurant pleinement les critères de neutralité et d'intégrité, elle ne pourra par ailleurs y parvenir qu'en atteignant l'autonomie[2411]. C'est dans ce contexte qu'une alliance avec des solutions d'IA pourrait être envisagée. Tout porte à croire que les solutions d'IA pourraient permettre aux algorithmes des *blockchains* de solutionner les « problèmes normalement résolus par les humains »[2412] et ainsi de dépasser leurs propres limites. En retour, elles bénéficieraient des capacités de traçabilité et de transparence des systèmes de *blockchains* pour s'assurer, vis-à-vis d'elles-mêmes et des utilisateurs, de l'intégrité des données qu'elles utilisent. Chacune trouverait alors dans l'autre la particularité qui fait défaut dans son propre code informatique. Toutefois, une telle combinaison de technologies n'exclut pas l'apparition de nouvelles problématiques juridiques[2413], notamment en matière de responsabilité, dont il conviendra d'évaluer les impacts.

[2409] « Research Announcement: Moody's - Blockchain standardisation will amplify benefits for securitisations », *Moody's* [online], 5 Sept. 2019, https://www.moodys.com/research/Moodys-Blockchain-standardisation-will-amplify-benefits-for-securitisations--PBS_1193318?WT.mc_id=AM%7ERmluYW56ZW4ubmV0X1JTQl9SYXRpbmdzX05ld3NfTm9fVHJhbnNYXRpb25z%7E20190905_PBS_1193318.
[2410] ZOLINSKY (Célia), art. cit., *loc. cit.*
[2411] MEKKI (Mustapha), « Les mystères de la blockchain », *D.* 2017, n° 37, pp. 2160 et s., n° 10.
[2412] COURTOIS (Georgie), « Blockchain et intelligence artificielle : vers une symbiose technologique ? », *in* « Dossier : Blockchain, une révolution juridique ? », *RLDA* 2017/9, n° 129.
[2413] *Supra* n° 77.

Annexes

Table des annexes

Annexe n° 1. Extrait d'une transaction sur *Bitcoin* 433

Annexe n° 2. Schéma simplifié du mécanisme de transaction sur *blockchain* 434

Annexe n° 3. Schéma simplifié du mécanisme d'inscription d'une transaction sur *blockchain*..... 435

Annexe n° 4. Schéma simplifié du principe du langage à pile 436

Annexe n° 5. Schéma simplifié de la cryptologie asymétrique, fondement des protocoles des *blockchains*..... 437

Annexe n° 6. Schéma exposant la provenance des bi-clés 438

Annexe n° 7. Schéma de la signature numérique *via blockchain* : l'exemple de *Bitcoin* 439

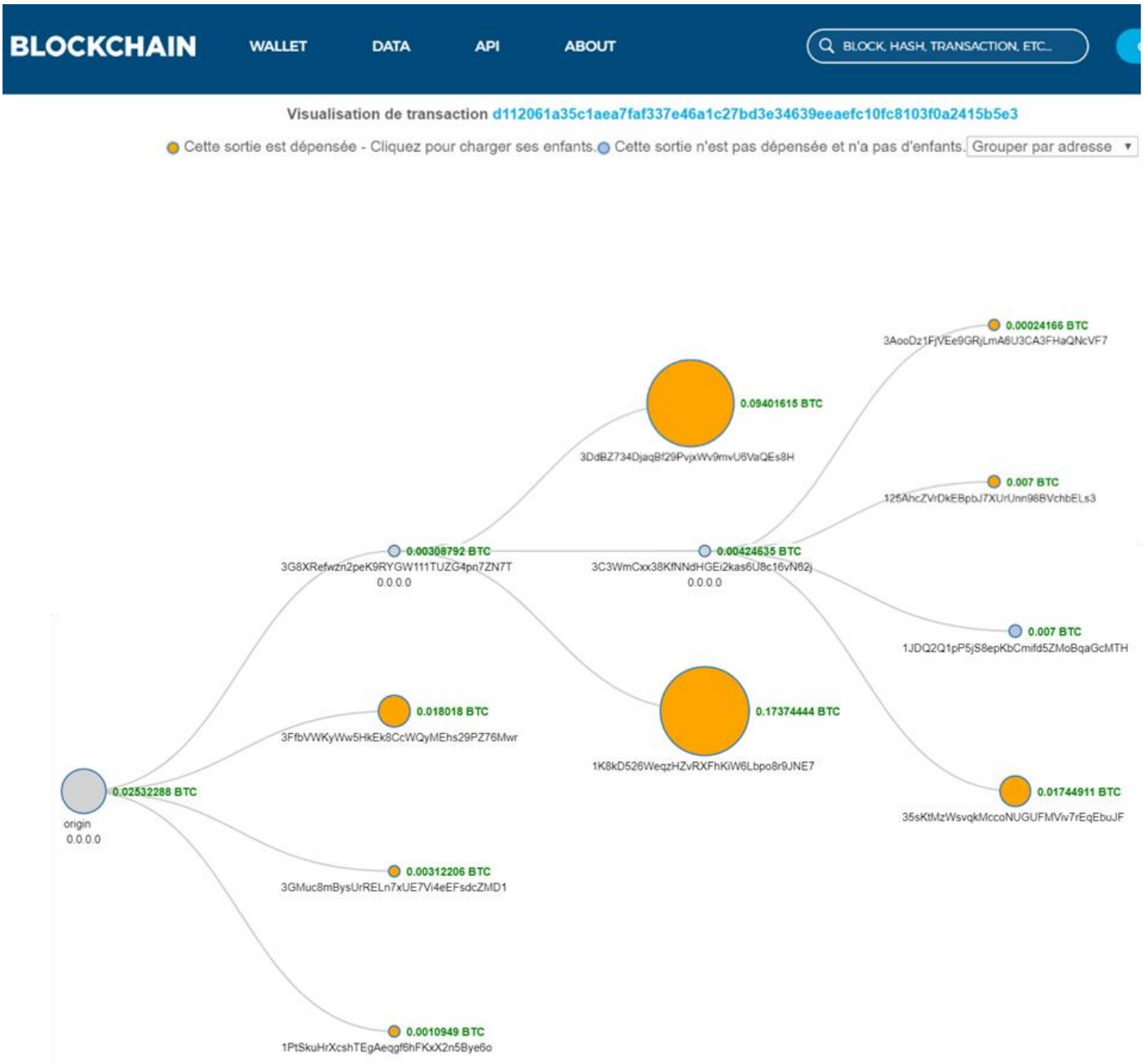
Annexe n° 8. Schéma de validation de blocs sur *blockchain* : l'exemple de *Bitcoin*... 440

Annexe n° 9. Traduction d'une chaîne de transactions sur *blockchain* : l'exemple de *Bitcoin*..... 441

Annexe n° 10. Schéma du contenu d'un bloc d'une *blockchain* : l'exemple de *Bitcoin* (blocs n^{os} 549 313 à 549 315)..... 442

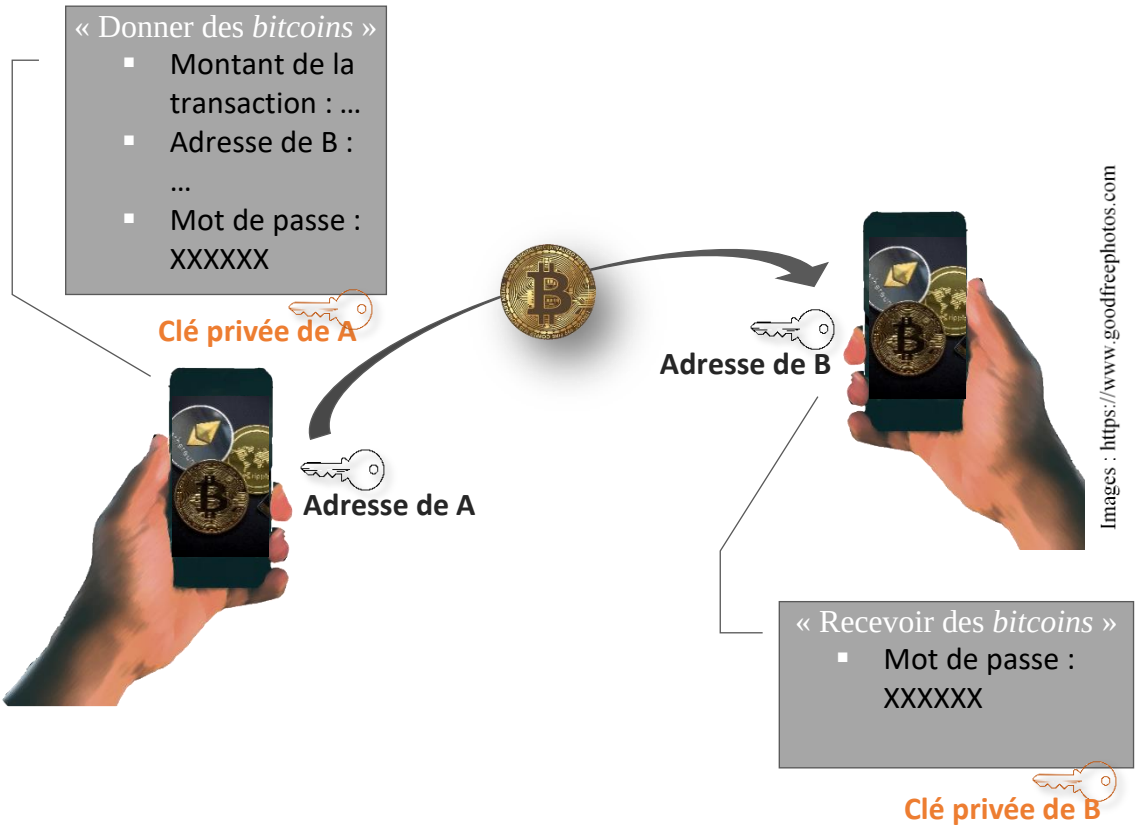
Annexe n° 11. Schéma d'un *fork* d'une *blockchain* 443

Annexe n° 1. Extrait d'une transaction sur *Bitcoin*[2414]

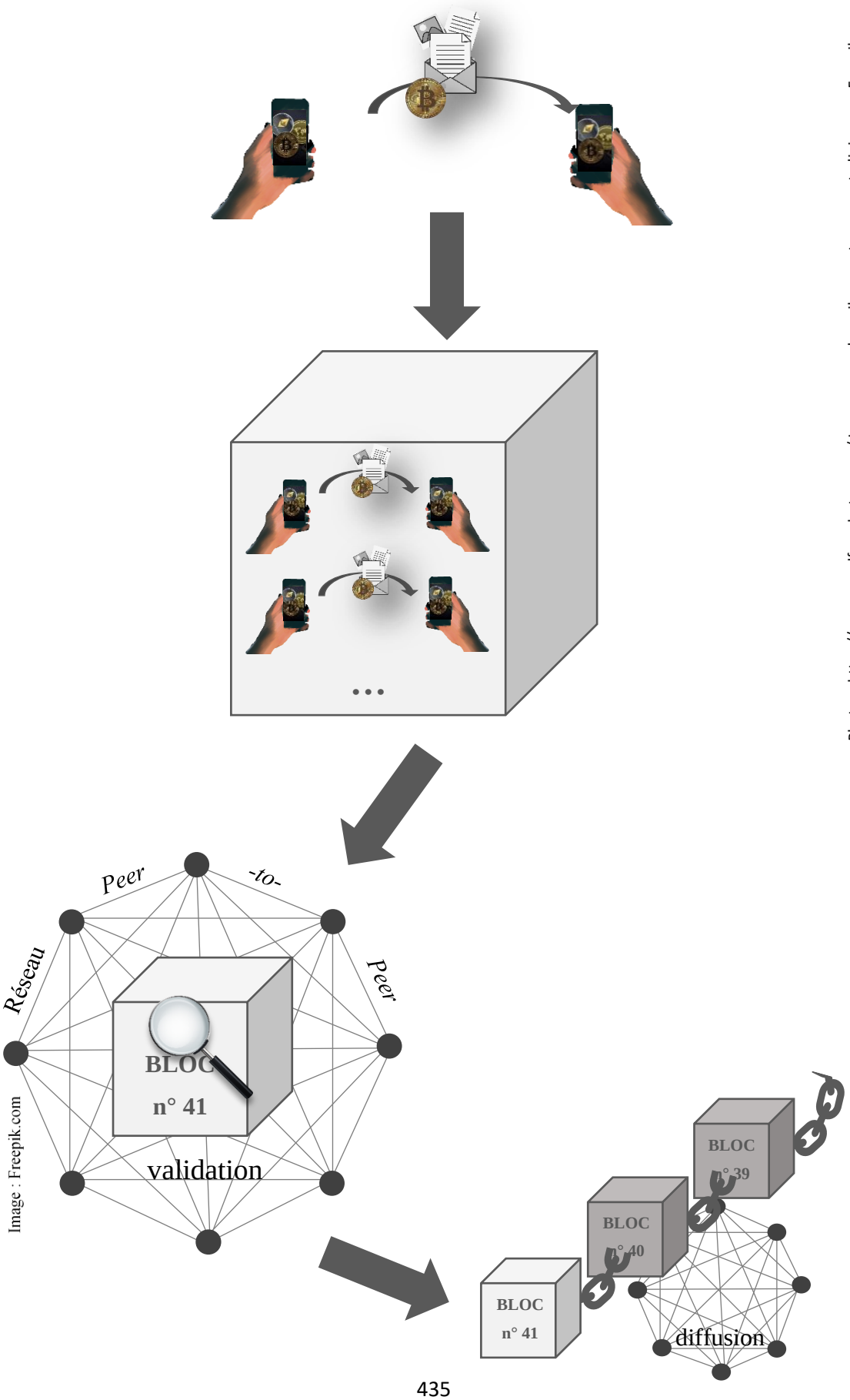


[2414] Blockchain.com, Données > Explorateur > Transactions > Voir le graphique. Ce site internet permet de visualiser l'origine d'une transaction émise en temps réel sur la *blochcin* du *Bitcoin*. En l'espèce, il s'agit d'un extrait de la chaîne de transactions « d112061a35c1aea7faf337e46a1c27bd3e34639eeaefc10fc8103f0 a2415b5e3 » [https://www.blockchain.com/fr/btc/tree/387809862].

Annexe n° 2. Schéma simplifié du mécanisme de transaction sur *blockchain*

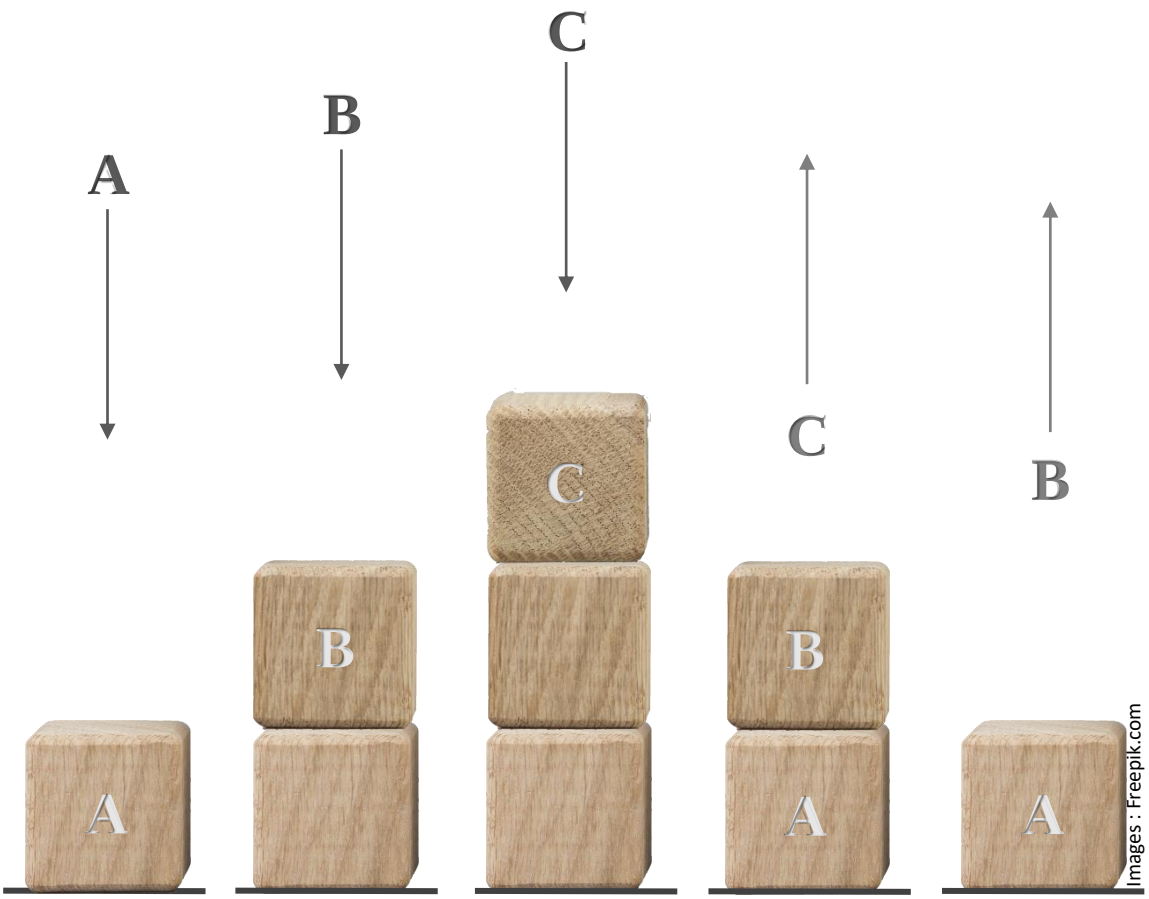


Annexe n° 3. Schéma simplifié du mécanisme d'inscription d'une transaction sur *blockchain*



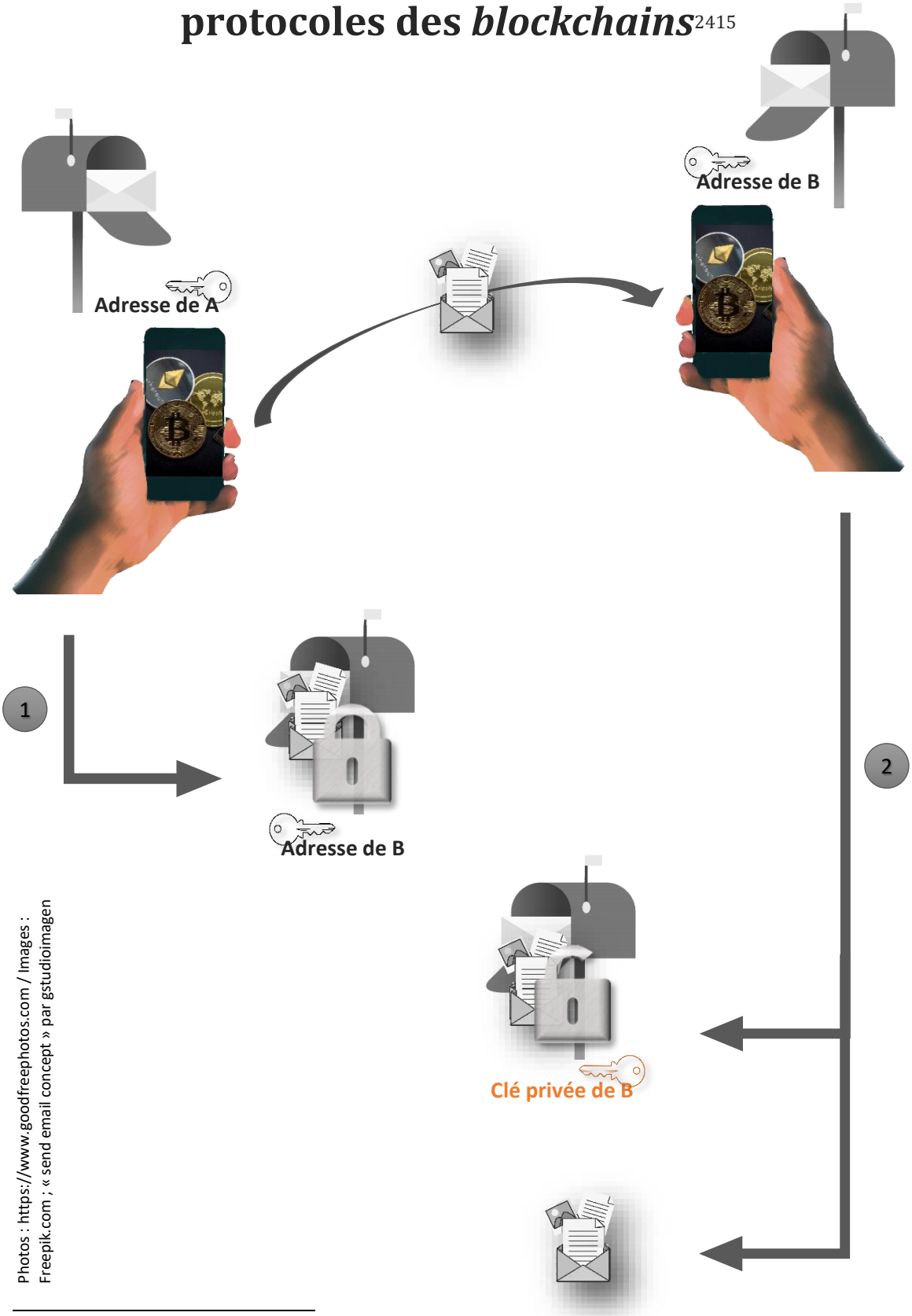
Photos : https://www.goodfreephotos.com / Images « send email concept » : par gstudioimagen, Freepik.com

Annexe n° 4. Schéma simplifié du principe du langage à pile



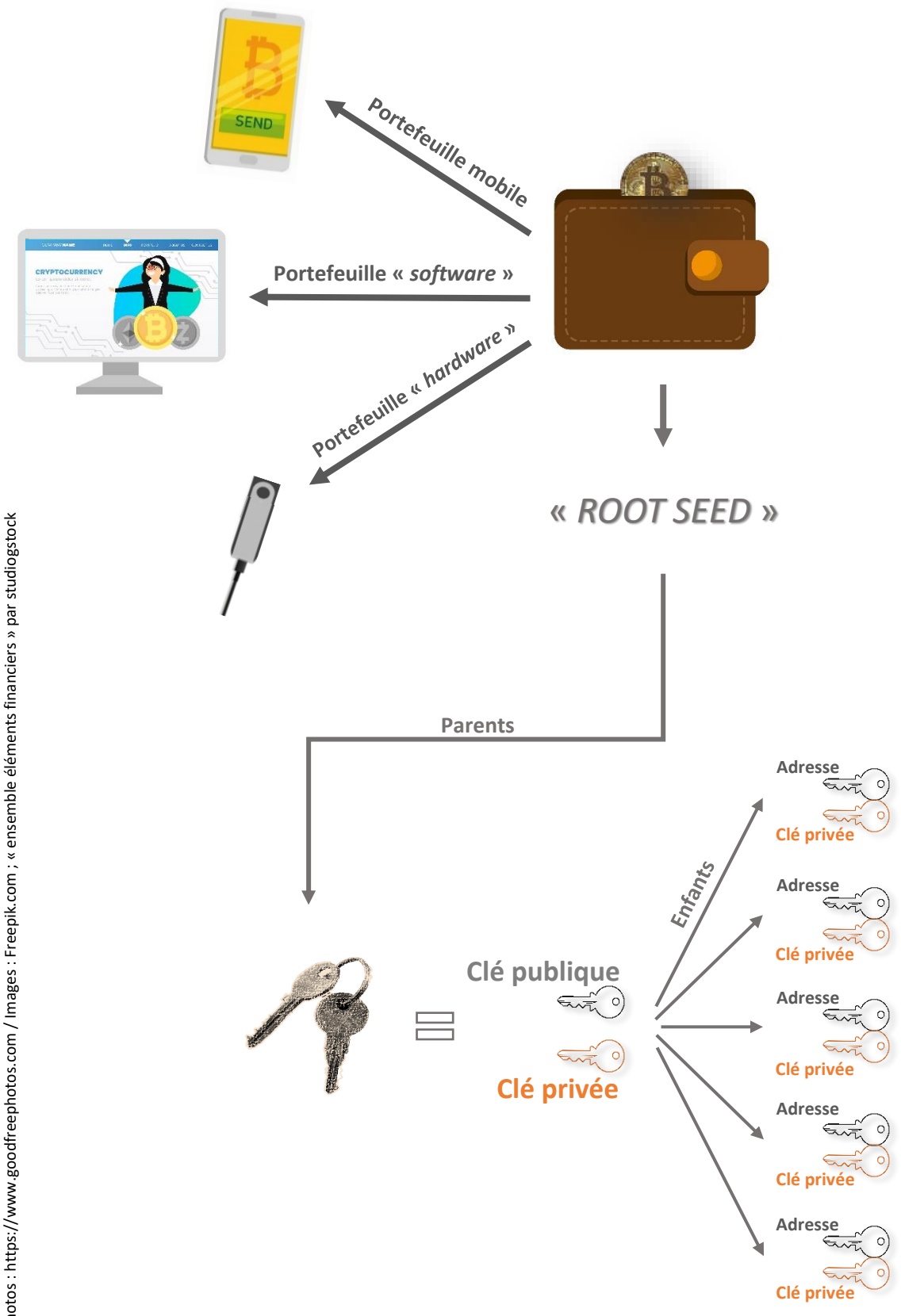
Comment récupérer A ?

Annexe n° 5. Schéma simplifié de la cryptologie asymétrique, fondement des protocoles des *blockchains*[2415]



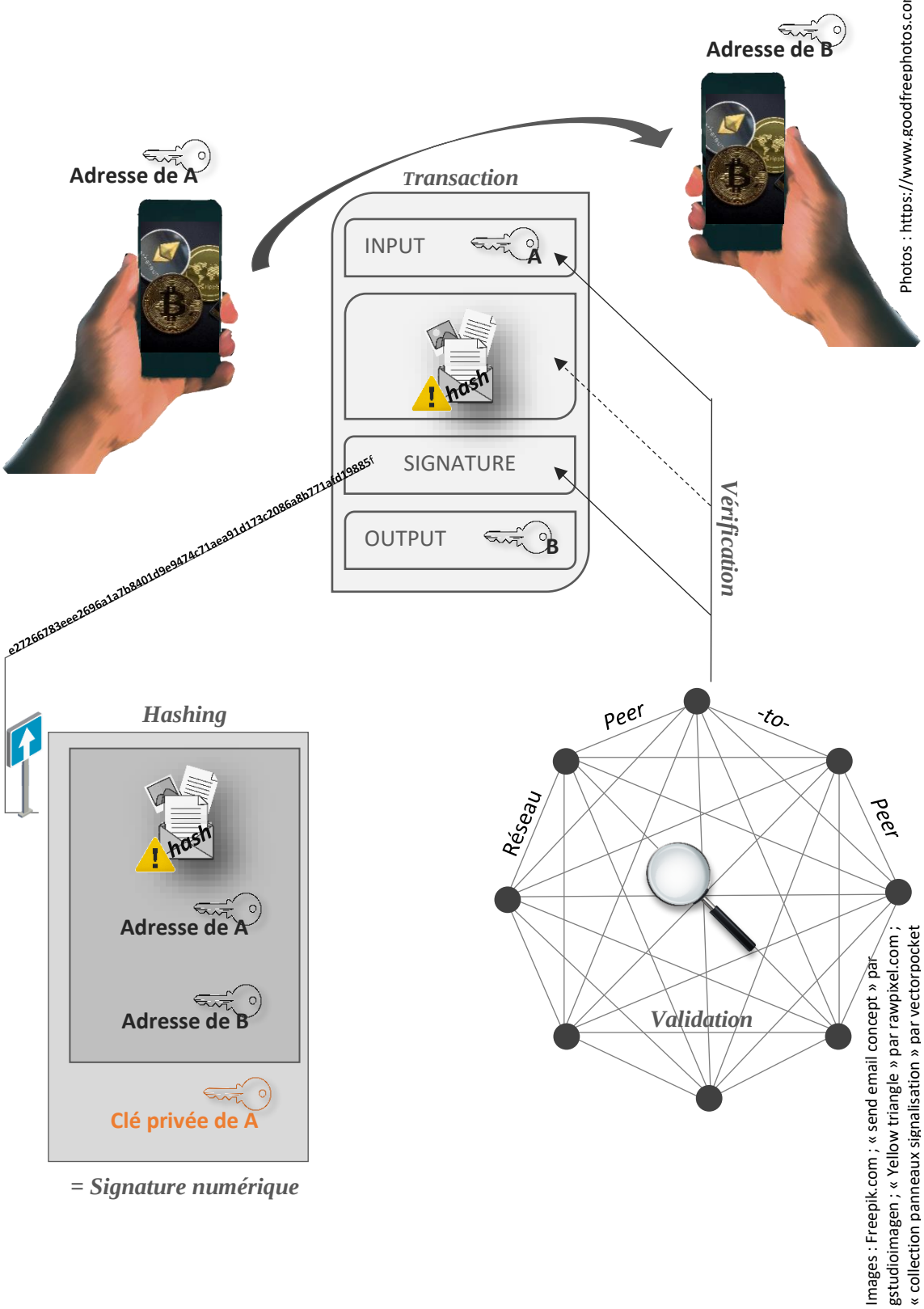
[2415] En effet, les *blockchains* actuelles ont complété (pour la plupart) et intégré ce procédé de chiffrement mathématique au sein de leur protocole. C'est notamment le cas de celle du *Bitcoin*, v., Annexe n° 7. Schéma de la signature numérique *via blockchain* : l'exemple de *Bitcoin*, p. 437.

Annexe n° 6. Schéma exposant la provenance des bi-clés

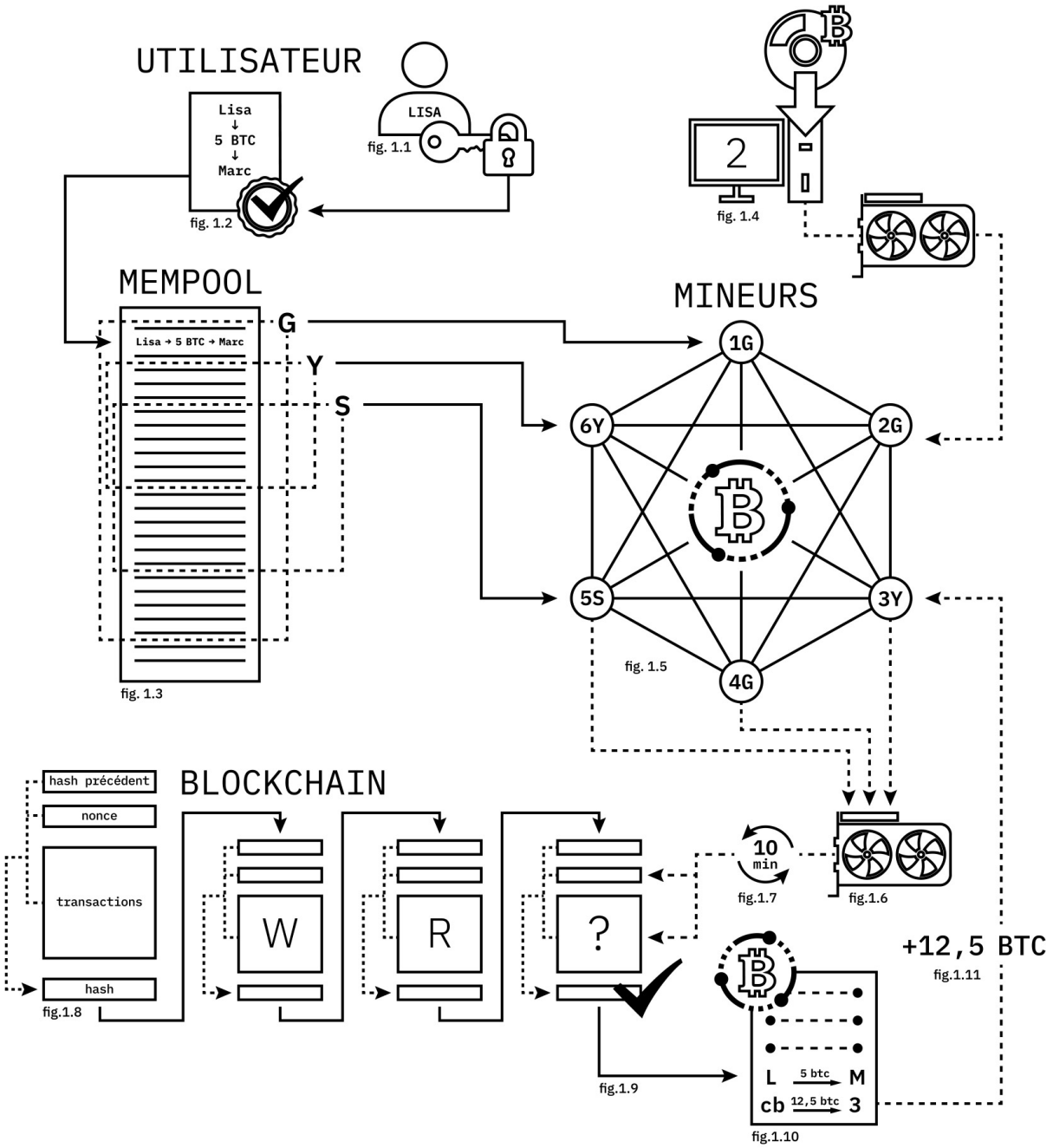


Photos : https://www.goodfreephotos.com / Images : Freepik.com ; « ensemble éléments financiers » par studiogstock

Annexe n° 7. Schéma de la signature numérique *via blockchain* : l'exemple de *Bitcoin*

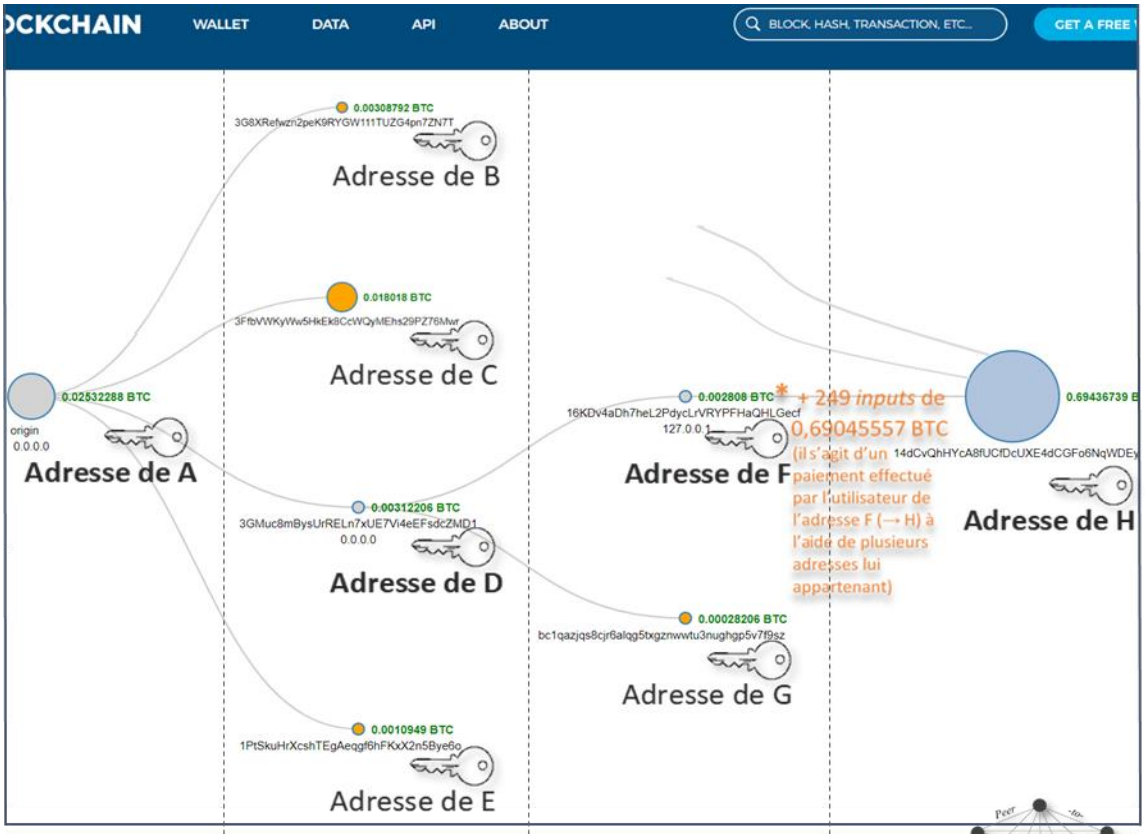


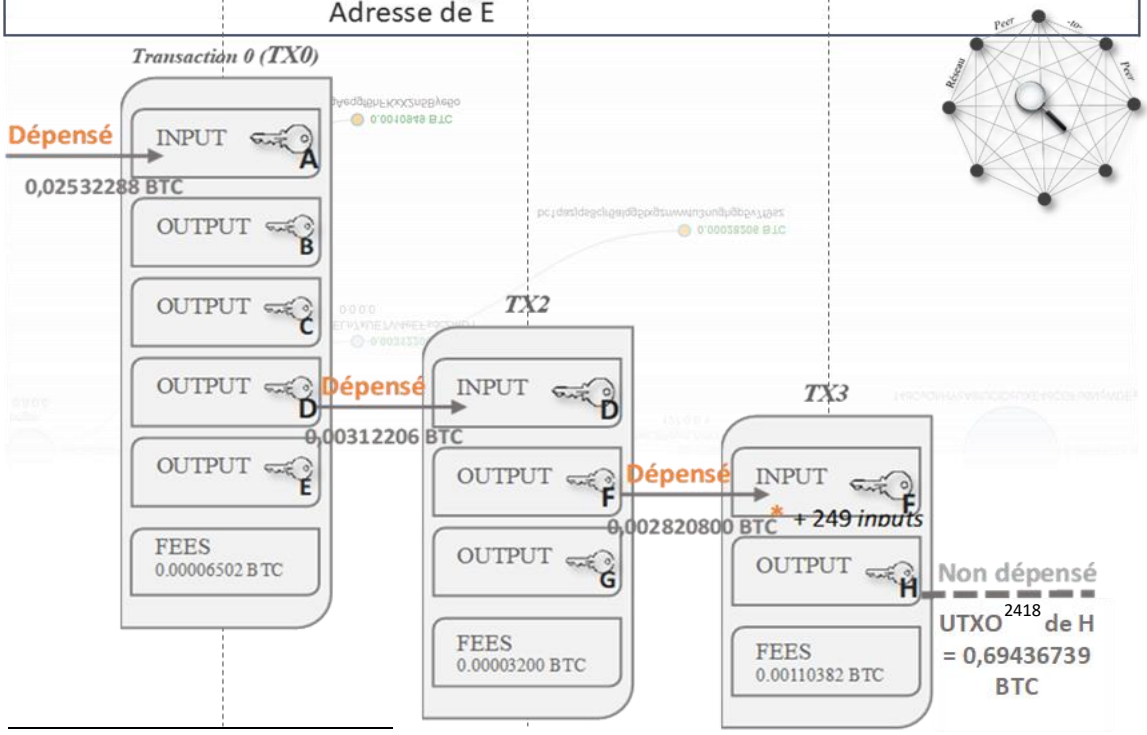
Annexe n° 8. Schéma de validation de blocs sur *blockchain* : l'exemple de *Bitcoin*[2416]



[2416] HELLEU (Guillaume), MASURE (Anthony), « *Total Record*. Les protocoles *blockchain* face au post-capitalisme », *Multitudes* 2018/2, n° 71.

Annexe n° 9. Traduction d'une chaîne de transactions sur *blockchain* : l'exemple de *Bitcoin*[2417]

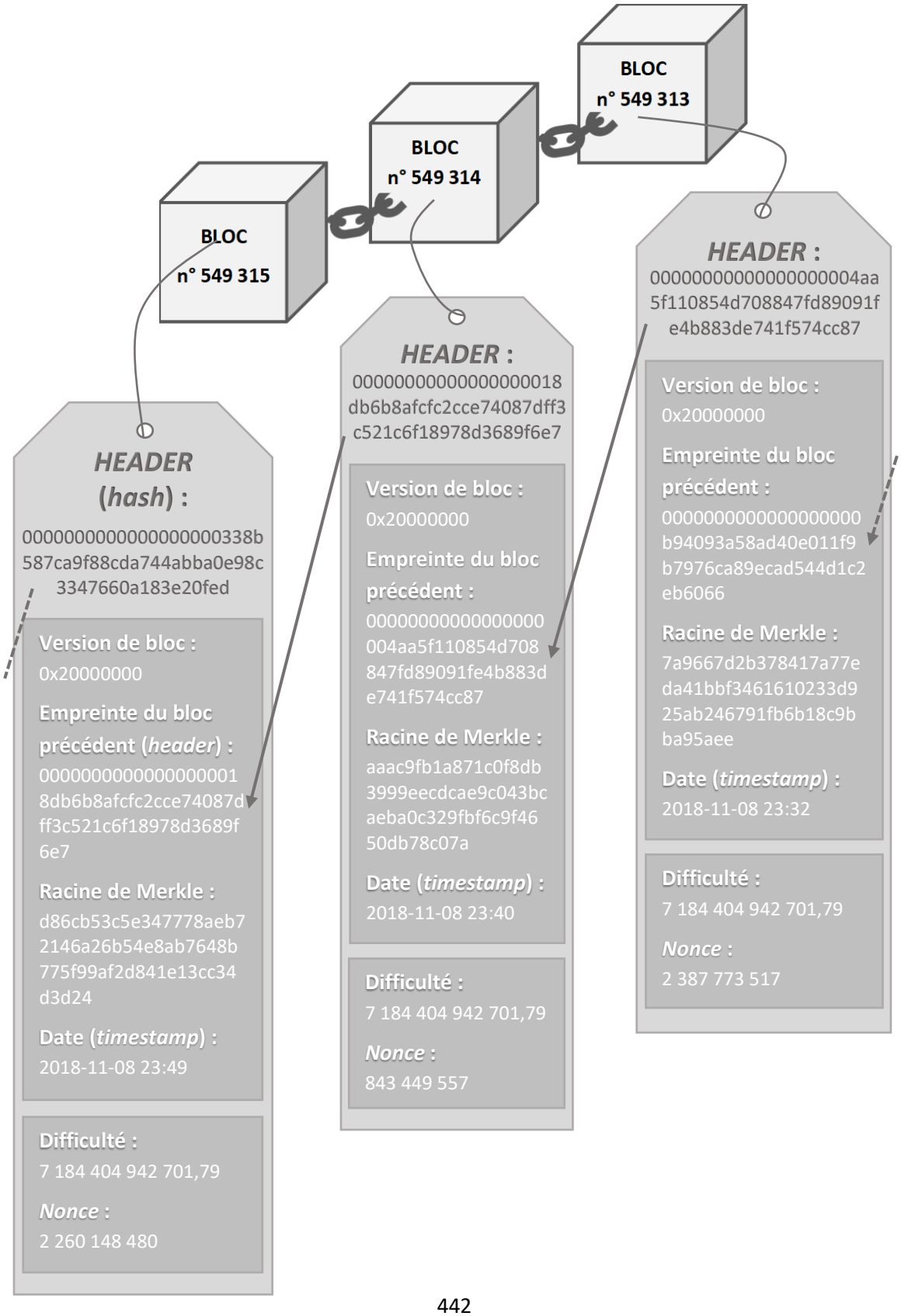




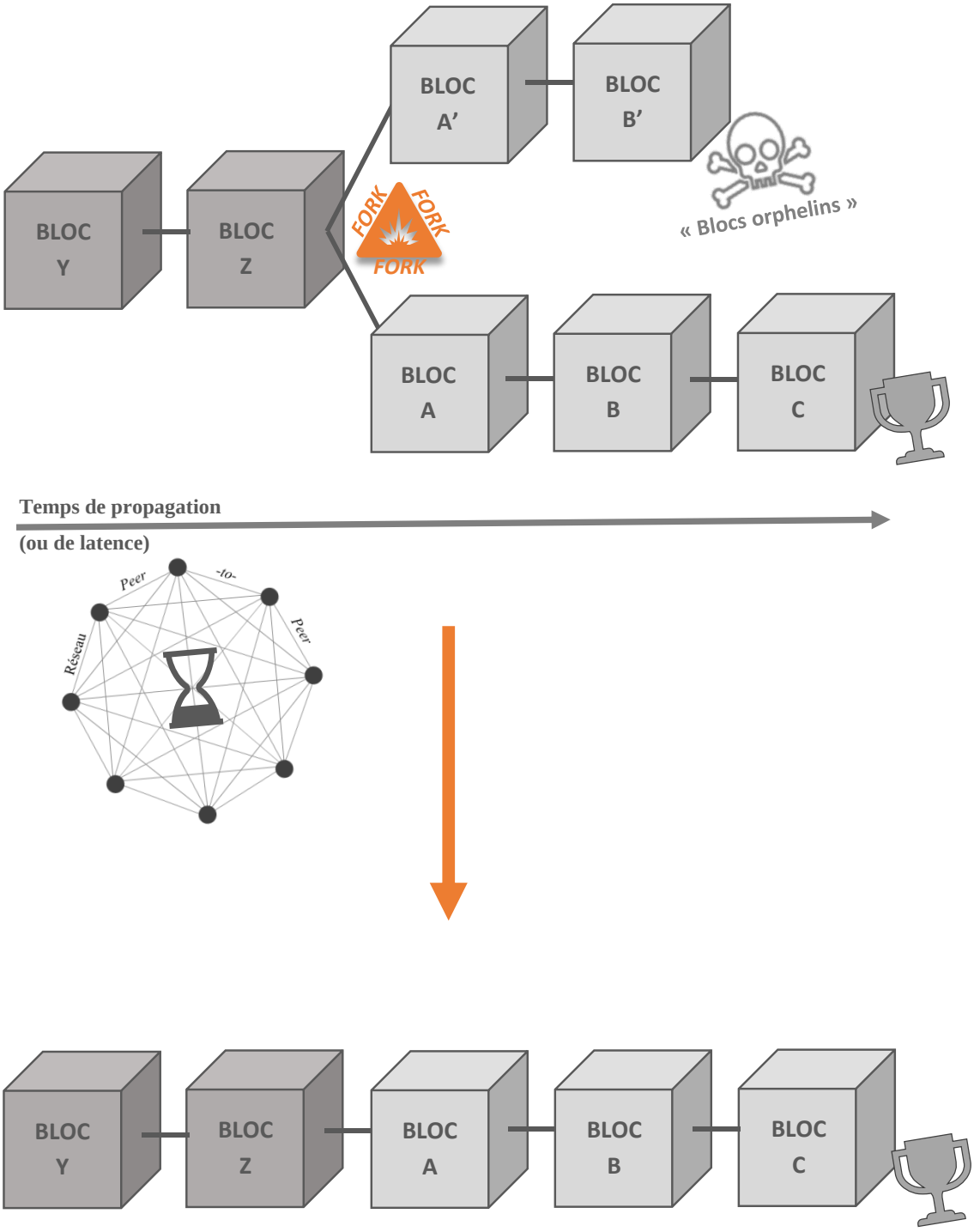
[2417] Blockchain.com, Données > Explorateur > Transactions > Voir le graphique, préc.

[2418] « UTXO » signifie « *Unspent Transaction Outputs* » qui sont l'ensemble des *outputs* des transactions passées antérieurement et non dépensées par des *inputs*. En l'espèce, l'adresse H peut donc dépenser les BTC détenus.

Annexe n° 10. Schéma du contenu d'un bloc d'une *blockchain* : l'exemple de *Bitcoin* (blocs n°s 549 313 à 549 315)



Annexe n° 11. Schéma d'un *fork* d'une *blockchain*



Bibliographie

I. Sources juridiques

A. Ouvrages généraux, manuels, cours, traités

ANCEL (Marie-Élodie), DEUMIER (Pascale), LAAZOUZI (Malik), *Droit des contrats internationaux*, éd. Sirey, 2e édition, coll. Sirey Université, 2019.

BEIGNER (Bernard), BEN HADJ YAHIA (Sonia), *Droit des assurances*, éd. LGDJ, 3e édition, coll. Précis Domat, Privé, 2018.

BENABENT (Alain), *Droit des obligations*, éd. LGDJ, 18e édition, coll. Précis Domat, Privé, 2019.

CARBONNIER (Jean), *Droit civil*, t. II, éd. PUF, Coll. Thémis, 5e édition, 1967.

CORNELOUP (Sabine), DELEBECQUE (Philippe), JACQUET (Jean-Michel), *Droit du commerce international*, éd. Dalloz, 3e édition, coll. Précis, Droit privé, 2015.

DEMOLOMBE (Charles), *Cours de Code Napoléon*, éd. Auguste Durand & Louis Hachette, vol. 29, t. VI, n° 502, 1876.

FABRE-MAGNAN (Muriel), *Le droit des* contrats, éd. Presses Universitaires de France, coll. « Que sais-je ? », 2018.

HOUTCIEFF (Dimitri), *Droit des contrats*, éd. Bruylant, 5e édition, coll. Paradigme – Manuels, 2020.

JULIEN (Jérôme), *Droit de la consommation*, éd. LGDJ, 3e édition, coll. Précis Domat, Privé, 2019.

LE BARS (Thierry), HÉRON (Jacques), *Droit judiciaire privé*, éd. LGDJ, coll. Domat privé, 7e édition, 2019.

LE TOURNEAU (Philippe), *Droit de la responsabilité et des contrats*, éd. Dalloz, 12e édition, coll. Dalloz action, 2020.

MOUGENOT (Dominique), *Droit des obligations, la preuve*, éd. Larcier, 4e édition, 2017.

PLANIOL (Marcel), RIPERT (Georges), *Traité pratique de droit civil français*, éd. LGDJ, t. III, 1931.

TOULLIER (Charles Bonaventure Marie), *Le droit civil français suivant l'ordre du Code*, t. VIII, éd. Jules Renouard et Cie, 4e édition, 1824.

VIGNAL (Thierry), *Droit international privé*, éd. Sirey, 2017.

B. Ouvrages spéciaux, mémoires, thèses

BACHOFEN (Blaise), BIZIOU (Michaël), BRAHAMI (Frédéric) *et al.*, *Le libéralisme au miroir du droit : l'État, la personne, la propriété*, éd. ENS, 2008.

BARBET-MASSIN (Alice), Fleuret (Faustine), Lourimi (Alexandre) *et al.*, *Droit des crypto-actifs et de la blockchain*, éd. LexisNexis, coll. Droit & professionnels, 2020.

BENSOUSSAN (Alain), FORSTER (Frédéric), *Droit des objets connectés et télécoms*, éd. Bruylant, coll. Lexing - Technologies avancées & Droit, 2017.

BONNEAU (Thierry), VERBIEST (Thibault), *Fintech et Droit : Quelle régulation pour les nouveaux entrants du secteur bancaire et financier ?*, éd. RB, coll. Les essentiels de la banque et de la finance, 2017.

CARON (Christophe), *Droit d'auteur et droits voisins*, éd. LexisNexis, 6e édition, 2019.

COTIGA-RACCAH (Andra), JACQUEMIN (Hervé), POULLET (Yves), *Les blockchains et les smart contracts à l'épreuve du droit*, éd. Larcier, 1e édition, coll. Collection du Crids, 2020.

DE FILIPPI (Primavera), WRIGHT (Aaron), *Blockchain and the Law: The Rule of Code*, ed. Hardcover, 2018.

DE TOCQUEVILLE (Alexis), *De la démocratie en Amérique*, éd. C. Gosselin, 1835 et 1840.

DEBARD (Thierry), GUINCHARD (Serge), *Lexique des termes juridiques 2020-2021*, éd. Dalloz, 28e édition, août 2020.

DESCOTEAUX (David), *Quel cadre réglementaire pour Bitcoin ?*, Institut Économique de Montréal, Les notes économiques, coll. Réglementation, juin 2014.

DEVERGRANNE (Thiébaut), *La propriété informatique*, sous la direction de Jérôme Huet, Paris : Université Panthéon-Assas (Paris II), 2007.

DOARÉ (Ronan), DANET (Didier), DE BOISBOISSEL (Gérard) (dir.), *Drones et killer robots : Faut-il les interdire ?*, éd. Presses universitaires de Rennes, coll. L'Univers des normes, 2015.

FAUCHOUX (Vincent), DEPREZ (Pierre), DUMONT (Frédéric) *et al.*, *Le droit de l'internet*, LexisNexis, 3e édition, coll. Droit & Professionnels, 2017.

FAVIER (Jacques), TAKKAL BATAILLE (Adli), *Bitcoin. La monnaie acéphale*, éd. CNRS, coll. Économie Droit, 2017.

FÉRAL-SCHUHL (Christiane), *CyberDroit : Le droit à l'épreuve de l'Internet*, éd. Dalloz, coll. Praxis Dalloz, 8e édition, 2020.

GARAPON (Antoine), *Bien juger. Essai sur le rituel judiciaire*, éd. Odile Jacob, 1997.

GEIBEN (Didier), JEAN-MARIE (Olivier), VERBIEST (Thibault), *et al*., *Bitcoin et Blockchain : Vers un nouveau paradigme de la confiance numérique ?*, éd. RB, coll. Les essentiels de la banque et de la finance, 2016.

GRYNBAUM (Luc), LE GOFFIC (Caroline), MORLET-HAÏDARA (Lydia), *Droit des activités numériques*, éd. Dalloz, 1ère édition, 2014.

KERIKMÄE (Tanel), RULL (Addi), *The Future of Law and eTechnologies*, ed. Springer, 2016.

LACROIX (Guillaume), *L'adaptation du contrat aux changements de circonstances*, Reims : Université de Reims, 2015.

LE TOURNEAU (Philippe), *Contrats du numérique*, éd. Dalloz, coll. Dalloz Référence, 2021-2022.

LEGEAIS (Dominique), *Blockchain et actifs numériques*, éd. LexisNexis, coll. Actualités, 2019.

LEMESLE (Bruno) *et al*., *La preuve en justice : de l'Antiquité à nos jours*, éd. Presses universitaires de Rennes, 2015.

LORRE (Pierre-Marie), *Blockchain : évolution ou révolution pour les contrats en France ?*, Courbevoie : Institut Léonard de Vinci, 2016.

MOUTON (Dimitri), *Sécurité de la dématérialisation : De la signature électronique au coffre-fort numérique, une démarche de mise en œuvre*, éd. Eyrolles, coll. Solutions d'entreprise, 2012.

NETTER (Emmanuel), *Numérique et grandes notions de droit privé*, éd. CEPRISCA, coll. Essais, 2019.

NEVEJANS (Nathalie), *Traité de droit et d'éthique de la robotique civile*, éd. LEH éditions, coll. Science, éthique et société, 2017.

PUIGELIER (Catherine) (dir.), *Dictionnaire juridique*, éd. Bruylant, 2e édition, 2017.

QUEMENER (Myriam), *Le droit face à la disruption numérique : Adaptation des droits classiques - Émergence de nouveaux droits*, éd. Gualino, Hors collection, 2018.

SUXE (Florent), *La preuve du contrat électronique*, Paris : Université Jean Monnet Paris XI, 2012.

TESTU (François Xavier), *Contrats d'affaires*, éd. Dalloz, 2e édition, coll. Dalloz Référence, 2021-2022.

WAHAB (Mohamed S. Abdel), KATSH (Ethan), RAINEY (Daniel), *Online Dispute Resolution: Theory and Practice*, ed. Eleven International Publishing, 2012.

ZICRY (Laure), *Cyber-risques : Le nouvel enjeu du secteur bancaire et financier*, éd. RB, coll. Les essentiels de la banque et de la finance, 2017.

C. Articles

BENABENT (Alain), « La bonne foi dans l'exécution du contrat », *in Travaux de l'Association Henri Capitant. La bonne foi*, (Journées. Louisianaises 1992), t. XLIII, éd. Litec, 1994, pp. 294 et s.

BLONDEAU (Alison), « Le juge civil face au secret entourant le système de clé privée sur blockchain », *in* NEVEJANS (Nathalie) (dir.), *Données et technologies numériques. Approches juridique, scientifique et éthique*, éd. mare & martin, coll. Droit & Science politique, 2021, pp. 155-164.

CAPRIOLI (Éric A.), « Introduction au droit de la sécurité des systèmes d'information », *in Droit et technique - Études à la mémoire du Professeur Xavier Linant de Bellefonds*, éd. Litec, 2007, pp. 75 et s.

CARBONNIER (Jean), « Les phénomènes d'inter-normativité », *in European Yearbook in Law and Sociology*, 1977, pp. 42-52.

DE FILIPPI (Primavera), « Perspectives et enjeux des blockchains de demain », *in* YERETZIAN (Antoine) (dir.), *La blockchain décryptée : les clefs d'une révolution*, éd. Netexplo, 2016, pp. 32-38.

GRIMALDI (Michel), « Le testament et le cyber-notaire », *in Mélanges Jérôme Huet*, éd. Lextenso, 2018, pp. 211 et s.

GUILLAUME (Florence), « Blockchain : le pont du droit international privé entre l'espace numérique et l'espace physique », *in* PRETELLI (Ilaria) (dir.), *Conflict of Laws in the Maze of Digital Platforms. Le droit international privé dans le labyrinthe des plateformes digitales. Actes de la 30e Journée de droit international privé du 28 juin 2018 à Lausanne*, éd. Schulthess Éditions Romandes, 2018, pp. 163-192.

MAXIME (Julienne), « Le nantissement de titres financiers inscrits en blockchain », *in* MAGNIER (Véronique), BARBAN (Patrick) (dir.), *Blockchain et droit des sociétés*, éd. Dalloz, 2019, pp. 54 et s.

NEVEJANS (Nathalie), « L'usine connectée : l'usine à l'ère du numérique sous le prisme du droit », *in* CHÉRIGNY (Florence), ZOLLINGER (Alexandra) (dir.), *Les objets connectés. Colloque "30 ans du magistère en droit des TIC" Vendredi 23 septembre 2016*, éd. Presses Universitaires juridiques de Poitiers, coll. Actes et colloques de la Faculté de Droit et des Sciences sociales, 2018, pp. 33-65.

D. Ouvrages encyclopédiques, fascicules

ANCEL (Pascal), « Imprévision : Approche historique et comparative », *Rép. civ. Dalloz*, v° Imprévision, 2018, n°s 14 et s.

BARBAROUX (Nicolas), BARRON (Richard), FAVREAU (Amélie), « Blockchain et finance – approche pluridisciplinaire », *Répertoire IP/IT et Communication Dalloz*, v° Les actifs Numériques, 2021, n°s 2-79.

CANTERO (Anne), CAPRIOLI (Eric A.), LE CERF (Xavier), « Commerce électronique », *Le Lamy droit des médias et de la communication*, n°468-107.

CHANTEPIE (Gaël), « Contrat : effet », *Rép. civ*. *Dalloz*, v° Contrat, 2018, n° 307.

CHANTEPIE (Gaël), SAUPHANOR-BROUILLAUD (Natacha), « Déséquilibre significatif », *Rép. com. Dalloz*, v° Déséquilibre significatif, 2019, n° 139.

CHOLET (Didier), « Vérification d'écriture », *Rép. pr. civ. Dalloz*, v° Rôle du juge et des parties, 2016 (actualisation : 2019), n°s 9-11.

DAVERAT (Xavier), « Saisie : protection du débiteur – Difficultés économiques du débiteur », *Rép. pr. civ. Dalloz*, v° Difficultés économiques du débiteur, 2019, n°s 123-144.

DEVÈZE (Jean) (dir.), « Innovations dans l'univers des cryptomonnaies », *Le Lamy Droit du Financement*, n° 2905.

FAGES (Bertrand), « La phase de conclusion », *Le Lamy Droit du Contrat*, n°s 400 et s.

FAGES (Bertrand), « La loi contractuelle », *Le Lamy Droit du Contrat*, n°s 1721 et s.

GASSIN (Raymond), « Fraude informatique », *Rép. pén. Dalloz*, v° Fraude informatique, 1995, n° 70.

GUÉVEL (Didier), « Force probante de la date d'un acte sous seing(s) privé(s) : Date certaine », *JCl. Civil Code*, fasc. Unique.

GUEZ (Philippe), « Contrat de courtage », *JCl. Contrats-Distribution*, fasc. 850, n° 6.

GUINCHARD (Serge), DRAGO (Guillaume), « Réforme de la procédure civile en 1958 et Constitution de la V^e^ République », *Rép. pr. civ. Dalloz*, v° Droit constitutionnel et procédure civile, 2018, n° 15.

LARDEUX (Gwendoline), « Preuve : modes de preuve », *Rép. civ. Dalloz*, v° Les preuves parfaites, 2019, n° 207.

LE TOURNEAU (Philippe), POUMARÈDE (Matthieu), « La bonne foi dans l'exécution du contrat », *Rép. civ. Dalloz*, v° Bonne foi, 2019, n° 81.

LECOURT (Arnaud), « Droit des sociétés et numérique », *Répertoire IP/IT et Communication Dalloz*, v° Numérique et constitution de la société, 2020, n°s 4-30.

LECOURT (Arnaud), « Droit des sociétés et numérique », *Répertoire IP/IT et Communication Dalloz*, v° Numérique et fonctionnement de la société, 2020, n°s 31-56.

LEGEAIS (Dominique), « Blockchain », *JCl. Com.*, fasc. 534.

LEGEAIS (Dominique), « Blockchain », *JCl. Sociétés Traité*, fasc. 2160.

MOURALIS (Jean-Louis), « Preuve : Modes de preuve », *Rép. civ. Dalloz*, v° Preuve, 2011, n°s 102, 193.

PERRAY (Romain), « Données à caractère personnel. Introduction générale et champ d'application de la règlementation relative à la protection des données personnelles », *JCl. Communication*, fasc. 930.

PICOD (Yves), « CONTRAT. – Force obligatoire du contrat. – Bonne foi », *JCl. Civil Code*, fasc. Unique.

PILLET (Gilles), « Le fonctionnement du pacte de préférence », *Rép. civ. Dalloz*, v° Pacte de préférence, 2016 (actualisation : janv. 2019), n°s 67 et s.

ROBINE (David), PAILLER (Pauline), « Instruments financiers », *Le Lamy droit des sûretés - Expert*, n° 251.

WARUSFEL (Bertrand), « Section 2 - Régulation du cyberespace et encadrement spécifique », *Le Lamy Droit du Numérique* 2020, n°s 2111 et s.

E. Revues, publications périodiques et ressources numériques

« Le notariat à l'heure de la blockchain », *AJ fam.* 2018, p. 260.

« Les Notaires du Grand Paris lancent la "Blockchain Notariale" », *Defrénois* 16 juill. 2020, n° DEF161W1, p. 11.

ALLEN (Jessie), « Blind Faith and Reasonable Doubts: Investigating Beliefs in the Rule of Law », *Seattle University Law Review*, Vol. 24, 2001, p. 716.

ALMASEANU (Stephen), « Le traitement pénal du Bitcoin et des autres monnaies virtuelles », *Gaz. Pal*. 30 août 2014, n° 242, p. 11.

ANCEL (Bruno), « Les smart contracts : révolution sociétale ou nouvelle boîte de Pandore ? Regard comparatiste », *Comm. com. électr*. 2018, n°s 7-8, étude n°13.

ANCIAUX (Arnaud), FARCHY (Joëlle), MÉADEL (Cécile), « L'instauration de droits de propriété sur les données personnelles : une légitimité économique contestable », *Revue d'économie industrielle* 2017/2, n° 158, pp. 9-41.

ARONICA (Charles), « La clause du client le plus favorisé », *AJCA* 2014, n° 2, p. 69.

AUDIT (Mathias), « Le droit international privé confronté à la blockchain », *Rev. crit. DIP* 2020, p. 669.

AVENA-ROBARDET (Valérie), « Prochaine réforme du surendettement », *AJ fam*. 2012, p. 363.

AYNÈS (Laurent), « La révocabilité du mandat irrévocable », *D.* 2002, n° 37, p. 2858.

AYNÈS (Laurent), « Le contrat, loi des parties », *Cahiers du conseil constitutionnel* [en ligne], n° 17 (dossier : loi et contrat), mars 2005, https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/le-contrat-loi-des-parties.

BABONNEAU (Marine), « L'acte d'avocat sera dématérialisé », *Dalloz actualité*, 23 juill. 2013.

BADOUR (Ana), VAN WIJNGAARDEN (Arie), « UK Financial Conduct Authority Proposes Global Fintech Regulatory Sandbox », *McCarthy Tetrault*, 23 Feb. 2018.

BALLARDINI (Rosa María), PITKÄNEN (Olli), « Balancing Exclusive Rights and Access to Technologies: Blockchain and Intellectual Property Rights », *D. IP/IT* 2019, n° 2.

BARBET-MASSIN (Alice), « Réflexions autour de la reconnaissance juridique de l'horodatage blockchain par le législateur italien », *RLDI* 2019/3, n° 157.

BARBIER-CHASSAING (Françoise), « Garantir la sécurité des données et mieux prendre en compte la cybercriminalité dans une logique de responsabilisation pour les entreprises », *D. IP/IT* 2019, n° 4.

BARBRY (Éric), « Smart contracts... Aspects juridiques ! », *Annales des Mines – Réalités industrielles* 2017/3 (août 2017), pp. 77-80.

BARRAUD (Boris), « Le droit en datas : comment l'intelligence artificielle redessine le monde juridique (PARTIE II : Les nouvelles technologies juridiques ou l'intelligence artificielle au service du droit) », *RLDI* 2019/12, n° 165.

BARRAUD (Boris), « Les blockchains et le droit », *RLDI* 2018/4, nº 147.

BARREAU (Catherine), « La régulation des smart contracts et les smart contracts des régulateurs », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), pp. 74-76.

BAUFUMÉ (Vivien), CARMINATI (Christophe), « La blockchain, un outil technologique… et juridique », *JCP N* 2020, entretien n° 30, p. 1162.

BEAUDEMOULIN (Nathalie) *et al*., « Les enjeux de la Blockchain pour la Banque de France et l'Autorité de Contrôle prudentiel et de Résolution (ACPR) », *Annales des Mines* - Réalités industrielles 2017/3 (août 2017), pp. 29-33.

BENOLIEL-CLAUX (Sylvie), « Protection par le droit d'auteur et le droit des dessins et modèles : cumul et contrefaçon, mode d'emploi », *D. IP/IT* 2019, n° 12.

BERBAIN (Côme), « La blockchain : concept, technologies, acteurs et usages », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), pp. 6-9.

BERBERICH (Mattthias), STEINER (Malgorzata), « Blockchain technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers? », *European Data Protection Law Review*, Vol. 2, Issue 3, 21 Mar. 2016, p. 422.

BERGÉ-LEFRANC (Clément), « La blockchain est une technologie très efficace pour se préconstituer une preuve », *RLDC* 2017/7, n° 150.

BESSON (Marie-Laure), « La responsabilité du rédacteur d'actes immobiliers à l'ère du numérique », *AJDI* 2021, n° 3, pp. 171-182.

BIGOT (Rodolphe), « La blockchain et l'assurance, la blockchain ou l'assurance ? », *RLDI* 2017/11, n° 142.

BIGOT (Rodolphe), « L'assurance, le droit et le digital : un mauvais remake du "bon, la brute et le truand" ? », *RGDA* janv. 2018, n° 115h0, p. 8.

BIRMINGHAM (Robert L.), « Breach of Contract, Damage Measures, and Economic Efficiency », *Rutgers Law Review*, No. 24, 1970, p. 284.

BOISMAIN (Corinne), « Quelques réflexions sur les contrats intelligents (smarts contracts) », *LPA* 1 mars 2021, n° 158q0, p. 6.

BOISSON (Alexis), FAVREAU (Amélie), « Actualité du droit des technologies nouvelles (juillet - décembre 2020) », *RLDC* 2021/1, n° 188.

BONDARD (Céline) (dir.), « Quelques utilisations actuelles de cet outil en droit des affaires - Monnaies virtuelles, transmission des instruments de paiement, outils de financement, smart contracts, etc. », *JCP E* 2017, n° 36, pp. 1471 et s.

BOSSÉ (Vianney), « L'Europe est à l'aube de l'ère de la blockchain », *Voxeurop*, 13 août 2020.

BOUDÈS (Thierry), « La blockchain déchaîne les questions ! », *Annales des Mines – Gérer et comprendre* 2018/1 (mars 2018), n° 131, pp. 83-85.

Cabinet d'avocats Simmons & Simmons LLP, « Le droit et la technologie blockchain : une approche sectorielle », *Contrats Concurrence et Consommation*, oct. 2017, n° 10, étude n° 10.

CALAIS-AULOY (Marie-Thérèse), « Le rôle du législateur et celui du juriste confrontes à l'idée de pacte républicain », *LPA* 31 août 1999, n° PA199917301, p. 4.

CANAS (Sophie), « Blockchain et preuve - Le point de vue du magistrat », *D. IP/IT* 2019, n° 2.

CAPRIOLI (Éric A.), « La blockchain ou la confiance dans une technologie », *JCP G* 2016, n°23-672, pp. 1162-1163.

CAPRIOLI (Éric A.), « Mythes et légendes de la blockchain face à la pratique », *D. IP/IT* 2019, n° 7-8.

CAPRIOLI (Éric A.), AGOSTI (Pascal), « Principales évolutions du régime de la signature, du cachet et de la copie numériques », *AJCA* 2016, n° 2.

CAPRIOLI (Éric) (dir.), « Blockchain et smart contracts : enjeux technologiques, juridiques et business », *JCP E* 2017, n° 2.

CAPRIOLI (Éric), « Charge de la preuve et signature électronique d'un contrat de crédit à la consommation : errances jurisprudentielles », *Comm. com. électr*. 2018, n° 10, comm. 78.

CAPRIOLI (Éric), « Première décision sur la preuve et la signature électroniques d'un contrat de crédit à la consommation », *JCP G* 2013, II, n° 18, pp. 866-869.

CAPRIOLI (Éric), « Signature électronique - Décret n° 2017-1416 du 28 sept. 2017 relatif à la présomption de fiabilité de la signature électronique », *Comm. com. électr*. 2017, n° 11, comm. 92.

CAPRIOLI (Éric), « Signature électronique d'un avenant électronique d'un contrat de crédit à la consommation », *Comm. com. électr*. 2014, comm. 2.

CAPRIOLI (Éric A.), « Vademecum juridique de la digitalisation des documents », *Fédération des Tiers de Confiance* [en ligne], 29 nov. 2016, pp. 28-32, https://fntc-numerique.com/upload/file/guides-fntc/Vademecum_Juridique.pdf.

CATTALANO (Garance), « Smart contracts et droit des contrats », *AJ contrat* 2019, p. 321.

CHARENTENAY (Simon), « Blockchain et Droit : Code is deeply Law », *Gaz. Pal*. 14 nov. 2017, n° GPL305g1, pp. 15 et s.

CHENEVIERE (Cédric), « *Fraudes et autres atteintes à l'intégrité du système d'échange de quotas d'émission* », *RLDA* 2011/1, nº 56.

CHEVALIER (Jacques), « L'internormativité », *HAL*, 2013, hal-01723912.

CHRISTODOULOU (Hélène), « Intelligence artificielle – Les nouvelles technologies à l'origine de l'évolution contractuelle », *Comm. com. électr*. 2020, n° 11, étude 20.

CIEPLAK (Jenny), « 5 reasons dispute resolution is critical for blockchain's growth », *World Economic Forum*, 14 Dec. 2020.

COHEN-HADRIA (Yaël), « Blockchain : révolution ou évolution ? », *D. IP/IT* 2016, n° 11, pp. 537 et s.

COIFFARD (Didier), « Entretien du mois : La Blockchain a un sens pour répartir une partie de la confiance en rendant une information infalsifiable mais cette confiance est très en deçà de celle conférée par le notaire », *RLDC* 2017/4, n° 147.

COLLOMB (Alexis), SOK (Clara), LEGER (Lucas), « Technologie des registres distribués : quel impact sur les infrastructures financières ? », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), pp. 29-33.

COURTOIS (Georgie), « Blockchain et intelligence artificielle : vers une symbiose technologique ? », *in* « Dossier : Blockchain, une révolution juridique ? », *RLDA* 2017/9, n° 129.

COUSIN (Anne), « Réparer le préjudice causé par la violation du RGPD », *D. IP/IT* 2019, n° 19.

D'ORNANO (Antoine), « Sur le projet Libra », *Rev. crit. DIP* 2020, vol. 1, n° 1, pp. 178-184.

DE POULPIQUET (Jeanne), « Exercice de la fonction notariale », *RDI* 2009 (actualisation : avr. 2020), pp. 252 et s.

DE THÉSUT DUFOURNAUD (Sylvie), « Les blockchains de consortium », *in* « Dossier : Blockchain, une révolution juridique ? », *RLDA* 2017/9, n° 129.

DEGOS (Louis), « Casser les codes ! », *Revue pratique de la prospective et de l'innovation* oct. 2017, n° 2.

DEJEAN (Philippe), SARTRE (Patrice), « La cyber-vulnérabilité », *Études*, vol. juill.-août, n° 7-8, 2015, pp. 21-31.

DELPECH (Xavier), « Un an de nouveau droit des contrats », *AJ contrat* 2017, p. 401.

DELZANNO (Clémentine), « Nouveaux process pour les gestionnaires de patrimoine », *Dr. & patr. Mensuel*, 1er oct. 2016, n° 162.

DENIS (Bénédicte), HEGEDUS (Orsolya), LAREDO (Anne), SOLERANSKI (Louis), « La Blockchain dans le secteur de l'assurance », *RLDA* 2017/12, n° 132.

DESOMBRE (Nicolas), DUVERNE (Denis), DE MONTCHALIN (Amélie), « Les stratégies d'internationalisation en assurances », *Rev. éco. fin.* 2017/2, n° 126, pp. 51-64.

DEVILLIER (Nathalie), « Jouer dans le « bac à sable réglementaire pour réguler l'innovation disruptive : le cas de la technologie de la chaîne de bloc », *RTD com*. 2017, p. 1037.

DOUVILLE (Thibault), « La dématérialisation des relations contractuelles en droit des assurances », *D. IP/IT* 2019, n° 11.

DOUVILLE (Thibault), VERBIEST (Thibault), « Blockchain et tiers de confiance : incompatibilité ou complémentarité ? », *D*. 2018, n° 5.

DRILLON (Sébastien), « La révolution Blockchain », *RTD com*. 2016, p. 893.

FABRIZI-RACINE (Nina), « La blockchain : (R)évolution d'État ? », *JCP A* 2017, n° 49, pp. 2306 et s.

FAVREAU (Amélie), « L'avenir de la propriété intellectuelle sur la blockchain », *Propriétés Intellectuelles*, 1er avr. 2018, n° 67, pp. 11-19.

FAVREAU (Amélie), « Présentation du projet de recherche sur les smart contracts », *D. IP/IT* 2019, n°1.

FÉNÉRON PLISSON (Claire), « La blockchain, un bouleversement économique, juridique voire sociétal », *Information, données & documents* 2017/3, vol. 54.

FINES SCHLUMBERGER (Jacques-André), « Les blockchains : une invention qui n'a pas dix ans », *Revue européenne des médias et du numérique* 2017, n° 44.

FITZGIBBON (Magali), « Analyses outillées de la propriété intellectuelle des logiciels et traçabilité des composants tiers », *RLDI* 2014/3, n° 102.

FLORI (Jean-Pierre), « Sécurité et insécurité de la blockchain et des smart contracts », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), pp. 98-101.

GALICHET (Charlotte), « Hébergeurs de sites internet : la loi pour la confiance dans l'économie numérique se superpose-t-elle à la loi Informatique et libertés ? », *D. IP/IT* 2019, n° 6.

GAVANON (Isabelle), « *Blockchain*, PI et mode : enjeux de la *blockchain* au regard des règles relatives à la preuve électronique », *D. IP/IT* 2019, n°2.

GELINAS (Fabien), CAMION (Clément), BATES (Karine), « Forme et légitimité de la justice – Regard sur le rôle de l'architecture et des rituels judiciaires », *Revue interdisciplinaire d'études juridiques* 2014/2, vol. 73, pp. 37-74.

GENESTIER (Philippe) *et al*., « Blockchains et Smart Contracts : des perspectives pour l'Internet des objets (IoT) et pour l'e-santé », *Annales des Mines – Réalités industrielles* 2017/3 (août 2017), pp. 70-73.

GEOFFRON (Patrice), VOISIN (Stéphane), « Comment mettre la *Blockchain* au service de la mise en œuvre de l'Accord de Paris sur le climat », *Annales des Mines - Responsabilité et environnement* 2019/2 (avr. 2019), n° 94, pp. 96 à 99.

GIJSBERS (Charles) *et al*., « Les fondamentaux du notariat confrontés à l'intelligence artificielle », *JCP N* 2018, n° 10, act. 1111.

GILLIOZ (Fabien), « Du contrat intelligent au contrat juridique intelligent », *D. IP/IT* 2019, n° 1.

GODEFROY (Lêmy), « La gouvernementalité des blockchains publiques », *D. IP/IT* 2019, n° 9.

GODEFROY (Lêmy), « Le code algorithmique au service du droit », *D.* 2018, n° 4, pp. 734 et s.

GOETZ (Charles J.), SCOTT (Robert E.), « Liquidated Damages, Penalties, and the Just Compensation Principle: A Theory of Efficient Breach », *Columbia Law Review*, Vol. 77, No. 4, May 1977, pp. 554-594.

GORCHS (Béatrice), « La responsabilité civile du médiateur civil », *Dr. et pr*. 2015, p. 194.

GOSSA (Julien), « Les blockchains et smart contracts pour les juristes », *D. IP/IT* 2018, n° 7-8, p. 393.

GRYNBAUM (Luc), « Assurances et blockchain », *RLDA* 2017/9, n° 129.

GUERLIN (Gaëtan), « Considérations sur les smart contracts », *D. IP/IT* 2017, n° 10.

GUILHAUDIS (Élise), « Comprendre la blockchain à travers l'étude d'un cas pratique : le covoiturage "Blockcar" », *RLDI* 2017/12, nº 143.

HAAS (Gérard), « Bilan après neuf mois d'application du RGPD », *D. IP/IT* 2019, n° 6.

HELLEU (Guillaume), MASURE (Anthony), « Total Record. Les protocoles blockchain face au post-capitalisme », *Multitudes* 2018/2, n° 71.

HERZOG (Philippe E.), « Tendances actuelles concernant les méthodes alternatives de résolution des controverses (Alternative dispute resolution – A.D.R.) aux États-Unis », *RGDP* 1999, pp. 774 et s.

HIELLE (Olivier), « La technologie Blockchain : une révolution aux nombreux problèmes juridiques », *Dalloz Actualité*, 31 mai 2016.

JAULT-SESEKE (Fabienne), « La blockchain au prisme du droit international privé, quelques remarques », *D. IP/IT* 2018, n° 10.

JOMNI (Adel), « Le RGPD : un atout ou un frein pour la cybersécurité ? », *D. IP/IT* 2019, n° 6.

JUANALS (Brigitte), « Protection des données personnelles et TIC au cœur des enjeux de société et de la mondialisation : les mécanismes d'un contrôle distribué », *TIC&société* 2014, vol. 8.

JULIENNE (Maxime), « Pratique notariale et numérique : état des lieux », *D. IP/IT* 2019, n° 2.

KEBIR (Mehdi), « Clause de conciliation préalable : application à une demande reconventionnelle », *AJDA* 2018, p. 308.

KORIN (Netta), « Using blockchain to monitor the COVID-19 vaccine supply chain », *World Economic Forum*, 20 Nov. 2020.

KRAJEWSKI (Trevor), LETTIERE (Rich), « Blockchain and Intellectual Property », *Les Nouvelles – Journal of the Licensing Executives Society*, Vol. LIV No. 1, 24 Mar. 2019, pp. 2-3.

KUNER (Christopher), CATE (Fred H.), LYNSKEY (Orla), MILLARD (Christopher), NI LOIDEAIN (Nora), « Blockchain versus data protection », *International Data Privacy Law*, Vol. 8, No. 2, 2 Jul. 2018, p. 104.

LASSERRE CAPDEVILLE (Jérôme), « L'avenir de la répression pénale contre certaines fraudes aux instruments de paiement. La transposition de la directive (UE) 2019/713 du 17 avril 2019 », *RD bancaire et fin*. 2021, n° 1, dossier 6.

LAURENT (Xavier), « Retour d'expérience sur le premier démantèlement d'une plateforme francophone du darkweb : le dossier Black Hand », *D. IP/IT* 2021, n° 2, p. 79.

LAURENT-BONNE (Nicolas), « La re-féodalisation du droit par la blockchain », *D. IP/IT* 2019, n° 7-8.

LE GUEN (Olivier), « Questions à Olivier Le Guen sur la perquisition et la saisie des crypto-actifs », *D. IP/IT* 2019, n° 10.

LE TROCQUER (Anne-Hélène), « Blockchain, gouvernance d'entreprise et infrastructures de marchés », *in* « Dossier : Blockchain, une révolution juridique ? », *RLDA* 2017/9, n° 129.

LEBEAU-MARIANNA (Denise), CAULIER (Tiphaine), « Délibération de la CNIL du 4 juillet 2019 sur les cookies : quelles conséquences pratiques pour les entreprises ? », D. IP/IT 2019, n° 12.

LECOURT (Arnaud), « Sanction des pratiques commerciales abusives d'Amazon », *D. IP/IT* 2019, n° 12.

LEGEAIS (Dominique), « La qualification des opérations portant sur le Bitcoin Observations sur la décision du tribunal de commerce de Nanterre du 26 février 2020 », *RD bancaire et fin*. 2020, n° 3, étude 7.

LEGRAND (Stéphanie), « Enjeux de la blockchain du point de vue du praticien », *D. IP/IT* 2019, n° 2.

LOUVET (Nicolas), « Les apports de la blockchain et des actifs numériques au secteur financier », *D. IP/IT* 2019, n° 10.

M. HYMAN (Gayle), P. DIGESTI (Matthew), « New Nevada Legislation Recognizes Blockchain and Smart Contracts Technologies », *Nevada Lawyer*, Aug. 2017.

MACLEAN (Fiona), « Governing the Blockchain: How to Determine Applicable Law », *Butterworths Journal of International Banking and Financial Law*, Jun. 2017, No. 6, pp. 359 et s.

MAGNIER (Véronique), « Enjeux de la blockchain en matière de propriété intellectuelle et articulation avec les principes généraux de la preuve », *D. IP/IT* 2019, n° 2.

MANAS (Arnaud), BOSC-HADDAD (Yoram), « La (ou les) blockchain(s), une réponse technologique à la crise de confiance », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), pp. 102-105.

MARC (François), « Comptes rendus de la commission des finances : Enjeux liés au développement des monnaies virtuelles de type bitcoin - Table ronde », *Sénat*, 15 janv. 2014.

MARGUÉNAUD (Jean-Pierre), « La Convention européenne des droits de l'homme et le notariat », *Defrénois* 15 déc. 1999, n° AD1999DEF1281N1, pp. 1293-1294.

MARIQUE (Enguerrand), « Les smart contracts en Belgique : une destruction utopique du besoin de confiance », *D. IP/IT* 2019, n° 1.

MARRAUD DES GROTTES (Gaëlle), « La blockchain : un secteur encore en phase d'exploration, mais très prometteur », *RLDI* 2017/2, n° 138.

MARRAUD DES GROTTES (Gaëlle), « Bitcoin, fork et prêt : un arrêt structurant vient d'être rendu », *Wolters Kluwer* [en ligne], 5 mars 2020, Actualités du droit > Tech&Droit > Blockchain, https://www.actualitesdudroit.fr/browse/tech-droit/blockchain/26266/bitcoin-fork-et-pret-un-arret-structurant-vient-d-etre-rendu.

MARRAUD DES GROTTES (Gaëlle), « DEEP : prochaine étape de régulation, la valeur légale de la preuve blockchain ? », *Wolters Kluwer* [en ligne], 2 sept. 2019, Actualités Du Droit > Tech&Droit > Blockchain, https://www.actualitesdudroit.fr/browse/tech-droit/blockchain/
23230/deep-prochaine-etape-de-regulation-la-valeur-legale-de-la-preuve-blockchain.

MARTIAL-BRAZ (Nathalie), « De quoi l'ubérisation est-elle le nom ? », *D. IP/IT* 2017, n° 4, pp. 133 et s.

MARTINON (Jacques), « Crypto-actifs : la justice pénale à l'épreuve des cryptomonnaies », *D. IP/IT* 2019, n° 10.

MARTINON (Jacques), « Phénomènes criminels célèbres ou exotiques dans le champ des crypto-actifs », *D. IP/IT* 2019, n° 10.

MAUGAIN (Géraldine), « Cas de recours préalable obligatoire aux modes de résolution amiable des différends », *in* « Dossier : Réforme de la procédure civile », *Dalloz actualité*, 20 janv. 2020, obs. MAUGAIN (Géraldine), SCHREIBER (Ulrik), MOURRE-SCHREIBER (Marie-Pierre) *et al*.

MAXIMIN (Nathalie), « Le plan d'action des douanes contre la contrefaçon », *D. IP/IT* 2021, n° 3, *in* Dossier de Presse « Présentation du plan contrefaçon 2021-2022 », Roissy, févr. 2021, p. 122.

MAYAUX (Luc), « Voyage au pays de l'assurance collaborative », *RGDA* juin 2017, n° 114r3, p. 337.

MAYMONT (Anthony), « La protection des particuliers face aux cryptomonnaies », *Contrats, conc. consom*. 2020, n° 3, alerte 10.

MEKKI (Mustapha), « La gestion conventionnelle des risques liés aux sols et sites pollués », *JCP N* 2014, n° 27.

MEKKI (Mustapha), « Les mystères de la blockchain », *D*. 2017, n° 37, pp. 2160 et s.

MEKKI (Mustapha), « Blockchain et métiers du droit en questions », *D. IP/IT* 2020, n° 2.

MEKKI (Mustapha), « Blockchain, entre mystères et fantasmes », *D. IP/IT* 2019, n° 7.

MEKKI (Mustapha), « Blockchain, smart contracts et notariat », *JCP N* 2018, n° 27-599, pp. 8-10.

MEKKI (Mustapha), « Le contrat, objet des smart contracts (Partie 1) », *D. IP/IT* 2018, n° 7.

MEKKI (Mustapha), « Le smart contract, objet du droit (Partie 2) », *D. IP/IT* 2019, n° 1.

MEKKI (Mustapha), « L'intelligence contractuelle et numérique au service de la responsabilité sociétale des entreprises », *AJ contrat* 2020, n° 3, pp. 112 et s.

MEKKI (Mustapha), DORAL (Sylvian), STREIFF (Vivien), BOYER (Sacha), *in* « Dossier : Blockchain et métiers du droit : une force vive ou subversive ? », *D. IP/IT* 2020, n° 2.

MIS (Jean-Michel), « Les technologies de rupture à l'aune du droit », *D. IP/IT* 2019, n° 7-8, p. 425.

MOREIL (Sophie), « Contrats - IA et contrats Optimiser les potentialités de l'IA »,*CDE* 2020, n° 3, dossier 13.

MORTON (Heather), « Blockchain State Legislation », *National Conference of State Legislatures* [online], 28 Mar. 2019, http://www.ncsl.org/research/financial-services-and-commerce/the-fundamentals-of-risk-management-and-insurance-viewed-through-the-lens-of-emerging-technology-webinar.aspx.

MOUNOUSSAMY (Ludovic), « Le smart contract, acte ou hack juridique ? », *LPA* 20 févr. 2020, n° 150t0, pp. 12 et s.

MOURON (Philippe), « Pour ou contre la patrimonialité des données personnelles », *Revue européenne des médias et du numérique* 2018, n° 46-47, pp. 90-96.

NAZAROV (Sergey), « The missing link between blockchains and Enterprises », *World Economic Forum*, 15 Dec. 2020.

NETTER (Emmanuel), « Règlement biométrie au travail », *D. IP/IT* 2019, n° 11.

NEVEJANS (Nathalie), « Le statut juridique du robot doit-il évoluer ? », *La Jaune et la Rouge* [en ligne], n° 750, déc. 2019, https://www.lajauneetlarouge.com/le-statut-juridique-du-robot-doit-il-evoluer/.

NOREAU (Pierre), « Belley Jean-Guy (dir.), Le droit soluble. Contributions québécoises à l'étude de l'internormativité, coll. Droit et Société, 1996 [compte-rendu] », *in* GUIBENTIF (Pierre), NIKLAS (Luhmann), « Dossier : L'emploi, l'entreprise : nouvelles normes, nouvelles règles », *Droit et société*, n° 41, 1999, pp. 171-172.

O'RORKE (William), « L'émergence d'un droit de la blockchain », *D. IP/IT* 2019, n° 7-8.

OST (François), VAN DE KERCHOVE (Michel), « De la pyramide au réseau ? Pour une théorie dialectique du droit », *RID comp*. 2003, n° 55-3, pp. 730-742.

PAVEL (Ilarion), « La blockchain – Les défis de son implémentation », *Annales des Mines - Réalités* industrielles 2017/3 (août 2017), pp. 20-24.

PEYRAT (Olivier), LEGENDRE (Jean-François), « Pourquoi la normalisation s'intéresse-t-elle à la blockchain ? », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), pp. 94-97.

PINTARIC (Pierre), « Sécuriser ses archives numériques », *Information, données & documents* 2017/3, vol. 54, pp. 40-41.

PONS (Jérôme), « La mise en œuvre de la blockchain et des smart contracts par les industries culturelles », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), pp. 81-90.

POPPE (Morgane), « Quelle relation entre la protection des données à caractère personnel et la blockchain ? *in* « Dossier : Blockchain, une révolution juridique ? », *RLDA* 2017/9, n° 129.

POULLET (Yves), « L'ODR au service de l'ADR : Quelques réflexions en marge du Colloque de Vienne : Kollektiver Rechtsschutz du 23 février 2005 », *CRID* [en ligne], févr. 2005, http://www.crid.be/pdf/public/5296.pdf.

POULLET (Yves), JACQUEMIN (Hervé), « Blockchain : une révolution pour le droit ? », *Journal des Tribunaux*, n° 6748, 10 nov. 2018, pp. 816 et s.

RABESANDRATANA (Vanessa), BACCA (Nicolas), « L'Oracle hardware : la couche de confiance entre les blockchains et le monde physique », *Annales des Mines - Réalités industrielles* 2017/3 (août 2017), pp. 91-93.

RESTREPO (David Amariles) *et al*., « Responsabilité sociale des entreprises. Enjeux globaux et technologiques », *Revue française de gestion* 2017/8, n° 269, pp. 161-182.

RODA (Jean-Christophe), « Smart contracts, dumb contracts ? », *D. IP/IT* 2018, n° 2.

ROTILY (Cassandra), ARCHAMBAULT (Laurent), « Drones civils professionnels et RGPD : enjeux liés à la collecte des données personnelles et au respect de la vie privée », *D. IP/IT* 2019, n° 6.

SPEARMAN (Kelli), « Protecting Blockchain Investments in a Patent Troll World », *Journal of Intellectual Property Law*, Vol. 6, Issue 1, Article 7, pp. 182-183.

STREIFF (Vivien), « Blockchain et propriété immobilière : une technologie qui prétend casser les codes », *Dr. & Patr.*, n° 262, oct. 2016, p. 25.

STREIFF (Vivien), « Blockchain et authenticité : pour copie non certifiée conforme », *D. IP/IT* 2020, n° 2.

TABAKA (Benoît), « L'archivage des contrats électroniques désormais opérationnels », *RLDI* 2005/3, nº 3.

TELLENNE (Cédric), « L'énergie, vecteur de développement et de puissance des États », *Géopolitique des énergies*, 2021, pp. 9-31.

THÉOCHARIDI (Eva), « La conclusion des smart contracts : révolution ou simple adaptation ? », *RLDA* 2018/6, n° 138.

VAN WAEYENBERGE (Arnaud), COLOMBANI (Lorenzo), « Responsabilité sociale des entreprises. Enjeux globaux et technologiques », *Revue française de gestion* 2017/8, n° 269.

VERBIEST (Thibault), « Blockchain : une révolution juridique ? », *RLDA* 2017/9, n° 129.

VERGÈS (Étienne) (dir.), « ETUDE : Les procédures amiables », *Encyclopédie Procédure civile*, Lexbase, 20 déc. 2018.

VINGIANO-VIRICEL (Iolande), « Quel usage de la donnée en assurance ? », *RGDA* sept. 2019, n° 116t7, p. 48.

WALTZ-TERACOL (Bélinda), « Blockchain et assurance : entre mythe et désillusion », *RGDA* nov. 2019, n° 116x8, p. 5.

WEINBAUM (Noémie), « La preuve du consentement à l'ère du RGPD et de la blockchain », *JCP E* 2018, n° 10, pp. 28-32.

ZOLINSKY (Célia), « Fintech - Blockchain et smart contracts : premiers regards sur une technologie disruptive », *RD bancaire et fin.* 2017, dossier 4, n° 8.

II. Sources non-juridiques

A. Ouvrages généraux

A. N. LEE (John), International Biographical Dictionary of Computer Pioneers, ed. Taylor & Francis, 1995.

ABITEBOUL (Serge), DOWEK (Gilles), Le temps des algorithmes, éd. Le Pommier, 2017.

ANTOINE (Charles), Introduction à la physique quantique, éd. Dunod, 2017.

ANTONOPOULOS (Andreas M.), Mastering Bitcoin, ed. O'Reilly, 2nd edition, 2017.

BACHOFEN (Blaise), BIZIOU (Michaël), BRAHAMI (Frédéric) et al., Le libéralisme au miroir du droit : l'État, la personne, la propriété, éd. ENS, 2008.

BARTHELEMY (Pierre), ROLLAND (Robert), VERON (Pascal), Cryptographie : principes et mises en œuvre. 2ème édition revue et augmentée, éd. Lavoisier, 2e édition (revue et augmentée), 2012.

BASHIR (Imran), Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained, ed. Packt Publishing Ltd, 2nd edition, 2018.

BENGHOZI (Pierre-Jean), BUREAU (Sylvain), MASSIT-FOLLEA (Françoise), L'Internet des objets – Quels enjeux pour l'Europe, éd. Éditions de la Maison des sciences de l'homme, coll. praTICs, 2012.

BLOCH (Laurent), Initiation à la programmation avec Scheme, éd. TECHNIP, 2011.

Blockchain France, La blockchain décryptée : Les clefs d'une révolution, éd. Netexplo, 2016.

BLOKDYK (Gerardus), Proof-of-stake: The One Essential Checklist, ed. CreateSpace Independent Publishing Platform, 2018.

BOS (Gerritt), BURNETT (Charles), Scientific weather forecasting in the middle ages: the writings of Al-Kindī: studies, editions, and translations, ed. Kegan Paul, 2000.

BOUJAT (Gérard), ANAYA (Patrick), Automatique industrielle en 20 fiches, éd. Dunod, 2013.

CHANG (Weng-Long), VASILAKOS (Athanasios V.), Molecular Computing: Towards a Novel Computing Architecture for Complex Problem Solving, ed. Springer, Vol. 4, coll. Studies in Big Data, 2014.

COLLIN (Denis), La fin du travail et la mondialisation. Idéologie et réalité sociale, éd. L'Harmattan, coll. « L'ouverture philosophique », 1997.

DE FILIPPI (Primavera), Blockchain et cryptomonnaies, éd. Presses Universitaires de France, coll. « Que sais-je ? », 2018.

DELAHAYE (Jean-Paul), Mathématiques et mystères, éd. Belin, coll. Pour la science, 2016.

EWALD (François), Histoire de l'État providence : Les origines de la solidarité, éd. Le livre de poche, coll. Biblio essais, 1996.

FOUQUE (Pierre-Alain), Cryptographie appliquée, éd. Techniques Ingénieur, 2002.

FRISBY (Dominic), Bitcoin: The Future of Money?, ed. Random House, 2014.

HAWKINS (Jeff), Intelligence, éd. Pearson Education France - CampusPress, 2005.

HERSANT (Olivier), L'Internet des objets : Les protocoles (KNX, ZigBee, 6LowPan...) et les principales applications M2M, éd. Dunod, coll. Automatiques et réseaux, 2014.

HOBBES OF MALMESBURY (Thomas), Leviathan or the Matter, Forme, & Power of a Common-wealth Ecclesiasticall and Civill, London. Printed for Andrew Crooke, 1651.

KELLY (Brian), The Bitcoin Big Bang: How Alternative Currencies are about to Change the World, ed. John Wiley & Sons, 2014.

LEE (David), CHUEN (Kuo), DENG (Robert H.), Handbook of Blockchain, Digital Finance, and Inclusion: vol. 2: ChinaTech, Mobile Security, and Distributed Ledger, ed. Academic Press, 2017.

LEE (John A. N.), International Biographical Dictionary of Computer Pioneers, ed. Taylor & Francis, 1995.

LEFEBURE (Antoine), L'affaire Snowden : Comment les États-Unis espionnent le monde, éd. La découverte, coll. Cahiers Libres, 2014.

LEHNING (Hervé), L'univers des codes secrets : De l'Antiquité à Internet, éd. Ixelles, 2012.

LELOUP (Laurent), Blockchain : la révolution de la confiance, éd. Eyrolles, 2017.

LILEN (Henri), Dictionnaire informatique numérique, éd. edi8, 2nd édition, 2014.

LOCQUENEUX (Cédric), DARRIEUMERLOU (Serge), Le guide de la maison et des objets connectés : Domotique, smart home et maison connectée, éd. Eyrolles, 2016.

LOIGNON (Stéphane), Big Bang Blockchain. La seconde révolution d'internet, éd. Tallandier, 2017.

MACKINNON (Rebecca), Consent of the Networked: The Worldwide Struggle for Internet Freedom, ed. Basic Books, 2012.

MANGEMATIN (Vincent), Des mondes de confiance : Un concept à l'épreuve de la réalité sociale, CNRS Éditions via OpenEdition, 2016.

MUKHI (Vijay), The Undocumented Internals of the Bitcoin Ethereum and Blockchains, ed. BPB Publications, 2018.

MUKHOPADHYAY (Mayukh), Ethereum Smart Contract Development: Build blockchain-based decentralized applications using solidity, ed. Packt Publishing Ltd, 2018.

ORDONNEAU (Pascal), Monnaies cryptées et blockchain : La confiance est-elle un algorithme ?, éd. Arnaud Franel, 2017.

PARET (Dominique), Objets communicants sécurisés : Applications, conceptions et concrétisation, éd. ISTE Group, 2017.

POULON (Frédéric), Économie générale, éd. Dunod, coll. Manuel, 8e édition, 2015.

RATTO (Stefania), Greece: Volume 3 de Dictionaries of civilization Dizionari delle civiltà, ed. University of California Press, Vol. 3, 2008.

RIFKIN (Jeremy), La troisième révolution industrielle - Comment le pouvoir latéral va transformer l'énergie, l'économie et le monde, éd. Les liens qui libèrent, 2012.

ROCHAIN (Serge), De la mécanographie à l'informatique : 50 ans d'évolution – Histoire des sciences et des techniques : Software, environnements and tools, éd. ISTE, 2016.

RODRIGUEZ (Philippe), La révolution blockchain : Algorithmes ou institutions, à qui donnerez-vous votre confiance ?, éd. Dunod, 2017.

SCHWAB (Klaus), La quatrième révolution industrielle, éd. Dunod, 2017.

SHASHA (Dennis) et LAZERE (Cathy), Quand la vie remplace le silicium : Aux frontières de la bio-informatique, éd. Dunod, coll. Quai des sciences, 2011.

SMYRNAIOS (Nikos), Les GAFAM contre l'internet, éd. Ina, 2017.

TAZDAIT (Tarik), L'Analyse Économique de la Confiance, éd. De Boeck Université, coll. Ouvertures Économiques, 2008.

TEQUI (Clément), HIAULT (François), DELLA CHIESA (Martin), Blockchain : Vers de nouvelles chaines de valeur, éd. Eyrolles, 2019.

VIAUD (Gaston), L'Intelligence, éd. Presses Universitaires de France, 1969.

WINZER (Kristina), "Chain Code". Smart Contracts demonstriert an einfachen Code-Beispielen, ed. GRIN Verlag, 2018.

YERETZIAN (Antoine) (dir.), La blockchain décryptée : les clefs d'une révolution, éd. Netexplo, 2016.

ZENNER (Alain), Le Dictionnaire ludique & érudit du Confinement, Éditions Luc Pire, 2020.

B. Articles

ANDONIA (Merlinda), ROBUA (Valentin), FLYNNA (David) *et al.*, « Blockchain technology in the energy sector: A systematic review of challenges and opportunities », *in* FOLEY (Aoife M.) (dir.), *Renewable and Sustainable Energy Reviews*, ed. Elsevier, Vol. 100, Feb. 2019, pp. 143-174.

BIRYUKOV (Alex), KHOVRATOVICH (Dmitry), PUSTOGAROV (Ivan), « Deanonymisation of clients in Bitcoin P2P network », *arXiv* [online], 28 May 2014, https://arxiv.org/pdf/1405.7418v1.pdf.

BIRYUKOV (Alex), KHOVRATOVICH (Dmitry), PUSTOGAROV (Ivan), « Deanonymisation of Clients in Bitcoin P2P Network », *arXiv.org* [online], 5 Jul. 2014, https://arxiv.org/abs/1405.7418.

BUTERIN (Vitalik), « CRITICAL UPDATE Re: DAO Vulnerability », *Ethereum Blog* [online], 17 Jun. 2016, https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/.

BUTERIN (Vitalik), « Ethereum and Oracles », *Ethereum Blog* [online], 22 Jul. 2014, https://blog.ethereum.org/2014/07/22/ethereum-and-oracles/.

BUTERIN (Vitalik), « White Paper Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform », *github* [liens de publication originaux supprimés] [online], Nov. 2013, https://github.com/ethereum/wiki/wiki/White-Paper.

CHEVANCE (René J.), « Serveurs multiprocesseurs et SGBD parallélisés », *Techniques Ingénieur* [en ligne], n° H2068 v1, 2000, https://www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9/bases-de-donnees-42309210/serveurs-multiprocesseurs-et-sgbd-parallelises-h2068/.

CLACK (Christopher D.), BAKSHI (Vikram A.), BRAINE (Lee), « Smart Contract Templates: foundations, design landscape and research directions », *Arxiv* [online], 4 Aug. 2016 (update 15 Mar. 2017), p. 3, https://arxiv.org/pdf/1608.00771.pdf.

COMTE (Jacqueline), « Stigmatisation du travail du sexe et identité des travailleurs et travailleuses du sexe », *Déviance et Société*, 2010/3 (vol. 34), pp. 425-446.

DAI (Wei), « b-money, an anonymous, distributed electronic cash system », [online], 1998, http://www.weidai.com/bmoney.txt.

DE KRUIJFF (Tilburg), WEIGNAND (Hans), « Ontologies for Commitment-Based Smart Contracts », *in* PANETTO (Hervé), DEBRUYNE (Christophe), GAALOUL (Walid) *et al*., *On the Move to Meaningful Internet Systems. OTM 2017 Conferences: Confederated International Conferences: CoopIS, C&TC, and ODBASE 2017, Rhodes, Greece, 23-27 October 2017, Proceedings, Partie 2 : Vol. 10574 de Lecture Notes in Computer Science*, ed. Springer, 2017.

DELAHAYE (Jean-Paul), « Déléguer un calcul sans divulguer ses données », *Pour la Science*, n° 456, oct. 2015.

DELAHAYE (Jean-Paul), « Les débats sur l'intelligence artificielle », *SPS* juill. 2015, n° 313.

DELAHAYE (Jean-Paul), « Les blockchains, clefs d'un nouveau monde », *Pour la Science*, n°449, mars 2015.

DELAHAYE (Jean-Paul), « Qu'est-ce qu'une blockchain ? », *Pour la Science*, 11 oct. 2017.

DELAHAYE (Jean-Paul), « Viète, inventeur de la cryptanalyse mathématique », *Pour la Science*, n° 313, nov. 2003, pp. 90-95.

DENIS (Jérôme), « L'informatique et sa sécurité. Le souci de la fragilité technique », *Réseaux*, vol. 171, n° 1, 2012, pp. 170 et s.

EL FIDHA (Chokri), HÉDI CHARKI (Mohamed), « Le rôle des technologies de l'information et de la communication dans le développement de la qualité de la "relation client". Application à la relation banque/entreprise », *La Revue des Sciences de Gestion* 2008/1, n° 229, pp. 121-127.

GATTY (Jean), « Sur Milton Friedman et son économie de la liberté », *Commentaire* 1996/3, n° 75, pp. 717-724.

GERSHENFELD (Neil), KRIKORIAN (Raffi), COHEN (Danny), « The Internet of Things: The principles that gave rise to the Internet are now leading to a new kind of

network of everyday devices, an "Internet-0" », *Scientific American* [online], Oct. 2014, https://www.scientificamerican.com/article/the-internet-of-things/.

GIRAUD (Thomas), « Vie culturelle - La *blockchain* est-elle l'avenir de la culture ? », *Vie culturelle JAC*, 2017, n° 51, p. 35.

HARRY (Guillaume), « Failles de sécurité des applications Web », *CNRS* [en ligne], 2012, https://hal.archives-ouvertes.fr/hal-00736013/document.

IBANDA KABAKA (Paulin), « L'intervention de l'État dans l'économie : du laisser-faire à la régulation », *HAL* [en ligne], <hal-01287474>, 13 mars 2016, https://hal.archives-ouvertes.fr/hal-01287474/document.

KEEGAN (Ryan), « Return of the Hidden Number Problem », *NCC Group Whitepaper* [online], 13 Jun. 2018, p. 12, https://medium.com/r/?url=https%3A%2F%2Fwww.nccgroup.trust%2Fglobalassets%2Four-research%2Fus%2Fwhitepapers%2F2018%2Frohnp-return-of-the-hidden-number-problem.pdf.

LACITY (Mary), VAN HOEK (Remko), « How the Pandemic Is Pushing Blockchain Forward », *Harvard Business Review* [online], 27 Apr. 2020, https://hbr.org/2020/04/how-the-pandemic-is-pushing-blockchain-forward.

LAMONTAGNE (Denys), « Blockchain en éducation : la gestion infalsifiable de la confiance – Certification, accès, authentification, découvrez les possibilités du blockchain », *Thot Cursus* [en ligne], 26 nov. 2015 (dernière mise à jour le 20 janv. 2016), https://cursus.edu/articles/34938#.W1rbxNUzbIU.

LAMPORT (Leslie), SHOSTAK (Robert), PEASE (Marshall), « The Byzantine Generals Problem », *ACM Transactions on Programming Languages and Systems* 1982, Vol. 4, No. 3.

LENHING (Hervé), « Jefferson et les mathématiques », *in* COHEN (Gilles) (dir.), *Mathématiques et politique*, Éditions Pôle Paris, coll. Bibliothèque Tangente, n°45, 2012.

LESSIG (Lawrence), « Code Is Law: On Liberty in Cyberspace », *Harvard Magazine* [online], 1st Jan. 2000, https://www.harvardmagazine.com/2000/01/code-is-law-html.

MAURER (Bill), « Blockchains Are a Diamond's Best Friend: Zelizer for the Bitcoin Moment », *in* BANDELJ (Nina), WHERRY (Frederick F.), ZELIZER (Viviana A.), *Money Talks: Explaining How Money Really Works*, ed. Princeton University Press, 2017, p. 215-229.

MAY (Timothy C.), « The Crypto Anarchist Manifesto », Activism.net [online], 22 Nov. 1992, https://www.activism.net/cypherpunk/crypto-anarchy.html.

MEIKLEJOHN (Sarah), POMAROLE (Marjori), JORDAN (Grant), LEVCHENKO (Kirill) *et al.*, « A fistful of bitcoins: Characterizing payments among men with no names », *in* LUCKIE (Matthew J.), BEVERLY (Robert), BRINKMEYER (William), CLAFFY (Kc Claire), *IMC'13: Proceedings of the 2013 Conference on Internet Measurement Conference*, ed. ACM, 2013, pp. 127-140.

NAKAMOTO (Satoshi), « Bitcoin: A Peer-to-Peer Electronic Cash System », [online], Oct. 2008, https://bitcoin.org/bitcoin.pdf.

PANZA (Marco), « François Viète, between analysis and cryptanalysis », *Studies in History and Philosophy of Sciences*, Vol. 37, Issue 2, Jun. 2006, pp. 269-289.

PRIVAT (Gilles), « Des objets communicants à la communication ambiante », *Les Cahiers du numérique*, 2002/4, vol. 3, pp. 23-44.

REID (Fergal), HARRIGAN (Martin), « An analysis of anonymity in the bitcoin system », *in* ALTSHULER (Yaniv), ELOVICI (Yuval), CREMERS (Armin B.), AHARONY (Nadav) *et al.*, *Security and Privacy in Social Networks*, ed. Springer, 2013, pp. 197-223.

RENARD (Isabelle), « E-commerce : Une bonne et une mauvaise nouvelle pour la signature électronique des contrats B to C », *Expertises*, mars 2013, n° 378.

RON (Dorit), SHAMIR (Adi), « *Quantitative analysis of the full bitcoin transaction graph* », *in* BÖHME (Rainer), BRENNER (Michael), MOORE (Tyler), SMITH (Matthew), *Financial Cryptography and Data Security*, ed. Springer, 2014, pp. 6-24.

ROUSSEAU (Denise M.), SITKIN (Sim B.), BURT (Ronald S.), CAMERER (Colin), « Not So Different After All: A Cross-Discipline View of Trust », *Academy of Management Review* 1998, Vol. 23, No. 3.

SAGNES (Nicolas), « Économie mondiale – 2008 : De la crise financière à la crise économique », *Encyclopaedia Universalis* [en ligne], 2008, https://www.universalis.fr/encyclopedie/economie-mondiale-2008-de-la-crise-financiere-a-la-crise-economique/.

SUSSMAN (Gerald Jay), STEELE, JR. (Guy L.), « The First Report on Scheme Revisited », Higher-Order and Symbolic Computation, Vol. 11, No. 4, 1st Dec. 1998.

SYLVESTRE (Guillaume), « Les types de failles et de risques sécurité », *I2D - Information, données & documents*, vol. 54, n° 3, 2017, pp. 30 et s.

SZABO (Nick), « Formalizing and Securing Relationships on Public Networks », [online], 1st Sept. 1997, http://firstmonday.org/ojs/index.php/fm/article/view/548/469.

SZABO (Nick), « Smart Contracts: Building Blocks for Digital Markets » [extract], Extropy #16 [online], 1996, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

VELDE (François R.), « Bitcoin pour remplacer les devises », *Rev. éco. fin*. 2016, 2015/4, n° 120.

VESSENES (Peter), « More Ethereum Attacks: Race-To-Empty is the Real Deal », *Vessenes* [online], 9 Jun. 2016, https://vessenes.com/more-ethereum-attacks-race-to-empty-is-the-real-deal.

ZHANG (Ying), « Technology framework of the Internet of Things and its application », *in 2011 International Conference on Electrical and Control Engineering*, IEEE, Yichang, 16-18 Sept. 2011, pp. 4109-4112.

C. Ressources numériques

BERTANI (Thomas), « Understanding oracles », *Oraclize* [online], 18 Feb. 2016, https://blog.
oraclize.it/understanding-oracles-99055c9c9f7b.

DAIAN (Philip), « Chasing TheDAO Attacker's Wake », *Phil Does Security* [online], 19 Jun. 2016, http://pdaian.com/blog/chasing-the-dao-attackers-wake/

DE CHARENTENAY (Simon), « Blockchain et Droit : Code is deeply Law », *Blockchain France* [en ligne], 19 sept. 2017, https://blockchainfrance.net/2017/09/19/blockchain-et-droit/.

DE QUENETAIN (Stanislas), « 4 étapes pour comprendre une transaction bitcoin », *Blockchains Experts* [en ligne], 2017, https://www.blockchains-expert.com/4-etapes-pour-comprendre-une-transaction-bitcoin/.

DE QUENETAIN (Stanislas), « L'arbre de Merkle : la Colonne Vertébrale de la Blockchain », *Blockchains Experts* [en ligne], 2015, https://www.blockchains-expert.com/larbre-de-merkle-colonne-vertebrale-de-blockchain/.

FERRON (Antoine), SAUZADE (Adrien), « Blockchain », *Institut des actuaires* [en ligne], 15 mars 2017, p. 34, https://www.institutdesactuaires.com/global/gene/link.php?doc_id
=9971&fg=1.

FRASER (Heather), « How Blockchains Can Provide New Benefits for Healthcare », *IBM* [online], 20 Feb. 2017, https://www.ibm.com/blogs/think/2017/02/blockchain-healthcare/.

GALEON (Dom), HOUSER (Kristen), « IBM Just Launched Blockchain Beyond Currency », *Futurism* [online], 22 Mar. 2017, https://futurism.com/ibm-just-launched-blockchain-beyond-currency/.

HALDER (Steve), « September 2019 Healthcare Data Breach Report », *HIPAA Journal* [online], 21 Oct. 2019, https://www.hipaajournal.com, Home > Healthcare Cybersecurity > September 2019 Healthcare Data Breach Report.

HINKES (Andrew), « Blockchains, smart contracts, and the death of specific performance », *Inside Consel* [online], 29 Jul. 2014, http://web3.insidecounsel.com/2014/07/29/blockchains-smart-contracts-and-the-death-of-speci?slreturn=1532806704.

HONIGMAN (Philippe), « Qu'est-ce qu'une DAO ? », *Ethereum France* [en ligne], 9 juill. 2019, https://www.ethereum-france.com/quest-ce-quune-dao/.

IBNOUHSEIN (Issam), « Programmation des blockchains et "smart contracts" », *Quantmetry* [en ligne], 31 mai 2016, https://www.quantmetry.com/single-post/2017/05/31/Programmation-des-blockchains-et-%E2%80%9Csmart-contracts%E2%80%9D.

LEFEVRE (Thierry), « Une très brève histoire de la technologie humaine », *Planète viable* [en ligne], 17 avr. 2017, http://planeteviable.org/histoire-technologie-humaine/.

LEHNING (Hervé), « Cryptologie et espionnage : comment a-t-on décrypté le télégramme Zimmermann ? », *Futura Sciences* [en ligne], 2017, https://www.futura-sciences.com/sciences/questions-reponses/mathematiques-cryptologie-espionnage-t-on-decrypte-telegramme-zimmermann-8082/.

LEHNING (Hervé), « Quels étaient les codes secrets de la première guerre mondiale ? », *Futura Sciences* [en ligne], 2017, https://www.futura-sciences.com/sciences/questions-reponses/mathematiques-etaient-codes-secrets-premiere-guerre-mondiale-8067/.

MARIN-DAGANNAUD (Gautier), « Comprendre la blockchain Ethereum – Article 1 : Bitcoin, première implémentation de la blockchain (1/2) », *Ethereum France* [en ligne], 3 juin 2016, https://www.ethereum-france.com/comprendre-la-blockchain-ethereum-article-1-bitcoin-première-implementation-de-la-blockchain-12/.

MARIN-DAGANNAUD (Gautier), « Comprendre la blockchain Ethereum – Article 1 : Bitcoin, première implémentation de la blockchain (2/2) », *Ethereum France* [en ligne], 30 mai 2017, https://www.ethereum-france.com/comprendre-la-blockchain-ethereum-article-1-bitcoin-premiere-implementation-de-la-blockchain-22/.

POLROT (Simon), « Comment obtenir des ether (ETH) ? », *Ethereum France* [en ligne], 12 fév. 2016, https://www.ethereum-france.com/obtenir-des-ether-eth/.

POLROT (Simon), « Déploiement de The DAO, "mère de toutes les DAO" », *Ethereum France* [en ligne], 30 avr. 2016, https://www.ethereum-france.com/deploiement-du-projet-the-dao-mere-de-toutes-les-dao/.

POLROT (Simon), « Hard fork ou non : faites entendre votre voix ! », *Ethereum France* [en ligne], 11 juill. 2016, https://www.ethereum-france.com/hard fork-ou-non-faites-entendre-votre-voix/.

POLROT (Simon), « Le Hard Fork "The DAO" aura bien lieu, mode d'emploi », *Ethereum France* [en ligne], 19 juil. 2016, https://www.ethereum-france.com/le-hard fork-the-dao-aura-bien-lieu-mode-demploi/.

POLROT (Simon), « Les Oracles, lien entre la blockchain et le monde », *Ethereum France* [en ligne], 13 sept. 2016, https://www.ethereum-france.com/les-oracles-lien-entre-la-blockchain-et-le-monde/.

POLROT (Simon), « Qu'est-ce qu'Ethereum ? », *Ethereum France* [en ligne], 14 fév. 2016, https://www.ethereum-france.com/quest-ce-que-lethereum/.

POLROT (Simon), « TheDAO : post mortem », *Ethereum France* [en ligne], 24 janv. 2017, https://www.ethereum-france.com/the-dao-post-mortem/.

POLROT (Simon), « To fork or not to fork, telle est la question ! », *Ethereum France* [en ligne], 27 juin 2017, https://www.ethereum-france.com/to-fork-or-not-to-fork-telle-est-la-question/.

SHARMA (Udit), « Blockchain in healthcare: Patient benefits and more », IBM [online], 30 Oct. 2017, https://www.ibm.com/blogs/blockchain/2017/10/blockchain-in-healthcare-patient-benefits-and-more/.

TYCHEY (Jde), « uPort ou la gestion de l'identité par la blockchain », *Ethereum France* [en ligne], 27 sept. 2016 (mis à jour : 30 mai 2017), https://www.ethereum-france.com/uport-ou-la-gestion-de-lidentite-par-la-blockchain/.

VERLETTE (Nicolas), « Bitcoin : Qu'est-ce qu'une adresse multi-signatures ? », *Achat-Bitcoins* [en ligne], 18 mai 2014, https://achat-bitcoins.com/bitcoin-definition-multi-signatures/.

III. Colloques

DE COETLOGON (Perrine) (dir.), « Réunion d'information #GTnum #Blockchain4E », Villeneuve d'Ascq (Laboratoire Cristal, M3, Cité scientifique), 26 juin 2018, non publié.

MÉNIÈRE (Yann), « The emerging blockchain patent landscape », *in* EPO Conference, « Patenting Blockchain », The Hague, 4 Dec. 2018, non publié [en ligne], https://www.epo.org/news-events/news/2019/20190314.html.

NEVEJANS (Nathalie), « Une introduction juridique à l'Objet Intelligent », communication au colloque « L'objet intelligent : normes, usages et responsabilités » de l'Institut d'électronique et des Systèmes (Université de Montpellier R 5214) et l'Unité Dynamiques du droit (Université de Montpellier R 5815) – Centre National de la Recherche Scientifique, Montpellier, Université de Montpellier, non publié, 6 nov. 2015.

ORISINI (Lawrence), « Transactive Grid: A Decentralized Energy Management Solution », *in* Fondation Ethereum, *Devcon1 Ethereum*, Developers Conference, London, Nov. 13, 2015, non-published [en ligne], https://www.youtube.com/watch?v=kq8RPbFz5UU.

ROLLAND (Maël), « Les crypto-monnaies à l'aune des monnaies parallèles, sociales et complémentaires : continuité et rupture dans le champ de la gouvernance monétaire », *in* MARTÍ (José) (dir.), *Conferencia Internacional Por El Equilibrio Del Mundo*, Cuba, 10-14 de mayo de 2017, inedito [en línea], https://www.swisscurrencyconfederation.ch/wp-content/uploads/2018/04/Rolland-M.-Les-crypto-monnaies-%C3%A0-laune-des-monnaies-sociales-et-compl%C3%A9mentaires-continuit%C3%A9-et-rupture-dans-le-champs-de-la-r%C3%A9appropriation-mon%C3%A9taire.pdf.

WÜST (Karl), GERVAIS (Arthur), « Do you need à blockchain ? », *in* 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, 20-22 Jun. 2018, *IEEE* [online], 8 Nov. 2018, https://eprint.iacr.org/2017/375.pdf.

IV. Références web

« Blockchain, catalyseur de nouvelles approches en assurance. Volume 2 : Quelles mises sur le marché concrètes et quelles évolutions pour 2019 ? », PwC [en ligne], 2018, https://www.pwc.fr/fr/assets/files/pdf/2018/09/pwc-blockchain-3-catalyseur-de-nouvelles-approches-en-assurance-2018.pdf.

« Device democracy Saving the future of the Internet of Things », IBM [online], Jul. 2015, https://www-935.ibm.com/services/multimedia/GBE03620USEN.pdf.

« Electric Vehicle Charging for Local Governments », Everty Pty Ltd [online], Aug. 2018, https://citiespowerpartnership.org.au/wp-content/uploads/2018/10/Everty-Council-Document-FINAL-CONTENT-1.pdf.

« Éthique de la recherche en robotique. Rapport n° 1 de la CERNA, Commission de réflexion sur l'Éthique de la Recherche en sciences et technologies du Numérique d'Allistene », CERNA [en ligne], nov. 2014, http://cerna-ethics-allistene.org/digitalAssets/38/38704_Avis_robotique_
livret.pdf.

« FNUF-14: Coup d'envoi de la première session technique du Forum des Nations Unies sur les forêts pour évaluer la mise en œuvre du Plan stratégique 2017-2030 », *Nations Unies* [en ligne], 6 mai 2019, Conseil Économique et Social > Forum des Nations Unies sur les Forêts > Quatorzième Session, 2e Et 3e Séances – Matin & Après-Midi, https://www.un.org/press/fr/
2019/envdev1944.doc.htm.

« La signature électronique : Note de synthèse », *Sénat* [en ligne], 4 nov. 2019, https://www.senat.fr/lc/lc67/lc67_mono.html.

« Le développement industriel futur de la robotique personnelle et de service en France », Ministère de l'économie [en ligne], avr. 2012, https://www.entreprises.gouv.fr/files/files/en-pratique/etudes-et-statistiques/dossiers-de-la-DGE/robotique.pdf.

« Présentation de la BlockChain Notariale. Dossier de Presse », Notaires du Grand Paris [en ligne], 7 juill. 2020, https://notairesdugrandparis.fr/sites/default/files/2020-07-07%20-%20DP%20-
20Pr%C3%A9sentation%20de%20la%20Blockchain%20Notariale%20VF2.pdf.

« Research Announcement: Moody's – Blockchain standardisation will amplify benefits for securitisations », *Moody's* [online], 5 Sept. 2019, https://www.moodys.com/research/Moodys-Blockchain-standardisation-will-amplify-benefits-for-securitisations--PBS_1193318?WT.mc_
id=AM%7ERmluYW56ZW4ubmV0X1JTQl9SYXRpbmdzX05ld3NfTm9fVHJhbnNYXRpb25z%7E20190905_PBS_1193318.

« Science and Technology Briefings – no. 4 – Understanding blockchains », Sénat [en ligne], Apr. 2018, https://www.senat.fr/fileadmin/Fichiers/Images/opecst/quatre_pages_anglais/
OPECST_2018_0038_understanding_blockchains_briefing.pdf.

« Sécurité numérique et risques : enjeux et chances pour les entreprises », *Sénat* [en ligne], 2 févr. 2015, https://www.senat.fr/rap/r14-271-1/r14-271-143.html.

« TLSnotary - a mechanism for independently audited https sessions », TLSnotary [online], White Paper, 10 Sept. 2014, https://tlsnotary.org/TLSNotary.pdf.

ACPR, « Identification et connaissance de la clientèle (KYC) », *ACPR-Banque de France* [en ligne], 12 juin 2018, https://acpr.banque-france.fr/autoriser/fintech-et-innovation/nos-dossiers-thematiques/identification-et-connaissance-de-la-clientele-kyc.

ADAM-KALFON (Pauline), DUBREUIL (Emmanuel), RICHARD (Marie-Line), « Blockchain, catalyseur de nouvelles approches en assurance », PwC [en ligne], mars 2017, https://www.pwc.fr/fr/assets/files/pdf/2017/03/blockchain-et-assurance/etude-blockchain-catalyseur-de-nouvelles-approches-en-assurance.pdf.

Autorité de Régulation des Communications Électroniques et des Postes (ARCEP), « Le "bac à sable" réglementaire », *arcep.fr* [en ligne], 18 avr. 2018, https://www.arcep.fr/index.php?id=13816.

Banque de France, « Focus n°10 : Les dangers liés au développement des monnaies virtuelles : l'exemple du bitcoin », Banque de France [en ligne], 5 déc. 2013, https://publications.banque-france.fr/sites/default/files/medias/documents/focus-10_2013-12-05_fr.pdf.

BAYLE (Aurélie) *et al.*, « Smart contracts : études de cas et réflexions juridiques », ECAN [en ligne], 19 sept. 2017, https://ecan.fr/Smart-Contracts-Etudes.pdf.

Bercy Infos, « Crypto-monnaies, crypto-actifs... Comment s'y retrouver ? », *economie.gouv.fr* [en ligne], 4 juill. 2018, https://www.economie.gouv.fr/particuliers/cryptomonnaies-cryptoactifs.

BYUNGKWON (Lim), LOW (Charles), « Thinking Inside the Box: The UK FCA Sandbox, a Playground for Innovation », Debevoise In Depth [online], 6 Mar. 2018, https://www.debevoise.com/~/media/files/insights/publications/2018/03/20180306_thinking_inside_the_box_client_update.pdf.

Chamber of Digital Commerce of NYC & Deloitte, « Smart Contracts: 12 Use Cases for Business & Beyond », [online], 6 Dec. 2016, https://digitalchamber.org/policy-positions/smart-contracts/.

CNIL, « Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data », *CNIL* [online], 6 Nov. 2018, https://www.cnil.fr/en/blockchain-and-gdpr-solutionsresponsible-use-blockchain-context-personal-data.

CNIL, « Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles ? », *CNIL* [en ligne], 24 sept. 2018, https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles.

CNIL, « Blockchain : Premiers éléments d'analyse de la CNIL », CNIL [en ligne], sept. 2018, https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf.

CNIL, « Drones et vie privée : un cadre à inventer, Rapport annuel d'activité », *CNIL* [en ligne], 2014, https://bit.ly/2KlvLCy.

CNIL, *Rapport d'activité de 2015*, éd. La Documentation Française [en ligne], 2016, https://www.cnil.fr/sites/default/files/atoms/files/cnil-36e_rapport_annuel_2015_0.pdf.

Commission des affaires économiques et monétaires, « Rapport sur les monnaies virtuelles » n° 2016/2007(INI), *European Parliament* [en ligne], 3 mai 2016, https://www.europarl.europa.eu/doceo/document/A-8-2016-0168_FR.html.

Congress of the United States House of Representatives (Committee on Energy and Commerce), *Committee on Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection – Hearing Notice*, CEC [online], 1st Jun. 2017, https://energycommerce.house.gov/news/press-release/subdccp-discusses-how-fintech-improves-consumers-financial-options/.

Conseil d'État, « Puissance publique et plateformes numériques : accompagner l'ubérisation – Étude annuelle 2017 », éd. Documentation française [en ligne], n° 68, sept. 2017, http://www.vie-publique.fr/actualite/dossier/conseil-etat/puissance-publique-plateformes-numeriques-accompagner-uberisation.html.

Conseil Supérieur du Notariat, « Règlement national », Approuvé par arrêté de Madame la Garde des Sceaux, Ministre de la justice en date du 22 juillet 2014, JO du 1er août 2014 [en ligne], p. 5, https://www.notaires.fr/sites/default/files/reglement_national_-_reglement_
intercours_-_arrete_du_22_07_2014_-_jo_du_01_08_2014.pdf.

CRE, « Dossier : Les objets connectés », *Smart Grids* [en ligne], 6 mars 2017, http://www.smartgrids-cre.fr/index.php?p=objets-connectes-introduction.

CSA ACVM, « The Canadian Securities Administrators Launches a Regulatory Sandbox Initiative », *Ontario Securities Commission* [online], 23 Feb. 2017, https://nssc.novascotia.ca/
sites/default/files/docs/Feb.%2023,%202017%20CSA%20RegSandbox-press%20release.

Direction de l'information légale et administrative, « L'Histoire de la fonction publique », *Vie publique* [en ligne], 12 oct. 2012, http://www.vie-publique.fr/decouverte-institutions/institutions/approfondissements/histoire-fonction-publique.html.

Direction Générale des Politiques Internes du Parlement Européen, PE 571.379, étude sur les règles européennes de droit civil en robotique, Département thématique C : droits des citoyens et affaires constitutionnelles, affaires juridiques [en ligne], oct. 2016, p. 16, https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_FR.pdf

Direction générale du marché intérieur, de l'industrie, de l'entrepreneuriat et des PME (Commission européenne), « Le financement participatif expliqué. Un guide pour les petites et moyennes entreprises », *Office des publications de l'Union Européenne* [en ligne], 4 juin 2017, https://op.europa.eu/fr/publication-detail/-/publication/d5e626ba-d7c8-11e6-ad7c-01aa75ed71a1.

Direction Générale du Trésor, « Consultation publique sur le projet de réformes législative et réglementaire relatif à la Blockchain », *Ministère des économies, des finances et de la relance* [en ligne], 24 mars 2017, https://www.tresor.economie.gouv.fr/Ressources/File/434688.

Direction Générale du Trésor, « Modernisation du régime des bons de caisse », *Ministère des économies, des finances et de la relance* [en ligne], 27 mai 2015, https://www.tresor.economie.gouv.fr/Ressources/13778_modernisation-du-regime-des-bons-de-caisse.

European Parliamentary Research Service, « Blockchain and the General Data Protection Regulation Can distributed ledgers be squared with European data protection law? », European Parliament [online], Panel for the Future of Science and Technology, Jul. 2019, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

European Parliamentary Research Service, « Blockchain and the General Data Protection Regulation Can distributed ledgers be squared with European data protection law? »,

European Parliament [online], Panel for the Future of Science and Technology, Jul. 2019, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

FIGUEIREDO DO NASCIMENTO (Susana), ROQUE MENDES POLVORA (Alexandre), ANDERBERG (Amanda) *et al.*, « Blockchain Now and Tomorrow », Publications Office of the European Union [online], 2019, http://publications.jrc.ec.europa.eu/repository/bitstream/JRC117255/blockchain_online.pdf.

FINCK (Michèle), « Blockchain and the General Data Protection Regulation Can distributed ledgers be squared with European data protection law? » *in* Panel for the Future of Science and Technology (STOA), European Parliament Research Service (EPRS) [online], Jul. 2019, http://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2019)634445.

Forum Fintech ACPR-AMF, « Pôle Fintech-Innovation : publication du rapport du groupe de travail sur la vérification d'identité à distance des personnes physiques », ACPR [en ligne], 20 sept. 2019, https://acpr.banque-france.fr/sites/default/files/medias/documents/20190919_synthese_verification_identite_distance_personnes_physiques.pdf.

France stratégie, *Les enjeux des blockchains*, [en ligne], 21 juin 2018, https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-rapport-blockchain-21-juin-2018.pdf.

G20 Financial Inclusion Action Plan, « G20 Principles for Innovative Financial Inclusion - Executive Brief », GPFI [online], 2010, http://www.gpfi.org/sites/default/files/documents/G20%20Principles%20for%20Innovative%20Financial%20Inclusion%20-%20AFI%20brochure.pdf.

Gibraltar Financial Services Commission, *Regulating Fintech: Proposals for a distributed ledger technology regulatory framework*, [online], 9 May 2017, www.fsc.gi/news/regulating-fintech-proposals-for-a-distributed-ledger-technology-dlt-regulatory-framework-235.

Groupe FinTech, « Les impacts des réseaux distribués et de la technologie blockchain dans les activités de marché », *Paris Europlace* [en ligne], 23 oct. 2017, https://www.paris-europlace.com/fr/file/2867/download?token=h3_Q1t6V.

KEMP (Leanne), « Blockchain applications in assurance », Deloitte LPP [online], 2016, https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-deloitte-blockchain-app-in-insurance.pdf.

MARC (François), « Comptes rendus de la commission des finances : Enjeux liés au développement des monnaies virtuelles de type bitcoin – Table ronde », *Sénat* [en ligne], 15 janv. 2014, http://www.senat.fr/compte-rendu-commissions/20140113/fin.html#toc3.

MASON (Stephen), *L'utilisation des preuves électroniques dans les procédures civiles et administratives et son impact sur les règles et modes de preuves. Étude comparative et analyse, rapport préparé par Stephen Mason, avec le concours de Uwe Rasmussen*, Strasbourg, 27 juill. 2016, CDCJ(2015)14-final [en ligne], https://rm.coe.int/16807007ca.

MAUBANT (Thierry), « UE : nouvelles mesures pour accélérer la numérisation des systèmes judiciaires et la formation des professionnels », *ActuIA* [en ligne], 3 déc. 2020, https://www.actuia.com/actualite/ue-nouvelles-mesures-pour-accelerer-la-numerisation-des-systemes-judiciaires-et-la-formation-des-professionnels/?u%E2%80%A6.

Mersenne Research Inc., « GIMPS Project Discovers Largest Known Prime Number: 277 232 917-1 », *GIMPS* [online], 3 Jan. 2018, https://www.mersenne.org/primes/?press=M77232917.

Ministère de la Justice et des Libertés, « Les officiers ministériels », [en ligne], juin 2010, Secrétariat général > Service de l'administration centrale > Département des archives, de la documentation et du patrimoine, http://www.archives-judiciaires.justice.gouv.fr/index.php?article=14875&rubrique=10774&ssrubrique=10827.

Notaires de France, « Le rôle du notaire et ses principaux domaines d'intervention », *notaires.fr* [en ligne], 2 avr. 2013, https://www.notaires.fr/fr/profession-notaire/r%C3%B4le-du-notaire-et-ses-principaux-domaines-dintervention/le-r%C3%B4le-du-notaire.

Notaires de France, « Propriété immobilière : entre progrès et confiance », Compte-rendu des travaux du 112e Congrès des notaires de France [en ligne], Nantes, 5-8 juin 2016, https://www.congresdesnotaires.fr/media/uploads/compte_rendu_complet_relu_version_finale_mise_en_ligne.pdf.

PIGNON (Vincent) (dir.), *Compte-rendu de projet : Preuve de concept blockchain appliquée au registre du commerce République et canton de Genève*, Direction générale des systèmes d'information [en ligne], Département de la sécurité et de l'économie, n° 2559, 1er janv. 2018, p. 16, https://www.ge.ch/document/rapport-experimentation-blockchain/telecharger.

Rapp. AN n° 1501, 12 déc. 2018, de Laure DE LA RAUDIÈRE et Jean-Michel MIS sur les chaînes de blocs (*blockchains*).

Rapp. AN n° 1092, rapp. Sénat n° 584, 20 juin 2018, Comprendre les blockchains : fonctionnement et enjeux de ces nouvelles technologies, présenté par Valéria FAURE-MUNTIAN, Claude DE GANAY, et Ronan LE GLEUT, au nom de l'office parlementaire d'évaluation des choix scientifiques et technologiques.

Rapp. n° 464, 15 mars 2017, pour une intelligence artificielle maîtrisée, utile et démystifiée, déposé par Claude DE GANAY et Dominique GILLOT, au nom de l'Office parlementaire d'évaluation des choix scientifiques et technologiques.

Rapport Groupe Fintech, « Les impacts des réseaux distribués et de la technologie blockchain dans les activités de marché », Paris Europlace [en ligne], 23 oct. 2017, p. 83, https://www.paris-europlace.com/sites/default/files/public/paris_europlace_-_livre_blanc_
blockchain_-_26_octobre_2017.pdf

Report No. ID G00465728, « Magic Quadrant for Contract Life Cycle Management », *Gartner* [online], 25 Feb. 2020, https://www.docusign.fr/gartner-magic-quadrant-gestion-cycle-de-vie-des-contrats.

Report of the European Blockchain Observatory and Forum, « Blockchain and the GDPR », EU Blockchain Forum [online], 16 Oct. 2018,

https://www.eublockchainforum.eu/sites/default/
files/reports/20181016_report_gdpr.pdf.

SONNET (François), « Blockchain-Enabled Solutions for the Uptake of Renewables Energy in Lebanon », UNDP [online], 26 Nov. 2020, https://www.lb.undp.org/content/dam/lebanon/
docs/2020/Publications/CEDRO%20_%20Blockchain%20Report%2025.11.2020_for%20publication.pdf.

STARK (Josh), « Applications of Distributed Ledger Technology to Regulatory & Compliance Processes », R3 Reports [online], 14 Dec. 2017, https://www.r3.com/wp-content/uploads/2018/01/Reg_Compliance_R3.pdf.

The European Union Blockchain Observatory & Forum, « Blockchain innovation in Europe », European Commission [online], 27 Jul. 2018, https://www.eublockchainforum.eu/sites/default/
files/reports/20180727_report_innovation_in_europe_light.pdf.

U Change, *Livre blanc : Comprendre la blockchain*, éd. Creative Commons [en ligne], 2016, https://www.finyear.com/attachment/648901/.

UNCITRAL, « 50e session Programme for the Congress Modernizing International Trade Law to support innovation and sustainable development », Austria : Vienna International Center [online], 4-6 Jul., 2017, http://www.uncitral.org/pdf/french/congress/CALL_FOR_
PAPERS_CONGRESS_Final-FR.pdf.

White Paper No. ECE/TRADE/457 UN Economic Commission for Europe, Sept. 2020, Blockchain in Trade Facilitation (revised version) [en ligne], https://unece.org/DAM/cefact/cf_plenary/2019_plenary/ECE_TRADE_C_CEFACT_2019_08E.pdf.

White Paper No. ECE/TRADE/457 UN Economic Commission for Europe, Blockchain in Trade Facilitation (revised version), submitted by the UN/CEFACT Bureau, UNECE [online], Sept. 2020, https://unece.org/DAM/trade/Publications/ECE-TRADE-457E_WPBlockchain
TF.pdf.

White Paper No. ECE/TRADE/C/CEFACT/2019/8 UN Economic Commission for Europe, 17 Jan. 2019, on the technical applications of Blockchain to United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) deliverables, submitted by the UN/CEFACT Bureau to the twenty-fifth session of the Plenary for noting.
https://unece.org/DAM/cefact/cf_plenary/2019_plenary/ECE_TRADE_C_CEFACT_2019_08E.pdf.

World Economic Forum, Deloitte (collab.), « Blueprint for Digital Identity », Industry Project of the Financial Services Community [online], Future of Financial Services Series, Aug. 2016, http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf.

World Economic Forum, Latham & Watkins, « Bridging the Governance Gap: Dispute resolution for blockchain-based transactions », World Economic Forum [online], Dec. 2020,

http://www3.weforum.org/docs/WEF_WP_Dispute_Resolution_for_Blockchain_2020.pdf.

Index alphabétique

Les numéros renvoient aux paragraphes.

Les numéros en gras renvoient au paragraphe indiqué et à ceux qui suivent.

A

Acte authentique, notarié : **162**

Blockchain Notariale (BCN) : 178

Cas d'usage de la *blockchain* dans le domaine notarial : 8, 178 (à l'international)

Certifier *vs*. authentifier : 173

Formalités d'apostille : 176

Nécessaire intervention du notaire : **172**

Obligation de paraphe (infalsifiabilité) : 176

Projet d'un outil *blockchain* : **175**

Propriété d'un bien immobilier : 169

Transmission des copies d'actes authentiques par voie électronique : 177

Vertus de l'authenticité : **164**, 169

Acte sous signature privée : **109**

Adaptation, adaptabilité de la technologie : 25, 35

Adaptation réciproque avec le juge étatique : 246

Algorithme d'exécution du droit des contrats : 35

Collaboration entre chaînes : 136

Conformité aux obligations d'information et de consentement, données à caractère personnel : 200

Délai raisonnable : 227

Diligences utiles, ou suffisantes : 227

Droit de rétractation : 30

Exigences de lisibilité et de présentation en droit des obligations : 25

Juriste-codeur : **225**

Know Your Customer (KYC, règles de conformité « Connaissance client ») : 132

Limites : **211**, 223

Privacy by default : 198

Problématique de l'identification : 114, **121**

Procédure de « double-clic » : 25 (validation contrat électronique), 129 (valant signature électronique)

Projet d'un outil au service de l'authenticité : **175**

Proposition de schéma probatoire visant la reconnaissance de la fiabilité du procédé de signature *blockchain* : **127**

Réciprocité : 246, 359

Admission en justice : **250**

« Juriste codeur » ou « augmenté » : 252 Technicien, expert : 251

Anticipation

Nécessité : 225, 324

Assurances : **50**

Assurances P2P : **56**

Assurances et DAO : 57

Limites : 58, 59

Assurances paramétriques, indicielles : 54, 339

Attentes des assureurs et consommateurs : 50, 51

Dispositif électroniques de suivi embarqués : 354

Exemples d'applications : **52**, **56**, 354

Attaques informatiques : **309**

Attaque à 51 % : **310**

Attaque par déni de service (*DoS attack, Denial of Service attack*) : 316, 317

Attaque par déni de service distribuée (*DDoS attack, Distributed Denial of Service attack*) : 316

Attaques de plateformes de *trading* de crypto-monnaies : 327

Escroqueries (*giveaways* et systèmes de Ponzi) : 331

Forks, attaques à 30 % : 321, 323

Blocs orphelins : 324

Rôle du développeur : 286, 318, 324

Side channel attack : 328

SIM hijacking : 330

TheDarkDAO : **275**

Traitement pénal : 317

Typo-quatting : 329

Atteintes aux systèmes de traitement automatisé de données : 317

B

Blockchain

Blocs : 10, **142**

Concept de la prise de décision par consensus, principe de consensus : 10, 98, 146, 147

Contenu des messages inscrits : 106

De *Bitcoin* à la *blockchain* : 7, 10

Débouchés technologiques de la *blockchain* : 8, 9

Définition et fonctionnement général de la *blockchain* : 10

Fonctions : 7

Horodatage : **152**

Idéologie libérale : 218, **232**, 307

Instantanéité : 25

Intégrité technique

Dispositif de l'arbre de Merkle (*Merkle Tree*) : 145

Fonction de hachage : 104, 105, 145

Neutralité, objectivité : 37, 269

Pratique du pseudonymat : 114, **259**

Preuve de participation (*proof of stake*, PoS) :145, 318

Preuve de travail (*proof of work*, PoW), *mining* : 145

Qualification de dispositif électronique d'enregistrement partagé (DEEP) : 10, 116

Sécurité : 10

Smart contracts : 7, 9, 18, 20

Transparence : 10, 25, 186

Utilité : 305

Blockchain des objets

Concept : **64**
Exemple d'ADEPT : **88**

Interopérabilité : 75, 88

L'objet comme initiateur de la relation contractuelle : 89, 90

Limites de l'auto-exécution dans les relations contractuelles : 91

Solution de la décentralisation : **73**

Bitcoin (le protocole)

Accès au protocole : 6

Adresse publique et clé privée associée, bi-clés (*Bitcoin*) : 100

Adresse *Bitcoin* : 6

Vulnérabilités : 123, **326**

Anonymat : 186, 187

Données réputées « anonymes » : 186, 187, 194

Balance financière : 143

bitcoin (la crypto-monnaie) : 6

Concept du P2P : 6, 7, 10, 57, 147, 233, 279, 280, 291

De *Bitcoin* à la *blockchain* : 7, 10

Fonctionnement : 6

Hash (empreinte), fonction de hachage *SHA256* : 104, 105, 145, 199

Histoire de *Bitcoin* : 5

Langage non-Turing complet : 9

Nœuds (*nodes*) : 6, 311

Preuve de travail (*proof of work*, PoW), *mining* :145

Pseudonymat : 114, **259**

Récompense (*block reward*) : 6

Théorie des jeux : 309

Transaction : 6, 101

Transparence : 186

Validation des transactions : 6, 146

Vérification des transactions : 7, 10, 143

Bugs informatiques : 263, 265, 322

Buterin, Vitalik : 9, 22, 25, 202, 314

C

Cachet électronique : **110**

Centralisation

Crise de confiance, crise des *subprimes* : 3, 5

Systèmes centralisés : 1, 11, **302**

Vulnérabilités de la centralisation : 2, 3, 11, **297**

Certificat de signature électronique (CSE) : 123, 128, 136

Clause attributive de juridiction (élection du for) : 256

Clause compromissoire : 256

Clause d'indexation : 226

Clause de *hardship* : 226

Clause résolutoire : 34

Clause sur la loi applicable : 256

Code is Law : **232**, 260

Collaboration interdisciplinaire : 226, 355

Compétence internationale : **254**

Compétence technique : **250**

Formation du corps juridique : 252

Confiance

« Contrat psychologique » : 1

Comportement de l'Homme : **308**

Confiance algorithmique : 11, **38**, 208, **232**, 288, 293, 298, 315, 333, **356**

Confiance dans les relations contractuelles : 1, 9, 15, 92

Confiance dans les relations humaines : 1, 11

Crise de confiance : 3

Excès de confiance dans l'agent-développeur : 259

Rôle du droit des contrats dans l'institution d'une confiance entre les Hommes : 11

Utilité de la confiance entre les Hommes : 11, 29, 92, 233, 298

Conflit de loi : **254**

Approche de Savigny : 254

Détermination contractuelle de l'ordre juridique et de la compétence juridictionnelle : 256

Consensus : 10, 98, 146, 147

Conservation de preuve d'intégrité (en matière d'actes juridiques) : **147**

Contrat

Auto-exécution *via* la *blockchain* : **27**

Contrat *fiat*, traditionnel : 18, 20

Contrats conclus par voie électronique : 25

Double signé : 150

Droit applicable : **254**

Efficacité de la force contractuelle : **28**

Preuve d'un acte juridique : 155

Principe de bonne foi, bonne foi : 15, 223

Risque de postdate, d'antidate : 153

Rrôle du droit des contrats dans l'institution d'une confiance entre les Hommes : 11

Sécurité juridique : 29

Contrat d'adhésion : 213, 244

Convention secrète de déchiffrement : 122, v. également « Cryptologie » > « Adresse publique et clé privée associée, bi-clés (*Bitcoin*) »

Création de preuve d'antériorité (en matière d'actes juridiques) : **152**

Crypto-actifs : 7

Crypto-monnaie : 5, 7

Cryptologie

Adresse publique et clé privée associée (ou convention secrète de déchiffrement), bi-clés (*Bitcoin*) : 100

Bitcoin : 5, 6

Bombe cryptologique : 4

Clés cryptographiques et cryptographie asymétrique : 5, 99, 100, 111, 199

Cryptographe : 4

Cryptographie, cryptanalyse : 4

Fonction de hachage (*hashing*) : 104, 105, 145

Métaphore du problème des généraux byzantins : 98

Procédé de chiffrement mathématique par clés : 98, 99

Traitement pénal des conventions secrètes de déchiffrement (clés privées) : 122

Cyberattaque : 1

Cybersécurité : 8, 74

Cypherpunks : 5

D

Dai, Wei : 5

Décentralisation

Code is Law : **232**, 260, 291

Concept de la crypto-monnaie, *Bitcoin* : 5, 6

Concept de la décentralisation : 5, 6

Double dépense, appréhension (*double-spending problem*) : 6, 146, 316

Intervention du juge étatique : **229**

Mécanisme de vérification décentralisé : 7, 143

Objectif de la décentralisation : 3, 6, 98, 291

Réseau décentralisé : 7, 10

Risques des *mining pools* : 301, 312, 313, 314

Decentralized Autonomous Applications (DAO) : 42, 57, 81, 237, 272

Délai raisonnable : 227

Déséquilibre « significatif » : 244

Déséquilibre contractuel : 213

Désintermédiation : 79

Substitution à l'Homme, limites : 91, 170, **225**

Désubérisation : 11

Difficultés économiques

Dispositifs et délais juridiquement accordés pour retard d'exécution : 223

Paramétrage d'une suspension temporaire d'exécution : 227

Pratique de la « seconde chance », tolérance : 223

Diligences utiles, ou suffisantes : 227

Dispositif de conservation de preuve d'intégrité (en matière d'actes juridiques) : **147**

Admissibilité de principe du support électronique : 149

Coffre-fort numérique : 148

Exigences légales concernant les documents électroniques archivés : 149

Typologie des méthodes d'archivage : 150

Dispositif de création de preuve d'antériorité (en matière d'actes juridiques) : **152**

Admissibilité : 157

Convention de preuve : 157

Horodatage *blockchain* : 154

Principe de non-discrimination entre les techniques d'horodatage électronique : 157

Dispositif électronique

Dispositif électronique doté de capacités d'action sur le réel : 64

Dispositif électronique doté de capacités d'adaptation à son environnement : 64

Dispositif électronique doté de capacités de communication des données captées : 65

Dispositif électronique doté de capacités de perception de son environnement : 64

Oracle physique, *hardware* : 68, 350, **352**

Dispositif électronique d'enregistrement partagé (DEEP) : 116, 117

Disruption, disruptif : 11, 186, 231, 234, 356

Distribution

Concept du P2P : 6, 7, 10, 57, 147, 233, 279, 280, 291

Principe de consensus : 10, 98, 146, 147

Processus décisionnel, vote : 146, 147, 292

BIP (*Bitcoin Improvement Proposal*) : 292

Risques des *mining pools* : 301, 312, 313, 314

Validation des blocs : 146

Vérité partagée : 291, 305

Données à caractère personnel

Adresse IP : 195

Attaques : 195

Avantages des systèmes centralisés : 302

Confiance : 205, 208

Consentement au traitement : 200

Dispositifs de fourniture et de contrôle d'identité : 190

Données contenues sur une *blockchain* : 186

Données réputées « anonymes » : 186, 187, 194

Désanonymisation : 195

Droit à l'oubli, à l'effacement : 206

Droit à la rectification, à la mise à jour de ses données : 206

Ledger : 188

Obligations d'information et de consentement : 200

Portefeuille (*wallet*) : 191

Potentiel identifiant des données : 193, 194, 195

Principe d'autodétermination informationnelle : 205

Principe de minimisation : 199

Privacy by default : 198

Privacy by design : 198

Responsable de traitement : 200, 201, 202, 203, 262

Smart contract : 189

Transfert hors UE : 207

Droit à la preuve : 123

Dysfonctionnement : **258**

Erreur humaine : 259, 260, 276

Faille technique : 262, 265

Perte de chance : 262

E

Économie collaborative, de pair à pair : 2

Environnement : 41, 44, 45, 46, **86**

Ethereum (protocole)

dApp : 20, 57, 86

Déploiement : 9

Frais de traitement (*gas*) : 20, 143

Langage Turing-complet, *Turing-completeness* : 9, 25, 68

Oracle : **333**

Ethereum Virtual Machine (EVM) : 9, 20

Exécutoire (*enforceable*) : 9, 28

F

Faille technique : 262, **320**

Force majeure : 35, 212, 226

Force probante d'un acte : 109, **139**, 155

Fork : 262, 280, 316, **321**

Formalités d'apostille : 176

Fournisseur d'accès à Internet (FAI) : 262

G

Gouvernance : **269**

Appropriation, monopoles : 299, 300

Mining pools : 301, v. également, 312, 313, 314

Modèles d'administration centralisée : **302**

Blockchain « de consortium » : 295

Avantages : 302, 303

Blockchain « privée » : 294

Avantages : 302, 303

Blockchain publique : **290**

« Vérité partagée » : 291

Décentralisation : 291

Distributivité, décision distribuée : 292, 293

Limites : 286, 296

Ouvert en lecture et en écriture : 290

Théorie du contrat social : 293

Decentralized Autonomous Applications (DAO) : 272

TheDAO : **273**

Facteur confiance : 281, 283, 285, 287

Recherche d'équilibre : 280, 281, 285, 286, 287

Rôle du développeur : 286

Sécurité : 283

H

Hacker : **275**

Hash : 104, 105, 145, 199

Hébergeur : 262

Hobbes, Thomas : 1

Horodatage : **152**, 157

Huissier de justice : 130, 158

I

Immuabilité, immutabilité : 6, 8, 10, 18, 25, 29, 52, 105, 176, 291

Limites : **183**

« Facteur d'accélération des difficultés » : 222, 223

Annulation : **215**

Inaltérabilité des inscriptions : 104, 105, 113, **184**

Modification : **212**

Principe d'exécution intégrale : 29, **210**

Privatisation des *blockchains* : 304, 305, 316

Théorie de la responsabilité : 216

Imprévision : 212

Clause d'indexation : 226

Clause de *hardship* : 226

Clauses de conciliation, de médiation préalable obligatoire, de client le plus favorisé, limitatives de responsabilité, de répartition des risques : 226

Juge étatique : 244

Inarrêtable (*unstoppable*) : 29

Limites : 206, **210**

Industrie culturelle : 48

Instructions algorithmiques : 18, 20

Intelligence artificielle : 22, 355

Intermédiaire : 2, v. également « Tiers de confiance »

Internet

Centralisation, privatisation d'Internet : 298

Histoire d'Internet : 4, 11, 298

Internet of Things (IoT, « Internet des Objets ») : 66, 355

J

Juge étatique

Application du principe d'équivalence fonctionnelle (matière probatoire) : 119

Conditions de l'intervention du juge : 246

Formation du corps juridique : 252

Intervention du juge : 37, **229**, **244**

Juge compétent (international) : **254**

Juridiction alternative : 245

Légitimité : 229, **244**

Pouvoir de contrainte : 244

Protection de la partie faible au contrat : 244

Juriste-codeur : **225**, 252

K

Know Your Customer (KYC, règles de conformité « Connaissance client ») : 8, 132, 191

L

Lésion : 213

Libéralisme : 232, 307

Code is Law : **232**

Limite, centralisation : **297**, **310**

Limite, principe du vote : 281, 282, 285

Lignes de code : 17

Locke, John : 293, 307

Logiciel informatique : 19

M

Machine-to-machine (M2M), système : 67, 79

Memory pool : 143

Mineurs : 10, 20, **142**, 263, 264, 311

Mise en demeure : 34, 35, 41

Mode de preuve : **140**

Vers une reconnaissance juridique ? : 160, 161

Multi-signatures, systèmes de : 30

N

Nakamoto, Satoshi : 5, 7, 18, 291, 292, 300, 304

Netziens : 1, 293

Neutralité

- Limite, centralisation : **297**
- Limite, erreur humaine : 260, 276
- Neutralité de l'outil informatique : 3
- Neutralité de la *blockchain* : 37, 269

Nœud (*node*) : **142**, 311

Nullité (contrat) : **215**

- Théorie de la responsabilité : 216

Notaire : **162**

- Confiance : 170
- Fonction notariale, office du notaire : **164**
  - Devoir d'authentification : 164
  - Devoir de conseil : 164
- La responsabilité professionnelle et collective des notaires : 168, 169

O

Objet dit « connecté » : 65

Objet dit « intelligent » : 64

Open source

- *Blockchain* publique : **290**, 306
- Propriété intellectuelle : 300
- Risques d'appropriation, monopoles : 299, 300, 301, 306

Opérateurs de de communications électroniques : 262

Oracle : 334

- Application du problème des généraux byzantins : 349
- Assurances indicielles : 339
- Confiance : 346, **347**
- Fiabilité (conditions) : 342, 343, 349, 350, 354
- Fonctionnement de l'Oracle : 68, 336
- Limites : 344, 345, 346, 347, 350, 351
- Marchés prédictifs : 340
- Oracle (*Ethereum*) : 335, 337
- Oracle physique, *hardware* : 68, 350, **352**
  - Capteurs : 352, 353, 354
  - Cas d'usage : 353, 354
  - Dispositifs électroniques : 352
- *Oraclize* : 338
- Responsabilité : 344, 349
- Turing-complet : 336

P

Pactes d'actionnaires : 28

Plateformes de change (de *trading*) de crypto-monnaies : 20

- Attaques informatiques : 327, 329
- Données à caractère personnel : 191, 195, 198, 203, 205, 207
- Systèmes d'identification des utilisateurs : 132, 135

Portefeuille numérique pour crypto-monnaies (*wallet*) : 6, 100

- Attaques informatiques : 327, 328, 329, 330
- Bi-clés (adresse publique et clé privée associée) : 100
- Données à caractère personnel : 191, 194, 195, 198, 205, 320
- *Online wallet / Offline wallet* : 100, 326
- *Root seed* (graine primaire/de récupération) : 100
- *Software wallet / Hardware wallet* : 100, 326

Transaction : 101

Vulnérabilité des bi-clés : **326**

Vulnérabilité des informations d'identification : 123, 320, 330

Préemption, droit de préemption : 28

Preuve de participation (*proof of stake*, PoS) :145, 318

Preuve de travail (*proof of work*, PoW), *mining* : 145

ASICs, processeurs, puissance de calcul : 311, 314, 317

Perspectives d'évolution : 318

Risques des *Mining Pools* : 301, 312, 313, 314

Principe de non-discrimination technologique (matière probatoire) : 119

Programme informatique : 19

Propriété intellectuelle

Brevet : 300

Licence : 300

Logiciel *open source* : 300

Preuve : 156, 158, 159 (exemple de la Chine)

Protection des données à caractère personnel

Données à caractère personnel : **185**, v. également « Données à caractère personnel »

R

Registre décentralisé et infalsifiable (*ledger*) : 7, 8

Actes notariés : 176, v. également « Actes authentiques »

Archivage décentralisé et infalsifiable : 8, **141**, 147

Dispositif de conservation de preuve d'intégrité : **147**

Données à caractère personnel : 188, 189, 206

Exemples de cas d'usage : 8, 156, 158, **175**

Force probante d'un acte : 109, **139**

Outil de preuves diverses : 25, 28, 35, 52, 156, 200

Pouvoir de contrainte d'un juge, non : 244

Typologie des méthodes d'archivage : 150

Vers une reconnaissance juridique officielle ? : 160

Règlement des conflits

Code is Law : **232**

Modes alternatifs de règlement des conflits (MARC) ou modes alternatifs de règlement des litiges (MARL) : 236

Mode de résolution des litiges intégré : **235**

Arbitrage : 241

Limites : **240**

Solution de règlement amiable des différends : 236, 237

Système originel, libertaire : 235

Online Dispute Resolutions (ODR) : 236

Relations

Établissement de relations sans intermédiaire : 10, 28, 92

Pérennité des relations établies *via blockchain* : 28, 92

Relations contractuelles : 1, 223

Relations humaines : 1, 28, 223

Responsabilité : **258**

Clauses d'exonération de responsabilité : 262

Défaut de sécurité : 262, 274, 283, 285, 318

Désignation du responsable : 264, 265

Propositions : 266

Dysfonctionnements : 259, 260, 263, 265

Mécanismes de détection des *bugs*, auditeurs de code : 265, 283

Oracle : 344

Origine du fait dommageable : 264, 280

Préjudice réparable (éléments constitutifs) : 262, 263

Problématique de l'identification : 261, 264, 277

Avantages des systèmes centralisés : 303

Responsabilité civile : 262

Risque numérique : 280

Responsabilité sociale et environnementale des entreprises (RSE) : 41, 267, 355

Restitutions et réparations contractuelles : 34

Rôle de l'État : 359

Rousseau, Jean-Jacques : 293

S

Sanction pour inexécution contractuelle : **33**

Sécurité juridique : 29, 112, 147

Self-sovereign identity : 134, 135, 138, 190

Données à caractère personnel : 190

Smart contracts (« contrat intelligent »)

Appellation trompeuse du « contrat intelligent » : **22**

Modalité technique d'exécution de contrats : 24

Possibilité d'adapter la conception : 25

Problématique du consentement : 25

Assistance à l'exécution : **28**

Automatisation de tâches réputées simples, répétitives et souvent chronophages : 30, 52

Blockchain au *smart contract* : 7, 9

Capacités d'adaptation des *smart contracts* : 25, 35

Clause résolutoire : 34

Contrat numérique auto-exécutant, auto-exécuté, automatisé, dynamique : 18, 20, 22, **27**, 52

Decentralized Autonomous Applications (DAO) : 42, 270, 272

TheDAO : **273**

Définition des *smart contracts* : 9, 18

Exemples de cas d'usage : 9, 30, **39**, **50**, 237, 241

Fonctionnement des *dApps* d'*Ethereum* : 20

Fonctionnement du *smart contract* : 18, 20

Inexécution contractuelle : **33**, 52

Programme ou logiciel ? : 19

Propositions de sanctions pour inexécution contractuelle spéciales : 36

Solution de règlement amiable des différends : 237, 241

Smart contract 2.0

Automatisation de la sanction pour inexécution contractuelle : 72

Blockchain des objets : **64**

Cybersécurité : 74, 86, 150

Désintermédiation : 79

Données à caractère personnel : 189, 194, 199, 202, 203, 205, 206

Exemples de cas d'usage : 81, **82**

Inarrêtable (*unstoppable*) : 206, **210**

L'objet comme initiateur de la relation contractuelle : 89, 90

Limites de l'auto-exécution dans les relations contractuelles : 91

Mise à exécution brutale : **220**

Mise à exécution matérielle instantanée : **71**, 79, 82, 86

Résolution pour inexécution : 72

Smart home : **85**

Projet d'une « blockchain de centaines de milliards d'objets » : **88**

Smart grid : **86**

Smart property : **78**

Domaine d'application : 83

Droit sur un bien : **79**

Mise à disposition d'un bien : **82**

Signature électronique

Dispositif de création de signature électronique : 111

Administration de la preuve électronique, exigences probatoires : **126**

Algorithme RSA avec fonction de hachage : 111

Autorité de certification (AC) : 123

Certificat de signature électronique (CSE) : 123

Infrastructure de gestion de clé (IGC) : 111

Limites du dispositif : 113

Exigences et conditions de validité : 109, 119

Logiciel de vérification de signature électronique : 123

Reconnaissance de la signature dématérialisée : 110

Signature numérique (*blockchain*) : **103**

Accord sur la preuve : 118

Comparaisons techniques avec la signature électronique traditionnelle : **112**, 122

Fiabilité : 113, **117**

Administration de la preuve électronique, exigences probatoires : **126**

Certificat de signature électronique (CSE) : 128, 136

Charge de la preuve : 121, 122, 139, 153

Méthode du faisceau d'indices : 122, 123

Principe de l'équivalence fonctionnelle : 119

Principe de neutralité technologique : 120

Proposition de schéma probatoire : **127**

Hash (empreinte), fonction de hachage : 104, 105, 113, 129

La *blockchain*, prestataire de service de confiance (PSCo) ? Non : 137

Problématique de l'identification : 114, **121**, **125**

Collaboration entre chaînes : 136

Mécanismes d'identification : **132**

Recherches de solutions conformes : **125**

Vulnérabilités : 123, 124, 326

Notaire : 176

Rôle de l'huissier : 130

Surendettement, procédure de rétablissement : 223

Systèmes de traitement automatisé de données : 117

Szabo, Nick : 5, 9, 20, 22, 25, 27, 30, 33, 80, 227

T

TheDAO : 225, 263, **273**

Algorithme : 274, 276

Attaque « *The DarkDAO* » : 275, 276

Création : 273

Fondation Ethereum : 277, **278**

Tiers de confiance

Disruption, disruptif : 11, 186, 231, 234, 356

Code is Law : **232**

Établissement de relations sans intermédiaire : 10, 11, 30, 52, 179, 233

Nouveaux tiers de confiance (spécialisés dans l'intermédiation) : 2

Pratiques monopolistiques, oligopolistiques : **298**

Ré-intermédiation : **278,** 298, **347**

Rôle du tiers de confiance : 2

Tiers de confiance historique : 2

Tiers-Léviathan selon Thomas Hobbes : 1, 293

Utilité du tiers de confiance : 11, 29

Token (jeton) : 42, 44, 90, 135

Transaction (*blockchain*)

Concept de la transaction : 6

Fonctionnement : 101

Inscription : **142**

Qualification juridique : 101

Turing, Alan Mathison : 4

V

Validation des blocs : 10, 146

Validité des conventions

Immuabilité : 217

Vérification des blocs : 7, 10, 143

Vices du consentement : 144

Vitesse de propagation : 143

Vulnérabilités

Risques d'attaques : **309**, v. également « Attaques informatiques »

Veille de la communauté, mises à jour : 207, 292, 318, 322

Table des matières

Les numéros renvoient aux pages.

À propos de l'auteure *3*
Remerciements 4
Sommaire 5
Liste des abréviations 7

INTRODUCTION 14

PARTIE 1

LES APPORTS DE LA* BLOCKCHAIN *EN TANT QUE

SYSTÈME INCUBATEUR DE CONFIANCE :

UNE VOLONTÉ DE SIMPLIFICATION DES RELATIONS CONTRACTUELLES

TITRE 1. Les *smart contracts* : programmation d'une modalité technique d'exécution inédite 53

Chapitre 1. Renforcer l'efficacité de la force contractuelle : l'automatisation comme aide et suivi à l'exécution 54

Section 1. Pour la pérennité des relations contractuelles 54

§ 1. Les propriétés du contrat auto-exécuté *via blockchain* 55

A. Fondements des smart contracts : le fonctionnement du « Bitcoin 2.0 » contractuel 55

B. Divergences doctrinales : l'appellation trompeuse du contrat intelligent 59

§ 2. Les bénéfices du contrat auto-exécuté *via blockchain* 66

A. Une assistance à l'exécution 67

B. Une dissuasion à l'inexécution 74

Section 2. Vers de nouveaux rapports de confiance 78

§ 1. Les diverses applications des *smart contracts* : optimisation des engagements 79

A. De nouveaux domaines de relations conventionnelles 79

B. Une mutation des relations actuelles 84

§ 2. Le fonctionnement des assurances « blockchaînées » : perspectives de changements 91

A. Réinstaurer le lien de confiance dans les assurances traditionnelles 93

B. Affranchir les systèmes traditionnels de mutualisation des risques à travers les assurances P2P 102

Chapitre 2. Amplifier l'efficacité de la force contractuelle : l'interconnectivité comme mise à exécution instantanée 110

Section 1. Une combinaison de technologies : connexion entre mondes physique et virtuel.....110

§ 1. Présentation des notions et technologies du projet « *smart contract* 2.0 » 111

A. Fonctionnement des dispositifs de perception de l'environnement, d'auto-adaptation et de communication..... 111

B. Fonctionnement des systèmes d'interconnexion des objets..... 116

§ 2. Apports réciproques entre technologies du concept « smart contract 2.0 » 120

A. Une mise à exécution matérielle instantanée 121

B. Une interconnexion d'objets décentralisée..... 123

Section 2. Une mutation des relations Homme-machine : transformation des relations contractuelles traditionnelles 127

§ 1. Le fonctionnement de la *smart property* 127

A. Établissement d'un droit immuable et dynamique de disposition d'un bien... 127

B. Programmation d'un mécanisme autonome de mise à disposition des biens . 130

§ 2. La nouvelle *smart home* décentralisée 133

A. Les systèmes d'autoconsommation d'énergie..... 134

B. Le projet d'une « blockchain de centaines de milliards d'objets »..... 137

TITRE 2. La *blockchain* : promesse d'une sécurité juridique accrue..... 143

Chapitre 1. Une variété de signature électronique existante 144

Section 1. Des mécanismes cryptographiques identiques : l'avantage de la sécurisation.....144

§ 1. La technicité du procédé de signature *via blockchain*..... 144

A. Offre et acceptation : l'usage de la cryptographie asymétrique 145

B. Authentification et intégrité : l'utilisation des mécanismes de hachage..... 150

§ 2. La fiabilité du procédé de signature *via blockchain*..... 154

A. Entre théorie et pratiques actuelles : des exigences légales à la création de la signature électronique..... 154

B. Face à face entre signatures électroniques classiques et signatures via blockchain : des similarités de procédés à la question de la fiabilité 158

Section 2. Des systèmes d'authentification divergents : le poids de la pseudonymisation 163

§ 1. L'effectivité des moyens de preuve de la fiabilité du procédé..... 165

A. Le principe de la liberté de la preuve..... 166

B. La dangerosité d'une divulgation d'informations identifiantes pour les utilisateurs d'une blockchain 169

§ 2. La recherche de solutions conformes aux exigences probatoires..... 175

A. Analyse des exigences probatoires..... 176

B. Préludes d'un système autonome d'identification..... 182

Chapitre 2. Une variété de preuve algorithmique naissante 195

Section 1. Une innovation probatoire dans les relations synallagmatiques entre personnes privées 195

§ 1. Entre les parties, la sécurisation des relations *via* une nouvelle forme d'archivage décentralisé 196

A. Un mécanisme de création de preuve d'intégrité 196

B. Un dispositif de conservation de preuve d'intégrité 201

§ 2. Vis-à-vis des tiers, l'horodatage des conventions *via* la création de preuves d'antériorité 208

A. Potentiel de l'horodatage blockchain 209

B. Perspectives de développement de la preuve d'antériorité 213

Section 2. Une solution d'optimisation plus que de substitution en matière d'actes authentiques 221

§ 1. Les spécificités de l'interlocuteur humain : un remplacement délicat .. 222

A. Qualités intrinsèques de la fonction notariale 223

B. Garanties inhérentes à l'intervention du notaire 227

§ 2. L'inaccessibilité du statut d'acte authentique : des solutions *blockchain* divergentes 230

A. Du refus de l'assistance humaine à l'adaptation de la technologie 231

B. Le projet d'un outil au service de l'authenticité 234

PARTIE 2

LES SPÉCIFICITÉS DE LA* BLOCKCHAIN *EN TANT QUE POTENTIELS FREINS À L'INSTITUTION D'UNE CONFIANCE ALGORITHMIQUE : DES RÉSISTANCES COMPLIQUANT L'APPLICATION DES EXIGENCES JURIDIQUES ACTUELLES

TITRE 1. Incohérences entre *blockchain* et droit : un besoin d'adaptation . 243

Chapitre 1. L'immuabilité, une difficile maîtrise des parties 244

Section 1. Le principe d'inaltérabilité des inscriptions face au RGPD 245

§ 1. Entre transparence des blocs et transparence des données 245

A. Étendue des données privées présentes sur la chaîne 245

B. Étendue de la notion de « données personnelles » 253

§ 2. Entre contradictions et freins à l'innovation 259

A. Une pêche aux données neutre mais dépourvue de responsable 260

B. Un traitement des données neutre mais non limité 270

Section 2. Le principe d'exécution intégrale face à la pratique des relations contractuelles 280

§ 1. La rigidité de la chaîne de transactions 281

A. Impossibilité de modifier le contrat 282

B. Impossibilité d'annuler le contrat 284

§ 2. L'importance du rôle joué par l'Homme 288
A. Face à la brutalité des rapports sur blockchain : les spécificités des règles humaines 288
B. Face à l'extrême nécessité d'anticiper : le retour du juriste-codeur 294
Chapitre 2. La décentralisation, une délicate intervention du juge étatique 300
Section 1. Le pouvoir du juge étatique dans la gestion des conflits 300
§ 1. L'application du principe « *Code is Law* » 301
A. Le refus de normalisation de l'État 301
B. Les propositions de mécanismes intégrés de règlement des conflits..... 304
§ 2. La recrudescence du rôle du juge 309
A. De l'imperfection des mécanismes vers une dépréciation de la confiance dans la technologie 310
B. De la protection de la partie faible vers une collaboration entre la technologie et le juge 315
Section 2. Les limites du juge étatique dans l'application des règles de droit 322
§ 1. Des problèmes de compétence(s) 322
A. Compétence technique : la nécessaire formation du corps juridique..... 323
B. Compétence internationale : l'inévitable appréhension d'une technologie sans frontières 327
§ 2. Une question de responsabilité(s) décentralisée(s)..... 332
A. Confiance initiale et barrières de la pseudonymisation 333
B. Difficile recherche et mise en œuvre de la responsabilité..... 336
TITRE 2. Problèmes créés de l'utilisation faite de la *blockchain* : un manque de fiabilité 348
Chapitre 1. Les enjeux de la gouvernance..... 349
Section 1. Le dilemme *TheDAO* : entre protection des utilisateurs et neutralité de la chaîne 349
§ 1. De TheDAO à The DarkDAO..... 350
A. Enjeux et conditions techniques du fonctionnement de TheDAO..... 350
B. Éléments factuels et techniques du détournement de TheDAO 353
§ 2. De l'apparence d'une ré-intermédiation à la remise en cause du système 356
A. Entre propositions et confrontations..... 356
B. Entre nécessité d'instaurer des règles sécuritaires et risques d'une centralisation déguisée 361
Section 2. Les différentes formes de privatisation de la technologie : entre gestion facilitée et réinstauration d'une organisation hiérarchique 365
§ 1. Analyse de la mutation de la *blockchain* en une chaîne centralisée : fermeture et autres divergences 366
A. Blockchain publique 366

B. Blockchains privatisées 370

§ 2. Analyse des conséquences de la privatisation des *blockchains* par des entités centralisées : contrôle et déséquilibres 373

A. La création de monopoles économiques 373

B. La création de modèles d'administration centralisée 379

Chapitre 2. Les vulnérabilités fonctionnelles 384

Section 1. Une technologie compromise par une pluralité de risques d'attaques 384

§ 1. Une faille au sein du principe de consensus décentralisé : les dangereuses prises de pouvoir des attaques à 51 % 385

A. Analyse des comportements de concentration du minage 385

B. Conséquences de la concentration et solutions en projet 389

§ 2. Des failles dans la cybersécurité du protocole distribué : la vulnérabilité des utilisateurs aux nouvelles méthodes de vols 396

A. Le risque des forks 397

B. Le risque des attaques de clés 401

Section 2. Un fonctionnement limité par la présence imposée des Oracles 407

§ 1. Fiabilité des yeux extérieurs à la *blockchain* 407

A. L'Oracle, outil de recherche instantanée d'informations 408

B. Entre risques de centralisation et responsabilité(s) 413

§ 2. Vers un déplacement de la confiance initiale 416

A. Entre ré-intermédiation et émergence de nouveaux tiers de confiance 417

B. L'Oracle physique, passerelle entre les deux mondes 421

CONCLUSION GÉNÉRALE 426

Annexes 431

Table des annexes 432

Bibliographie 444

I. Sources juridiques 444

A. Ouvrages généraux, manuels, cours, traités 444

B. Ouvrages spéciaux, mémoires, thèses 445

C. Articles 447

D. Ouvrages encyclopédiques, fascicules 447

E. Revues, publications périodiques et ressources numériques 449

II. Sources non-juridiques 459

A. Ouvrages généraux 459

B. Articles 462

C. Ressources numériques 466

III. Colloques 468

IV. Références web 468

Index alphabétique 476