LIÈGE université Library

https://lib.uliege.be

https://matheo.uliege.be

De quelques aspects juridiques d'une technologie nommée Blockchain

Auteur : Clemens, Alexandre
Promoteur(s) : Thirion, Nicolas
Faculté : Faculté de Droit, de Science Politique et de Criminologie
Diplôme : Master en droit à finalité spécialisée en droit des affaires (aspects belges, européens et internationau
Année académique : 2021-2022
URI/URL : http://hdl.handle.net/2268.2/15762

Avertissement à l'attention des usagers :

Tous les documents placés en accès ouvert sur le site le site MatheO sont protégés par le droit d'auteur. Conformément aux principes énoncés par la "Budapest Open Access Initiative"(BOAI, 2002), l'utilisateur du site peut lire, télécharger, copier, transmettre, imprimer, chercher ou faire un lien vers le texte intégral de ces documents, les disséquer pour les indexer, s'en servir de données pour un logiciel, ou s'en servir à toute autre fin légale (ou prévue par la réglementation relative au droit d'auteur). Toute utilisation du document à des fins commerciales est strictement interdite.

Par ailleurs, l'utilisateur s'engage à respecter les droits moraux de l'auteur, principalement le droit à l'intégrité de l'oeuvre et le droit de paternité et ce dans toute utilisation que l'utilisateur entreprend. Ainsi, à titre d'exemple, lorsqu'il reproduira un document par extrait ou dans son intégralité, l'utilisateur citera de manière complète les sources telles que mentionnées ci-dessus. Toute utilisation non explicitement autorisée ci-avant (telle que par exemple, la modification du document ou son résumé) nécessite l'autorisation préalable et expresse des auteurs ou de leurs ayants droit.

LIÈGE université
Droit, Science Politique & Criminologie

Département de Droit

De quelques aspects juridiques d'une technologie nommée Blockchain

Alexandre CLEMENS

Travail de fin d'études

Master en droit à finalité spécialisée en droit des affaires

Année académique 2021-2022

Recherche menée sous la direction de :

Monsieur Nicolas THIRION

Professeur ordinaire

RÉSUMÉ

Alors que la notoriété du bitcoin n'est plus à faire, la technologie sur laquelle il repose reste, pour l'heure, encore méconnue du grand public. Cette avancée technologique se nomme *blockchain* et se trouve être à la base du fondement technique sur lequel repose l'ensemble des crypto-monnaies.

Cette présente contribution aura pour modeste ambition de démystifier les contours de la technologie *blockchain* tout en présentant quelques aspects juridiques qu'il est déjà possible de mettre en exergue.

Une première grande partie concernera les aspects techniques de cette technologie innovante, d'une part en présentant l'intégralité du fonctionnement d'une *blockchain*, d'autre part, en analysant deux domaines d'application que la *blockchain* rend possible : les cryptos-actifs et la DeFi.

Une deuxième partie concernera les aspects juridiques des deux domaines d'applications que nous aurons analysés, aussi bien dans une perspective de droit *de lege lata* que de droit *de lege ferenda*.

Au travers de cette contribution, nous tenterons de rendre cette technologie la plus accessible possible tout en offrant une analyse de qualité. Le lecteur désireux de découvrir la technologie *blockchain* trouvera dans cette contribution un premier point de départ.

REMERCIEMENTS

Je tiens tout particulièrement à remercier mon tuteur académique, Monsieur Nicolas Thirion, Professeur ordinaire à la Faculté de droit de l'Université de Liège, pour sa disponibilité et la qualité de ses conseils.

TABLE DES MATIERES

INTRODUCTION

Qui peut encore se targuer de dire qu'il n'a pas vu passer, au travers de médias *mainstream* usant de titres pour le moins racoleurs, la notion de « bitcoin » ? Qui n'a pas au sein de son entourage une personne « inconsciente » s'adonnant au trading de crypto-monnaies ? Qui n'a pas dû, à un moment ou l'autre, s'extirper d'une discussion (ennuyeuse ?) sur les avantages et inconvénients d'une *blockchain* ? En définitive, qui n'a pas essayé de répondre, l'espace d'un instant, à la question de savoir ce qu'était ce nouveau phénomène ?

Alors que la notoriété du bitcoin n'est plus à faire, la technologie sur laquelle il repose reste, pour l'heure, encore méconnue du grand public. Cette avancée technique se nomme *blockchain* et se trouve, très certainement, au fondement d'une des plus grandes révolutions que le XXI^{e} siècle connaitra.

De par les innombrables applications que la *blockchain* tend à offrir, nous verrons que l'ensemble des sujets de société peuvent être, de près ou de loin, touchés par cette technologie, comprendre la *blockchain* devient, à notre sens, inévitable.

C'est pourquoi le monde juridique se doit de devenir un acteur incontournable de cette avancée en apprivoisant au mieux ce concept de *blockchain*. D'abord, en se formant intelligemment et en prenant conscience du rôle qu'auront les juristes dans ce tournant technologique. Ensuite, en légiférant de manière pertinente tout en laissant une certaine souplesse au développement de la technologie.

Cet exposé aura comme modeste ambition, dans un premier temps, d'offrir un tour d'horizon technique de ce qu'est la technologie *blockchain*. Nous nous efforcerons de rendre compréhensible un sujet qui peut être fastidieux en le vulgarisant et en l'illustrant au mieux. Étant donné que la bonne compréhension de cette technologie est l'essence même de son fonctionnement, une majeure partie de cette contribution lui sera destinée. Nous terminerons le développement du concept en présentant les différents changements de paradigme que la *blockchain* a produit, produit et produira encore, ainsi que les domaines d'application où elle tend à se développer.

Nous poursuivrons en présentant deux domaines d'application particuliers de cette technologie : les crypto-actifs et la finance décentralisée. Ce choix est de mise attendu que la majeure partie des applications est développée, pour l'instant, dans ces deux cadres-là, sans parler des investissements colossaux y afférant et du contrôle croissant des pouvoirs étatiques.

Ensuite, il sera temps de présenter un aperçu du cadre juridique actuel entourant les deux domaines d'application examinés dans la deuxième partie. Cette présentation sera réalisée via une analyse de l'état actuel des cadres législatifs européens.

Enfin, une analyse critique de la situation nous permettra de nous positionner par rapport à la réception de cette technologie par les institutions connues du monde financier et également par les institutions juridiques.

I. ASPECTS TECHNIQUES

CHAPITRE 1 : *BLOCKCHAIN*, UNE TECHNOLOGIE SOUS-JACENTE

1) Approche liminaire et « définition »

Une blockchain[1], ou « chaine de blocs », est d'abord et avant tout le nom d'une technologie. Tout à fait récente du point de vue de l'histoire du stockage et de la transmission d'informations, elle est pourtant déjà bien connue des milieux scientifiques comme les sciences informatiques. Alors que les premiers travaux sur le concept de « blockchain » remontent aux années 1990[2], cette technologie gagna sa notoriété avec la création du bitcoin en 2008 par Satoshi Nakamoto[3].

En effet, cet individu ou ce groupe de personnes[4] fut le premier à utiliser la technologie blockchain, et cela dans un contexte particulier mais également dans un domaine « controversé » : celui des crypto-monnaies.

D'une part, la crise financière et bancaire de 2008 instaura une certaine méfiance vis-à-vis du monde financier au sens large, ce qui obligea certaines personnes à repenser le monde monétaire/financier tel qu'on l'avait connu. D'autre part, le bitcoin avait été initialement pensé[5] pour rendre obsolète l'utilisation de monnaies ayant cours légal ou du moins trouver un palliatif au système monétaire classique. Nous reviendrons sur ces changements de paradigme[6].

Quoi qu'il en soit, la technologie blockchain fut la toile de fond nécessaire pour voir émerger, depuis ces dix dernières années, l'ensemble des crypto-monnaies existantes[7]. Notons d'emblée que réduire l'application de cette technologie à la seule utilisation de monnaies cryptographiques reviendrait à l'amputer de tous les domaines d'application qu'elle tend à recouvrir.

Le concept de « blockchain » n'ayant d'ailleurs aucune définition juridique, il doit être compris comme un système qui stocke de l'information sous la forme de blocs contenant des données.

---

1 Ce terme sera dès à présent compris comme un mot français ; dès lors, nous ne ferons plus usage de l'italique.

2 Haber, S., Stornetta, W.S., How to time-stamp a digital document. J. Cryptology 3, 99–111 (1991), disponible sur https://doi.org/10.1007/BF00196791 .

3 S. NAKAMOTO, « Bitcoin : A Peer-to-Peer Electronic Cash System », 2008, disponible sur https://bitcoin.org/bitcoin.pdf .

4 À l'heure actuelle, personne ne connaît l'identité réelle qui se cache derrière le pseudonyme de Satoshi Nakamoto. Il est d'ailleurs préférable, à notre sens, que cet anonymat persiste. En effet, si la paternité de la blockchain Bitcoin venait à être révélée, il est fort probable que l'essence même de cette blockchain viendrait à vaciller vu l'ébranlement de son caractère TOTALEMENT décentralisé.

5 S. NAKAMOTO, op. cit., Introduction, p. 1 ; E., SOTIRI, *Précis sur les crypto-monnaies*, Bertrange, Luxembourg, Legitech, 2018, p. 41.

6 Voyez *infra* p. 27.

7 Nous préférons l'utilisation du terme « crypto-actifs » qui, suite aux évolutions, correspond mieux à l'utilisation qui en est faite actuellement. Voyez *infra* p. 31, la section 1 : *Qu'est-ce qu'un crypto-actif ?*

Chaque nouveau bloc créé est lié avec les précédents, d'où le terme « chaîne de blocs »[8]. Ce système de stockage est ensuite répliqué sur des nœuds (ou système informatique composé d'ordinateurs), l'ensemble formant un registre décentralisé. Pourquoi décentralisé ? Parce que l'ensemble des nœuds n'est pas sous le contrôle d'une autorité centrale mais que, à l'inverse, le contrôle se fait conjointement par l'ensemble du réseau (composé de nœuds). On appelle dès lors ce réseau : un réseau *peer-to-peer*[9].

Concrètement, une blockchain peut être vulgarisée comme étant un registre (*ledger*, en anglais) ou encore comme un grand livre comptable contenant l'ensemble des transactions[10] faites au sein d'un réseau. Ce registre, ouvert et donc accessible à tous, permet à qui le veut de vérifier une information et également de mettre en avant l'irrégularité d'une transaction ou d'une information échangée. La dernière grande particularité de ce registre est qu'il n'est la propriété d'aucun des individus utilisant le dit réseau, ce qui évite la falsification et la manipulation de certaines données contenues dans le registre.

Avant de passer en revue l'ensemble des caractéristiques composant cette technologie, il nous convient d'apporter une distinction importante quant à la compréhension du concept. En effet, nous parlerons plus volontiers d'UNE blockchain parmi tant d'autres et non pas de LA blockchain comme s'il n'en existait qu'une seule[11]. On comprendra, à la lecture de cette contribution, qu'il existe une multitude de blockchains (voire d'écosystèmes) ayant chaque fois des spécificités propres ainsi que des objectifs différents.

2) Caractéristiques

Pour parler d'une blockchain, il est indispensable que celle-ci remplisse plusieurs caractéristiques principales (a) qui sont fondamentales et cela au niveau du concept même de « blockchain ». Par la suite, d'autres caractéristiques peuvent venir s'ajouter. Ces caractéristiques « secondaires » (b) sont tantôt des choix techniques dans une perspective de concurrence (économique) entre les blockchains, tantôt des choix qui ont trait à la politique d'une blockchain, c'est à dire des choix qui caractérisent une chaîne de blocs pour une utilité précise.

---

8 A., BEELEN, *Tout sur la blockchain et ses applications*, Limal, Anthemis, 2021, p. 31.

9 J.-N., COLIN, « Du Bitcoin aux DAO : les fondations techniques de la blockchain » in Cotiga-Raccah, A. et al. (dir.), *Les blockchains et les smart contracts à l'épreuve du droit*, 1e édition, Bruxelles, Larcier, 2020, p. 10 ; Voyez *infra* p. 11.

10 Le terme « transaction » doit être compris comme une information inscrite dans une blockchain indépendamment de la nature de cette information. Nous verrons *infra* (p. 23 et 24), qu'il existe une multitude d'informations de natures différentes avec des finalités propres, reprises sous le vocable « transaction ».

11 J., SÉNÉCHAL, « blockchains « publiques », smart contracts, organisations autonomes décentralisées et gouvernance » in Cotiga-Raccah, A. et al. (dir.), *op. cit*., 1e édition, Bruxelles, Larcier, 2020, p. 52.

a) Caractéristiques principales

1. La décentralisation

Le caractère décentralisé d'une blockchain est certainement l'élément le plus novateur et important de cette technologie, du moins en ce qui concerne les blockchains dites publiques[12]. Habituellement, nos institutions (étatiques, bancaires, administratives, scolaires, médicales, etc.) ont la particularité d'être centralisées. Cela signifie qu'un pouvoir surplombant le tout délègue à un tiers de « confiance » la possibilité de réguler notre situation.

Par exemple, lorsque je veux émettre un virement bancaire à l'attention d'une personne X, je dois passer par l'intermédiaire d'une institution bancaire et de son banquier (tiers de confiance) afin que ce dernier valide et permette le transfert d'argent.

Or, la blockchain permet justement de se passer de ce tiers de confiance pour que le transfert se fasse directement entre la personne destinataire du transfert d'argent et moi-même. C'est ce que l'on appelle un réseau de pair à pair ou *peer-to-peer*. En effet, chaque nœud du réseau peut remplir le rôle du tiers de confiance et un nœud défaillant peut être remplacé instantanément par un autre[13]. Nous verrons comment *infra*[14].

De plus, l'intégralité du réseau, donc l'ensemble des nœuds constituant le réseau, se charge de contrôler la validité des transactions sur une blockchain. C'est par des mécanismes dits de consensus installés au sein des blockchains que la décentralisation est rendue possible[15].

2. La sécurité

De par son fonctionnement technique (voyez *infra*[16]), une blockchain est composée de différents nœuds qui répliquent simultanément l'ensemble des informations stockées dans les blocs, au contraire donc des institutions centralisées. Ce qui veut dire qu'il est « pratiquement »[17] impossible de falsifier une information inscrite dans un bloc.

Car on ne peut venir qu'ajouter de l'information dans une blockchain, c'est d'ailleurs une de ses grandes spécificités. Sans rentrer dans les détails, la modification d'une transaction obligerait un nœud à recalculer l'ensemble des blocs déjà émis depuis la transaction que l'on veut modifier. Ensuite, l'ajout d'une information devrait nécessairement faire l'objet d'une

---

12 Selon qu'une blockchain est publique ou privée, ses caractéristiques intrinsèques peuvent être différentes mais nous y reviendrons lorsque nous ferons état de cette différence (voyez *infra*, p. 13).
13 J.-N., COLIN, *op. cit.*, p. 12.
14 Voyez p. 17 et s.
15 A., BEELEN, *op. cit.*, p. 32 ; Voyez *infra*, p. 17 et s.
16 Voyez p. 15 et s.
17 En effet, il réside tout de même certaines craintes que nous développerons *infra*, p. 17 et s.

validation par l'ensemble du réseau. Un individu seul est donc incapable d'opérer de telles modifications sans que l'ensemble du réseau (des nœuds) en soit averti[18].

3. La confidentialité

À nouveau, de par son fonctionnement technique et cryptographique, les informations/ transactions sur une blockchain sont rendues confidentielles.

L'un des grands arguments utilisés par les détracteurs de la technologie est la présentation de celle-ci comme un moyen de rendre complètement anonymes les utilisateurs d'une blockchain même lorsque ceux-ci l'utilisent à des fins illicites. Par exemple, pour financer le terrorisme ou blanchir de l'argent.

Afin de couper court à toutes les idées reçues, le lecteur doit savoir que d'une part, il est tout à fait possible, grâce à des moyens informatiques, de se rendre compte de l'identité d'une personne derrière l'utilisation d'une crypto-monnaie. Des entreprises sont d'ailleurs spécialisées dans l'analyse des transactions sur les blockchains[19]. D'autre part, moins de 1% des crypto-monnaies sont utilisées à des fins illicites[20].

4. La transparence

Enfin, l'intégralité des transactions passées sur une blockchain est vérifiable et traçable. Ceci est une conséquence du caractère décentralisé de la technologie. En effet, les différents nœuds d'un réseau, donc d'une blockchain, sont partagés par tous ses utilisateurs. L'on parlera ainsi d'un réseau/registre dit « distribué » et, par conséquent, transparent. Il est donc permis à tout individu de se renseigner sur une transaction particulière, et cela sans l'intervention d'une partie tierce[21] ; mais cette transaction sera à tout le moins confidentielle étant donné l'utilisation de procédés cryptographiques que nous verrons *infra*[22].

En pratique, il suffit de se rendre sur un site spécialisé pour se rendre compte de la transparence d'une blockchain[23].

---

18 A., BEELEN, *op. cit*., p. 34.
19 *Ibidem.* : Prenez l'exemple de l'entreprise Chainanalysis fondée en 2014.
20 https://www.reuters.com/article/crypto-currencies-criminals-idUSKBN28J1IX(https://cutt.ly/9xZD1EA); https://cryptoforinnovation.org/resources/Analysis_of_Bitcoin_in_Illicit_Finance.pdf (https://cutt.ly/sb6i6zO).
21 A., BEELEN, *op. cit*., p. 32.
22 Voyez *infra*, p. 21.
23 Par exemple, l'entièreté des informations sur la blockchain Ethereum peut être consultée sur www.etherscan.com (https://cutt.ly/ZxZFtYN).

b) Caractéristiques secondaires

Les caractéristiques « secondaires » sont des ajouts, des particularités propres à chaque blockchain lors de sa conception par les fondateurs. Elles ont comme principal objectif de venir soit renforcer soit diminuer une des caractéristiques principales analysées *supra* (*1.*). Elles peuvent aussi ajouter tout simplement une caractéristique innovante faisant la spécificité d'une blockchain (*2.*).

1. Publique, privée ou de consortium

a. Blockchain publique

Comme l'explique M. Beelen, une blockchain publique est « ouverte à tous (comme la blockchain Ethereum et celle qui gère les bitcoins), appelée en anglais *permissionless* : tous les participants peuvent soumettre des transactions, ont accès à la base de données, peuvent en héberger une copie et proposer des modifications en mettant à disposition leur puissance de calcul. Ces blockchains sont sécurisées grâce aux protocoles de consensus de style « preuve de travail » (*Proof-of-Work*) ou « preuve de dépôt » (*Proof-of-Stake*). »[24]

b. Blockchain privée

Les blockchains privées ne sont pas ouvertes à tous, les droits d'accès et de modification de la base de données sont conditionnés par l'autorisation d'une autorité centrale[25].

C'est pourquoi nous écrivions, lors de l'analyse du caractère décentralisé d'une blockchain, que cette caractéristique se retrouvait moins dans une chaîne de bloc privée et cela principalement au niveau de son accessibilité. Sinon, techniquement, les blockchains privées fonctionnent de manière décentralisée.

Ce type d'installations est particulièrement intéressant pour l'organisation interne de certaines structures comme des sociétés, des hôpitaux ou bien encore des administrations publiques. Elles offrent l'avantage d'être créées sur mesure suivant la spécificité de l'institution, de pouvoir contrôler qui y a accès et surtout elles n'ont pas besoin, pour fonctionner, de rémunérer leurs mineurs[26] avec l'adoption d'une crypto-monnaie[27].

c. Blockchain de consortium

Les blockchains de consortium sont à notre sens de nature hybride. Malgré le fait qu'elles soient ouvertes au public, certaines informations ne sont pourtant pas accessibles à tous. De plus, les droits entre les utilisateurs ne sont pas les mêmes et la validation des blocs s'effectue suivant des modalités prédéfinies. Autrement dit, elle fonctionnera sur la base d'un partenariat contractuel définissant qui peut faire quoi. Par exemple, l'aval de 50% des participants sera

---

[24] A., BEELEN, *op. cit*., p. 34.
[25] *Ibidem.*
[26] Voir le point « Le minage et les mineurs », p. 16.
[27] A., BEELEN, *op. cit*., p. 34.

nécessaire dans une chaine pour valider un bloc, une information[28], ou encore seuls certains acteurs auront le droit de vote.

Dans une blockchain privée, l'organisation est centralisée autour d'un acteur unique. Ici, certains des acteurs ont plus de droits que d'autres, ce qui *de facto* leurs permet de prendre certaines décisions sans devoir s'en remettre à l'entièreté du réseau.

d. Comparaison entre une blockchain privée et une blockchain publique

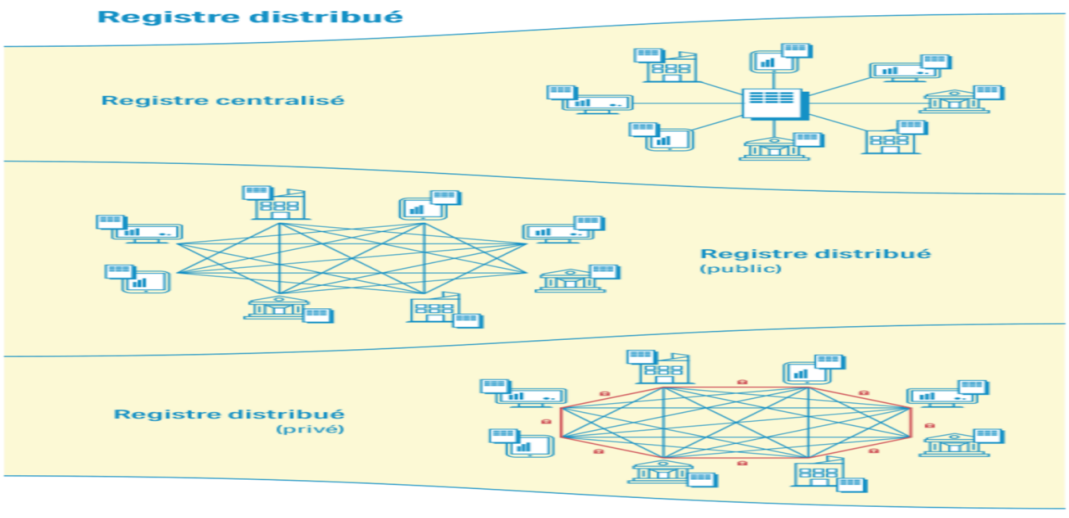
Selon M. Beelen[29], les avantages d'une blockchain privée (et par conséquent les désavantages d'une blockchain publique) peuvent être résumés de la manière suivante : dans une blockchain privée ou de consortium, la confidentialité des informations inscrites dans la chaîne est réellement de mise vu que l'on peut restreindre l'accès à certains participants – contrairement à une blockchain publique où l'intégralité des informations est transparente, vérifiable par l'ensemble du réseau.

Par ailleurs, le protocole de consensus est parfaitement malléable aux besoins des spécificités, alors que dans une blockchain publique, il est fixe et inamovible.

De plus, la survenance d'une attaque externe est pratiquement inexistante vu que l'on connaît l'identité de chaque participant.

Ensuite, les coûts afférents à une blockchain privée sont moindres car l'information est validée et vérifiée par un moins grand nombre de nœuds validateurs. De plus, un plus petit nombre de nœuds signifie que son mode de fonctionnement sera forcément plus rapide et plus performant que dans les blockchains publiques.

À titre d'illustration[30], voyez ici une image reprenant les concepts d'« institution centralisée », « blockchains publiques » et de « blockchains privées/de consortium » :



[28] A., BEELEN, *op. cit.*, p. 35 ; J., SÉNÉCHAL, « blockchains « publiques », smart contracts, organisations autonomes décentralisées et gouvernance » in Cotiga-Raccah, A. et al. (dir.), *op. cit.*, 1e édition, Bruxelles, Larcier, 2020, p. 53.

[29] A., BEELEN, *op. cit.*, p. 35.

[30] A., BEELEN, *op. cit.*, p. 36.

2. Choix d'un protocole de consensus

Une partie entière de la présente contribution sera dédiée à l'analyse de ce concept lorsque nous développerons le fonctionnement technique des blockchains, voyez *infra* (p. 17).

Le choix d'un protocole plutôt qu'un autre muni les blockchains de certaines caractéristiques que l'on ne retrouve pas forcément dans toutes les blockchains.

3) Fonctionnement technique

Pour rappel, une blockchain est « une structure de stockage d'information, sous forme de blocs de données chaînés entre eux. Cette structure de stockage est répliquée sur des nœuds, formant ce qui est communément appelé un registre décentralisé (DLT – *Distributed Ledger Technology*). Les nœuds sont organisés en un réseau P2P – *peer-to-peer* – dans lequel il n'existe pas d'autorité centrale, mais au contraire, dans lequel le contrôle est exercé conjointement par tous les nœuds. »[31]

En d'autres termes, les blocs d'informations forment une chaine où chaque nouveau bloc vient s'attacher aux anciens pour être ensuite répliqués sur tous les nœuds du réseau informatique sans qu'aucune autorité centrale n'ait le contrôle. La somme des nœuds/réseaux forme un registre décentralisé.

Cependant, si une blockchain est bien décentralisée sans autorité de contrôle centrale, elle n'est pour autant pas dépourvue d'un certain type de gouvernance. En effet, l'ensemble des nœuds composant un réseau informatique et plus largement une blockchain se doivent de suivre une certaine politique de conduite afin de valider ou de refuser les transactions/informations contenues dans les blocs, formant la chaine. Cette gouvernance est appelée « protocole de consensus »[32].

1. La gouvernance

Avec le caractère décentralisé des blockchains, se pose la question de savoir à qui ou comment valider ou refuser l'ajout d'une transaction dans un bloc. En effet, le pouvoir de décision n'étant plus centralisé, il revient donc à l'intégralité du réseau de décider du sort des inscriptions de transactions au sein des blocs.

En pratique, trois grandes interrogations se posent. Premièrement, comment valider les transactions tout en vérifiant leur légitimité et leur authenticité ? Deuxièmement, comment s'assurer de la cohérence des copies contenant les transactions entre chaque nœud du réseau ?

---

[31] J.-N., COLIN, *op. cit.*, p.10.
[32] Ibidem.

Troisièmement, comment garantir la continuité du système et cela même en présence de nœuds malicieux ou défaillants[33] ?

C'est le type de gouvernance choisi qui détermine la réponse à ces questions. Concrètement, lors de la programmation initiale d'une blockchain, le ou les développeurs conviennent d'un mode de fonctionnement qu'ils inscrivent dans le code source de la blockchain. Une fois mise en place, la blockchain s'exécutera d'elle-même et répondra aux différentes questions selon le mode de gouvernance choisi.

Cependant Madame Sénéchal est plus nuancée sur le concept de gouvernance. Selon elle, la gouvernance serait certes mi-algorithmique de par l'utilisation d'un protocole de consensus mais elle serait également mi-humaine. En effet[34], cela tient, selon la chercheuse, principalement à trois raisons :

« Tout d'abord, le consensus algorithmique ne fonctionne, en matière de blockchains, que couplé à des incitations financières qui induisent des aspects humains, communautaires et sociaux dans la validation des blocs.

En second lieu, une gouvernance hors chaîne opérée par la communauté épistémique chargée de la maintenance, de la préservation et de l'évolution de la chaîne fait de nouveau apparaître l'aspect humain et communautaire de la blockchain.

En troisième lieu, certaines blockchains récentes intègrent une gouvernance sur la chaîne pour les questions de maintenance et d'évolution de la chaîne qui empruntent à des méthodes d'édiction de la règle de droit conceptualisées par des constitutionnalistes. »[35]

En ce qui nous concerne, nous nous attarderons uniquement sur la partie algorithmique de la gouvernance.

2. Le minage et les mineurs

Le « minage », ou *mining* en anglais, est le procédé par lequel un bloc est constitué via l'inscription de plusieurs transactions en son sein. Le bloc est formé et peut venir se greffer aux blocs précédents continuant ainsi la chaîne[36]. À titre d'illustration, un bloc est formé plus ou moins toutes les dix minutes au sein de la blockchain Bitcoin[37].

Le « mineur » est le nœud du réseau qui valide et forme définitivement un bloc, cela suivant les règles de gouvernance et celles du protocole de consensus dont nous parlerons *infra*[38].

Une fois le bloc miné, il est transmis à l'intégralité des autres nœuds du réseau pour que ceux-ci puissent à leur tour vérifier son authenticité et la véracité des transactions inscrites dans le bloc. Les autres nœuds du réseau veilleront aussi à venir rajouter le bloc miné à leur propre

---

33 J.-N., COLIN, *op. cit.*, p. 18.
34 J., SÉNÉCHAL, *op. cit.*, p. 53.
35 J., SÉNÉCHAL, *op. cit.*, p. 59-60.
36 J.-N., COLIN, *op. cit.*, p. 19.
37 J.-N., COLIN, *op. cit.*, p. 23; A., BEELEN, *op. cit.*, p. 51.
38 J.-N., COLIN, *op. cit.*, p. 23; Voyez p. 17 et s.

copie des blocs précédemment minés[39]. Autrement dit, chaque nœud travaille égoïstement pour être le premier à créer un bloc, ce que nous développerons *infra*. Paradoxalement, l'ensemble des nœuds travaille de concours car, lorsqu'ils reçoivent un bloc miné, ils mettent fin au bloc qu'ils étaient en train de construire/valider pour venir le chainer à leur propre copie de la blockchain[40].

Pour effectuer ce travail de minage les mineurs sont récompensés par un incitant financier qui est un certain montant d'une crypto-monnaie native[41] sur une blockchain. Pour prendre un exemple, initialement, les mineurs de bitcoin recevaient un montant de 50 bitcoins à chaque bloc validé. Notons que cet incitant financier est nécessaire pour s'assurer que les mineurs vérifient les transactions[42].

Sans rentrer dans les détails, rare est la situation où deux mineurs parviennent à calculer un bloc au même moment. La conséquence d'une telle situation serait la scission de la chaîne en deux. Les nœuds du réseau choisiront à l'avenir la chaine de blocs la plus longue, choix justifié par le fait que c'est certainement cette chaine-là où il y a eu le plus de travail (entendez calcul) et qui serait donc la plus digne de confiance[43].

3. Le protocole de consensus

Il existe plusieurs types de gouvernance appelés protocole de consensus. Chacun d'eux offre certains avantages et inconvénients et répond à certaines spécificités et utilités propres à la blockchain pour laquelle ils fonctionnent.

Une décision est prise par consensus lorsque plusieurs personnes s'accordent pour donner une réponse commune à un problème ou une question. En langage informatique, on entend par consensus « une convergence vers un intérêt commun. Le consensus garantit que les nœuds s'entendent sur une demande unique ou sur une séquence de demandes : dans tout protocole de consensus, il y a deux événements : la proposition et la décision. »[44]

C'est exactement ce qui se produit au sein d'une blockchain lorsqu'un bloc est miné par un mineur et que ce bloc doit ensuite être accepté par les autres nœuds du réseau. On qualifiera d'ailleurs ce consensus par le terme de consensus « distribué »[45]. Chaque mineur est également à la base de la validation de ce bloc.

Ce protocole de consensus distribué est à notre sens la base du principe même d'une blockchain mais également à la base de son fonctionnement, outre tous les aspects techniques déjà développés et que nous continuerons à développer *infra*.

---

39 J.-N., COLIN, *op. cit.*, p. 23.
40 A., BEELEN, *op. cit.*, p. 51.
41 Voyez *infra* (p. 33), le concept de « jeton natif ».
42 E., SOTIRI, *Précis sur les crypto-monnaies*, Bertrange, Luxembourg, Legitech, 2018, p. 54.
43 J.-N., COLIN, *op. cit.*, p. 23.
44 J., SÉNÉCHAL, *op. cit.*, p. 60.
45 E., SOTIRI, *op. cit.*, p. 45.

D'une part, c'est ce qui donne l'essence de la décentralisation, du moins dans les blockchains publiques. Dans une moins forte mesure, nous avons vu que les blockchains privées/de consortium peuvent perdre de leur décentralisation.

D'autre part, ce procédé garantit la sécurité des informations inscrites sur une blockchain.

Cependant, une blockchain reste soumise à deux grands problèmes, le premier étant « l'attaque des 51 ». Nous le développerons *infra* mais, dans tous types de protocoles, il faut donner la preuve de sa bonne foi selon des mécanismes divers. Or, via ces différents mécanismes, un mineur pourrait réussir à s'accaparer plus de 50% du réseau et, par conséquent, il pourrait imposer sa vision au sein d'une blockchain en validant les transactions qu'il considère comme justes[46].

Le second problème est « l'attaque à double dépense »[47]. Surtout avec la blockchain Bitcoin, les transactions inscrites dans les blocs concernent l'envoi et la réception de crypto-monnaies bitcoin. Dans ces circonstances, la double dépense « a pour but d'effectuer une transaction dans le réseau sans pour autant dépenser ses monnaies [et est] l'action par laquelle un utilisateur dépense simultanément deux fois la même somme : une fois vers un utilisateur légitime et une fois vers un autre, généralement un portefeuille appartenant à un utilisateur malhonnête. »[48]

Cette vision du problème est plus propre aux blockchains qui utilisent le protocole de la preuve de travail et peut donc être atténuée par l'utilisation d'autres protocoles. Mais dans tous les cas, la question de la concentration du réseau par un mineur isolé ou une minorité de mineurs fera perdre aux blockchains leur caractère décentralisé[49]. Une réglementation en matière de position dominante au sein des blockchains trouve tout naturellement une raison d'exister[50]. À notre sens, c'est encore plus le cas lorsque celles-ci sont utilisées par un grand nombre de particuliers et acteurs (économiques) du milieu.

Il convient de partir du postulat que la confiance entre les nœuds n'est pas de mise. Pour que cette confiance soit restaurée, il a fallu faire appel à un algorithme dit « de consensus ». Un protocole de consensus tend à ce que les participants d'un même réseau (les nœuds) arrivent à se mettre d'accord mais surtout à se faire confiance sur ce qui doit être accepté. La validité d'une information ne reflète en rien sa véracité mais suppose simplement que le protocole de consensus ait accepté de la considérer comme valide[51].

Prenez une ville encerclée de généraux qui doivent se mettre d'accord sur la stratégie d'invasion à adopter alors qu'il existe dans leurs rangs certains félons. Leurs différents moyens de communication n'étant plus sûrs, ils vont devoir s'accorder sur les messages qu'ils acceptent

---

46 E., SOTIRI, *op. cit.*, p. 68.

47 G. O. karame, E. androulaki et S. Capkun, 2012, « Double-Spending Fast Payments in Bitcoin », in Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS '12), Association for Computing Machinery, New York, NY, USA, 906-917. DOI: https://doi.org/10.1145/2382196.2382292 .

48 E., SOTIRI, *op. cit.*, p. 71.

49 Étant entendu que certaines blockchains privées ont volontairement centralisé leur mode de gouvernance.

50 E., SOTIRI, *op. cit.*, p. 73.

51 J.-N., COLIN, *op. cit.*, p. 13; J.-P., PINTE, « La blockchain : nouveau paradigme économique et sociétal » in Cotiga-Raccah, A. et al. (dir.), *Les blockchains et les smart contracts à l'épreuve du droit*, 1e édition, Bruxelles, Larcier, 2020, p. 49.

de croire ou non. De façon imagée, c'est ce que l'on a appelé le problème des généraux byzantins[52].

Il existe principalement deux protocoles de consensus actuellement utilisés. Le premier se trouve à la base de la blockchain Bitcoin et Ethereum[53] et se nomme *Proof-of-Work* (PoW) ou preuve de travail en français (a.). Le second se nomme *Proof-of-Stake* (PoS) ou preuve d'enjeux (b.). Il existe également d'autres protocoles (c.) beaucoup moins répandus et parfois toujours à l'état d'expérimentation, voire de concept. Chaque protocole a ses forces et ses faiblesses et caractérise le fonctionnement d'une blockchain.

a. PoW

Le consensus par la « preuve de travail » (*Proof-of-Work*) est caractérisé par la réalisation d'un calcul, réalisé aux moyens de matériels informatiques[54]. Chaque nœud, lorsqu'il produit un bloc, est soumis pour ce faire à un travail qui correspond à une puissance de calcul produit. Le travail que doit fournir un nœud est une sorte de problème complexe qui doit être résolu mais dont la réponse peut être facilement vérifiable[55].

La probabilité de trouver la solution au problème est une question de chance. Ceci signifie que, pour une même force de calcul entre les nœuds, la chance est égale. Évidemment, on augmente sa chance en augmentant sa force de calcul, d'une part, en se coalisant avec d'autres mineurs et, d'autre part, en investissant dans du matériel informatique plus puissant. La charge de travail portée et consentie par le mineur prouve sa bonne foi vis-à-vis des autres mineurs et lui permet de produire un bloc[56].

L'inconvénient majeur du système *Proof-of-Work* est certainement son côté énergivore. C'est d'ailleurs souvent l'argument utilisé par les médias (avec celui sur le financement du terrorisme) contre l'utilisation du bitcoin et des crypto-monnaies en général. *De facto*, l'argument n'est pas faux, mais il y aurait lieu de le relativiser.

En effet, les installations informatiques nécessaires pour résoudre les calculs sont gourmandes en électricité et, lorsqu'un nœud du réseau résout le calcul, il faut bien se rendre compte que les autres nœuds ont, d'une certaine façon, consommé de l'électricité pour rien.

Dernière remarque : nous développions le problème de l'« attaque des 51 », qui est possible dans une blockchain *Proof-of-Work* si un nœud arrivait à prendre le contrôle de 51% du réseau. Or, on peut relativiser ceci par le fait que, premièrement, produire plus de 51% de la force de calcul serait un gouffre financier, vu l'investissement nécessaire pour acquérir le matériel

---

[52] L. lamport, R. shostak et M. pease, 1982, « The Byzantine Generals Problem », in ACM Transactions on Programming Languages and Systems (July 1982), 382-401.

[53] Pour être précis, ce n'est qu'une question de temps avant que la blockchain Ethereum se passe de la preuve de travail pour n'utiliser que la preuve d'enjeux. Voyez : https://cryptoast.fr/ethereum-selon-nouveau-calendrier-merge-attendue-19-septembre/ .

[54] Par exemple pour miner du bitcoin, les machines le plus souvent utilisées sont des machines de type ASIC's.

[55] J.-N., COLIN, *op. cit.*, p. 22.

[56] *Ibidem.*

informatique. Deuxièmement, la résolution du calcul est sans cesse de plus en plus compliquée[57].

b. PoS

Pour comprendre comment fonctionne la « preuve d'enjeu » (*Proof-of-Stake* ou PoS), il y a lieu de reprendre conceptuellement les notions de mineurs et de minage et de les remplacer par les termes « validateurs » et « validation »[58]. Cependant, le mode de validation des blocs diffère de la preuve de travail (*Proof-of-Work*).

En effet, il n'est plus question ici de se munir de matériels informatiques coûteux pour résoudre des calculs complexes afin de prouver sa bonne foi vis-à-vis du réseau, mais plutôt de prouver sa participation active en détenant un certain nombre de crypto-monnaies[59] au sein de la blockchain.

Le nœud du réseau (d'une blockchain), donc un validateur, qui souhaite participer au minage d'un bloc doit démontrer son intérêt en déposant en garantie un certain nombre de *token* (jeton), qu'il viendra bloquer au sein de la blockchain : on appelle ce procédé le *staking*[60]. En contrepartie, le nœud devient validateur et est autorisé à participer à une loterie qui déterminera qui des validateurs aura la possibilité d'établir/valider le nouveau bloc[61].

Le raisonnement pour pouvoir miner un bloc reste la même dans les deux protocoles. Plus un mineur arrive à démontrer « la preuve » de sa contribution pour calculer un bloc, plus les chances qu'il valide le bloc deviennent proportionnelles[62]. La seule différence dans le principe du PoS réside dans le fait qu'il faut être détenteur d'une crypto-monnaie.

Contrairement au *Proof-of-Work*, la preuve d'enjeux est beaucoup moins énergivore et, pour prendre le contrôle du système, il faudrait par conséquent posséder au moins 51% des crypto-monnaies en circulation. Cela est impensable vu le coût que cela représenterait et le fait que la valeur du cours de la crypto-monnaie dégringolerait instantanément dès que l'attaque serait rendue publique[63].

Cependant, un problème persiste dans les deux protocoles. En effet, à terme, on peut voir se produire une concentration du réseau dans les mains d'une minorité. Dans la preuve de travail, les mineurs doivent sans cesse apporter toujours plus de puissance de calcul ce qui élimine donc les « petits » mineurs. Dans le protocole d'enjeu, on voit que les validateurs sont ceux possédant le plus de crypto-monnaies et donc ceux possédant les moyens financiers les plus importants[64].

---

57 *Ibidem.*
58 A., Beelen, et al., *Tout sur la blockchain et ses applications*, Limal, Anthemis, 2021, p. 48.
59 *Ibidem.*
60 *Ibidem.*
61 J.-N., COLIN, *op. cit.*, p. 23.
62 E., SOTIRI, *op. cit.*, p. 57; A., BEELEN, *op. cit.*, p. 48.
63 A., BEELEN, *op. cit.*, p. 48.
64 E., SOTIRI, *op. cit.*, p. 58.; J., SÉNÉCHAL, *op. cit.*, p. 61.

c. Autres protocoles

Les deux protocoles de consensus précédemment cités ne sont pas les seuls existants. À titre d'illustration, il existe notamment la « preuve d'activité » (*Proof-of-Activity*) qui combine la PoW et la PoS. Néanmoins, aucune blockchain n'utilise cette méthode[65].

Existe aussi la « preuve par autorité » (*Proof-of-Authority*) qui délègue le pouvoir de création de blocs à certains participants spécifiques du réseau. Dans ce type de blockchain, on s'éloigne de la philosophie selon laquelle aucun nœud du réseau ne se fait confiance et selon laquelle il faut donc restaurer cette confiance aux moyens de protocoles comme la PoW ou la PoS. Ici, la confiance est présupposée en désignant certains nœuds comme étant dignes de confiance et à qui il revient de valider les blocs. Ce mode de fonctionnement est plus propice pour les blockchains privées où les acteurs du réseau se connaissent[66]. La célèbre institution bancaire JP Morgan utilise notamment ce procédé pour fluidifier et faciliter la gestion de ses fonds[67].

Or, à chaque avantage sa faiblesse ; dans ce cas-ci, l'efficacité est mise en avant au détriment de la décentralisation.

Enfin, un algorithme du nom de *Practical Byzantine Fault Tolerant*[68] propose de soumettre aux votes la validation des blocs, supprimant le caractère aléatoire que l'on retrouve dans la « preuve d'enjeu » et permettant une négociation entre les participants du réseau. De nouveau ces mécanismes sont plus propices pour des blockchains privées, composées d'un plus petit réseau [69].

4. Implication de la cryptographie

La science informatique qu'est la cryptographie est à la base du caractère sécuritaire et confidentiel d'une blockchain. L'ensemble des informations stockées et des transactions inscrites dans les fameux blocs est garanti par deux mécanismes qu'il y a lieu de combiner[70] : le chiffrement asymétrique et l'empreinte numérique.

a. Le chiffrement asymétrique

Le chiffrement est une opération visant à rendre une information inintelligible au moyen d'un algorithme et d'une clé, ceci dans le but de conserver la confidentialité de l'information. Le déchiffrement est l'opération inverse permettant de retrouver la signification d'un texte[71].

Avec le chiffrement asymétrique, tant l'émetteur d'un message que le destinataire possèdent une clé publique et une clé privée. Les clés publiques peuvent être partagées alors que les clés

---

65 E., SOTIRI, *op. cit.*, p. 58.
66 J.-N., COLIN, *op. cit*., p. 24; A., BEELEN, *op. cit*., p. 50.
67 A., Beelen, et al., *Tout sur la blockchain et ses applications*, Limal, Anthemis, 2021, p. 50.
68 J.-N., COLIN, *op. cit*., p. 24; M. Castro et B. liskov, 1999, « Practical Byzantine Fault Tolerance », in Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI '99), USENIX Association, USA, 173-186.
69 Ibidem.
70 J.-N., COLIN, *op. cit*., p. 15.
71 J.-N., COLIN, *op. cit*., p. 14.

privées ne doivent jamais être divulguées par leur propriétaire[72], le principe étant que ce qui est chiffré avec une clé publique est déchiffré avec une clé privée[73].

Concrètement, imaginons la situation dans laquelle X veut envoyer un message à Y. Dans ce cas, X va utiliser la clé publique de Y qui est accessible à tous pour chiffrer son message et Y utilisera sa clé privée qu'il se gardera de partager pour déchiffrer le message reçu par X.

À l'inverse, si X utilise sa clé privée pour envoyer un message à Y, tout le monde pourra déchiffrer le message au moyen de la clé publique de X[74].

Donc, il est possible d'accéder à la clé publique avec une clé privée mais il sera impossible d'accéder à la clé privée depuis une clé publique[75].

b. L'empreinte numérique

Sans rentrer dans les détails, l'empreinte numérique ou fonction de hachage est la conversion d'un texte intelligible en un texte inintelligible, et cela sous le couvert d'une apparence aléatoire, le but étant simplement de permettre de vérifier que deux mêmes textes ont bien la même empreinte numérique[76]. Dans le cas contraire, cela voudrait dire que les deux textes n'étaient pas les mêmes. C'est, par conséquent, ce qui donne aux transactions, inscrites dans la blockchain, leur caractère authentique.

De plus, il n'est pas possible de retrouver la version originale d'une information avec le résultat obtenu par la fonction de hachage. À noter également : une modification même minime d'une information produirait un *hash* complètement différent[77], d'où son caractère confidentiel et l'utilisation du chiffrement asymétrique vu *supra*.

C'est cette empreinte numérique qui vient remplir les blocs stockant l'information.

En définitive, c'est la combinaison du chiffrement (et du déchiffrement) asymétrique et de l'empreinte numérique qui assurent l'authenticité, la confidentialité et la sécurité des informations sur une blockchain.

De plus, la cryptographie n'est basée que sur les mathématiques, ce qui permet un peu plus de s'éloigner d'un tiers de confiance, qu'il soit étatique ou privé[78].

---

72 A., BEELEN, *op. cit*., p. 38.
73 J.-N., COLIN, *op. cit*., p. 14.
74 J.-N., COLIN, *op. cit*., p. 14
75 E., SOTIRI, *op. cit.,* p. 47.
76 J.-N., COLIN, *op. cit*., p. 14-15.
77 E., SOTIRI, *op. cit.*, p. 45 ; Rob, Sobers, "The Definitive Guide to Cryptographique Hash Functions (Part II)" *Varonis,* 14 août 2012, disponible sur https://goo.gl/sg4MzW
78 A., BEELEN, *op. cit*.,, p. 39.

5. Les deux grandes fonctions de la technologie blockchain

a. La fonction de stockage

Une blockchain se différencie des bases de données classiques en ce sens qu'on ne peut qu'y ajouter de l'information. Chaque transaction est inscrite à la suite de la transaction précédente, formant ainsi une chaine successive de transactions qui *in fine* composera un bloc, au contraire des bases de données habituelles où l'on peut aisément venir supprimer, modifier ou ajouter une information. La rectification d'une information dans une blockchain se fera donc par l'ajout d'une nouvelle transaction en fin de chaine[79]. C'est donc en comparant deux transactions (entendez empreintes numériques) que l'on peut se rendre compte d'une modification. C'est également ce procédé qui permet de dire qu'une blockchain est transparente car l'information est vérifiable par tous et aucune manipulation ne peut être faite à l'insu du réseau.

Ces fameuses transactions sont l'essence même des informations inscrites dans un bloc constituant une blockchain. Concrètement, les natures de ces transactions sont aussi diverses que variées et souvent propres à la spécificité d'une blockchain.

Par exemple, la blockchain Bitcoin n'est conçue que pour envoyer ou recevoir du bitcoin entre deux utilisateurs sans tiers de confiance. Cela veut donc dire que l'intégralité des transactions constituant les blocs de cette blockchain ne comprend que des transactions où l'on peut lire que X a reçu un montant de 10 bitcoins provenant de Y. Voilà donc un type de transactions propre à une blockchain.

L'on pourrait imaginer une blockchain propre au système de vote belge où l'intégralité des transactions concernerait uniquement le choix des citoyens belges pour un candidat. La transaction serait donc le vote émis, rendue illisible par les moyens cryptographiques et rendue confidentielle par l'utilisation d'une clé publique et privée, le tout sécurisé par la blockchain.

b. La fonction d'exploitation

Nous avons commencé le début de cette contribution en ne présentant que la fonction de stockage que pouvait offrir une blockchain. Or, suite aux récentes évolutions[80] de la technologie, il est désormais possible d'exécuter des programmes informatiques de manière automatisée. Ceux-ci sont appelés *smart contracts*[81] et sont déjà d'une certaine manière une autre forme d'application que la blockchain tend à offrir.

(i) Au sens technique

Un *smart contract* est « un code informatique enregistré dans une blockchain dont l'exécution est déclenchée par une transaction et dont le résultat est soumis au consensus des nœuds validateurs avant enregistrement dans le nouveau bloc. L'exécution d'un *smart contract* se

---

79 J.-N., COLIN, *op. cit.*, p. 16.

80 Notons que l'expression *smart contract* est attribuée à Nick Szabo et remonte aux années 1990 : N. SZABO, « Smart Contracts : formalizing and Securing Public networks», First Monday, septembre 1997, n° 9 : « *smart contracts combine protocols with user interfaces to formalize and secure relationships over computer networks. Objectives and principles for the design of these systems are derived from legal principles, economic theory, and theories of reliable and secure protocols* ».

81 J.-N., COLIN, *op. cit.*, p. 11.

déroule automatiquement dans un environnement d'exécution fourni par la blockchain. Le *smart contract* n'a rien d'un contrat au sens juridique du terme, même s'il peut, le cas échéant, être utilisé pour transcrire juridiquement une clause afin de l'exécuter de façon automatique. »[82]

Autrement dit, le *smart contract* est un programme informatique installé sur une blockchain qui s'exécutera automatiquement lorsque ses conditions de réalisation seront remplies. Rien ne peut venir empêcher sa réalisation si ce n'est la non-réalisation d'une des conditions contenues dans le programme informatique[83].

Un exemple assez simple est celui du prêt. Prenons X qui prête à Y un montant de 100. Y, lui, s'engage à rembourser X tous les mois, pendant un an, en plus d'un intérêt préalablement défini. Une fois l'ensemble des informations inscrites dans le *smart contract* et la prestation accomplie, les transactions financières sous-jacentes se feront automatiquement sans aucune autre intervention[84]. De plus, à la différence d'un virement bancaire qui dépend du bon vouloir de la banque, ici, le montant est préalablement bloqué dans le code informatique[85].

Les *smart contracts* trouvent de parfaites applications dans le domaine des transactions financières. Cependant, et c'est là, à notre sens, l'intérêt réel de cette application, qu'en est-il lorsque les informations contenues dans les *smart contracts* doivent provenir de sources extérieures à la blockchain ?

En effet, dans l'exemple du prêt, de simples données chiffrées (« objectives ») étaient à la base du *smart contract* : il suffisait donc d'encoder les informations et celles-ci faisaient partie intégrante du *smart contract*[86]. Or, il est des situations où l'information contenue dans le *smart contract* doit provenir du monde extérieur[87] ; on parlera alors d'informations hors chaîne. C'est là qu'entre en jeu le rôle des *Oracles*[88].

Un oracle est un « lien interface de la blockchain avec une source de données provenant du monde physique réel pour intégrer des informations dans le monde virtuel de la blockchain. »[89] L'oracle peut-être une personne physique (un juriste ?), une personne morale, un opérateur de plateforme en ligne[90], des capteurs, un réseau internet, etc. L'information émise par l'oracle est de toute nature : indice financier, température, niveau de l'eau dans une piscine, réception d'un colis par une agence de livraison.

---

82 A., BEELEN, *op. cit*.,, p. 154 ; Voyez également J., SÉNÉCHAL, *op. cit.*, p. 54 ; H., JACQUEMIN, et A., CASSART, « Les blockchains et les smart contracts en droit belge des obligations » in Cotiga-Raccah, A. et al. (dir.), Les blockchains et les smart contracts à l'épreuve du droit, 1e édition, Bruxelles, Larcier, 2020, p. 150-151.

83 E., SOTIRI, *op. cit.,* p. 79; Simont, POLROT, « "Smart contract", ou le contrat auto-exécutant", Ethereum, 20 mars 2016, disponible sur https://goo.gl/RHG1t1; A., BEELEN, *op. cit*.,, p. 42.

84 J.-N., COLIN, *op. cit*., p. 25.

85 E., SOTIRI, *op. cit.,* p. 79.

86 E. MELCHIOR, « Réflexions juridiques autour de la blockchain : analyse sous l'angle du droit des contrats », op. cit., n° 72, p. 52.

87 H., JACQUEMIN, et A., CASSART, *op. cit.*, p. 155.

88 Pour de plus amples informations sur la nature juridique des oracles et de leurs relations avec les *smart contract* voyez : H., JACQUEMIN, et A., CASSART, « Les blockchains et les smart contracts en droit belge des obligations » in Cotiga-Raccah, A. et al. (dir.), Les blockchains et les smart contracts à l'épreuve du droit, 1e édition, Bruxelles, Larcier, 2020, p. 137-184

89 A., BEELEN, *op. cit*., p. 153.

90 J., SÉNÉCHAL, *op. cit.*, p. 68.

Reprenons un exemple très souvent utilisé dans le domaine des assurances. Imaginons que vous souscrivez une assurance encodée dans un *smart contract* installé sur la blockchain Ethereum. L'assurance vous indemnise automatiquement si votre avion est en retard ou s'il est annulé sans qu'aucune demande de réclamation ne soit envoyée. Jusque-là c'est le principe même du *smart contract*. Or dans ce cas-ci, le *smart contract* a dû être informé du retard ou de l'annulation du vol, ce qui a été fait par l'oracle, c'est-à-dire ce tiers indépendant des parties qui a prévenu la blockchain que l'événement s'est produit. Dans notre exemple, ce sont les organes de contrôles supervisant les horaires des avions qui remplissent le rôle d'oracle[91].

(ii) Au sens juridique

L'analogie juridique entre les *smart contracts* et ceux visés par l'article 1101 du Code Civil[92] ne semble pas être de mise. D'abord, la qualification juridique du *smart contract* ne peut se faire en l'absence de législation plus spécifique. N'oublions pas que, dans les faits, il ne s'agit que d'un code informatique[93].

À notre sens, le fait que les *smart contracts* ne soient techniquement qu'un code informatique n'enlève rien à l'interprétation contractuelle que l'on pourrait en faire, et cela suivant une interprétation évolutive des contrats. De plus, l'exécution automatisée d'un contrat juridique est tout à fait envisageable[94]. Une partie de la doctrine pense qu'en formalisant les termes contractuels, on réduirait les problèmes d'interprétation et de malentendus. On permettrait d'être plus rapide et cela grâce au fait que l'on puisse puiser dans une collection de *smart contracts* déjà utilisés par le passé. Enfin, l'intégralité des évènements réalisés du *smart contract* sera consultable et ne laissera aucun doute quant à la preuve de leur survenance[95].

Ensuite, la majeure partie de la doctrine considère, à juste titre selon nous, qu'un *smart contract* n'est aujourd'hui pas encore l'égal d'une relation contractuelle classique, et ce pour plusieurs raisons.

Pour commencer, la sémantique des termes « *smart* » et « *contract* » recouvre des réalités différentes de ce que nous entendons par une véritable relation contractuelle. Le mot « *smart* » renvoie au code informatique qui rend automatique la réalisation du contrat une fois les conditions remplies. Cette automatisation n'a donc rien d'intelligent ou de *smart*. Ce n'est donc qu'un moyen d'exécution d'obligations sans que les parties puissent interférer en refusant, retardant ou en exécutant mal une obligation[96].

Toutes les situations juridiques ne se prêtent pas pour autant à un *smart contract*. Il est des contrats juridiques qui amènent des constructions complexes, où le facteur temps joue un rôle important et où l'ajout de nuances subjectives ne pourra rencontrer l'automatisation d'un *smart*

---

91 A., BEELEN, *op. cit*., p. 42.
92 Loi du 21 mars 1804, ancien Code Civil , *M.B.,* 21 mars 1804.
93 E., SOTIRI, *op. cit.,* p. 80.
94 J., SÉNÉCHAL, *op. cit.*, p. 68.
95 J., SÉNÉCHAL, *op. cit.,* p. 69.
96 H., JACQUEMIN, et A., CASSART, *op. cit.*, p. 154.

contract. Le rôle d'un juriste humain sera dès lors indéniable[97]. En effet, « le smart contract ne gère ni l'imprévu, ni l'imprévision »[98].

Ensuite, le terme « *contract* » qui concerne le langage juridique concrètement utilisé devra faire preuve de certaines garanties en cas de dysfonctionnement ou d'insuffisance du *smart contract*[99]. Une grande partie des questions juridiques devront résoudre l'ensemble des questions qu'un *smart contract* amènerait s'il venait à être non suffisant pour la réalisation du contrat en cause. Il est également possible que le *smart contract* soit soumis à un défaut de programmation[100]. En effet, n'oublions pas qu'une des spécificités techniques des blockchains est l'irréversibilité des informations ajoutées. Il est donc primordial d'écrire correctement un *smart contract* car, une fois déployé sur le réseau, il ne sera pas possible de revenir dessus[101]. D'où l'importance de programmeurs et de juristes spécialisés dans le domaine[102].

Enfin, une des dernières questions à résoudre serait l'exécution d'un contrat. La question semble moyennement réglée pour tout ce qui touche à des transactions financières (encore que, sur les blockchains, on ne retrouve que de la crypto-monnaies et non de l'argent ayant cours légal). Cependant, la Banque Centrale Européenne vient récemment d'annoncer la création d'un euro-numérique[103]. Par contre, qu'en est-il de l'exécution forcée en nature ?

Tant de questions qui ne permettent pas aujourd'hui de trouver dans les *smart contracts* une véritable correspondance avec les relations contractuelles que nous connaissons. Quoi qu'il en soit, il convient d'agir avec prudence dans la qualification juridique du terme *smart contract* vu l'absence de législation qui l'entoure.

Cette capacité d'exploitation offerte par les *smart contracts* rencontre les mêmes exigences de vérifiabilité, de transparence, d'authenticité et de sécurité offerte par la fonction de stockage. Ces deux fonctions sont donc bien sous-tendues par la technologie blockchain.

Dernière remarque : nous évoquions que certaines caractéristiques dites « secondaires » étaient propres à certaines blockchains, ce qui fait donc la particularité d'une chaine de blocs vis-à-vis d'une autre. La particularité de la blockchain Bitcoin est qu'elle n'est conçue que pour un seul type de transactions (l'envoi et la réception de bitcoin). En effet, son langage de programmation n'a pas été conçu pour pouvoir y installer des *smart contract*. Il faudra attendre 2014 et la création de la blockchain Ethereum, par son fondateur Vitalik Buterin[104], pour voir se développer cette fonction d'exploitation basée sur les *smart contracts*.

---

97 J., SÉNÉCHAL, *op. cit*., p. 69.

98 H., JACQUEMIN, et A., CASSART, *op. cit.*, p. 155 ; M., MEKKI, « Le contrat, objet des smart contracts (partie 1) », op. cit., pp. 409 et s.

99 E., SOTIRI, *op. cit.,* p. 81.

100 J., SÉNÉCHAL, *op. cit.*, p. 69.

101 A., BEELEN, *op. cit*.,, p.44 ; J., SÉNÉCHAL, *op. cit*., p. 71.

102 C., LEVENEUR, *Le rôle des professions juridiques face à la blockchain,* in « Tout sur la blockchain et ses applications », Limal, Anthemis, 2021, p. 87-88.

103 https://www.ecb.europa.eu/paym/digital_euro/html/index.fr.html .

104 A., BEELEN, *op. cit.*, p. 42 et 56 ; https://www.ethereum-france.com/livre-blanc-white-paper-ethereum-traduction-francaise/ (https://cutt.ly/ixZGN8u).

6. Différents concepts basés sur la même technologie

La dernière grande précision à apporter, pour clôturer ce modeste tour d'horizon technique, est la notion de « stratification[105] des technologies » autour d'une blockchain.

Depuis le début de cette contribution, nous tentons de développer le fonctionnement global d'une blockchain tout en complexifiant celui-ci par l'ajout de différents concepts. Cet ajout de concepts est dû au fait que, depuis le lancement de la blockchain Bitcoin en 2008, cette technologie n'a eu de cesse d'évoluer.

Nous avons passé en revue la notion de transaction au sein d'un bloc composant une blockchain. Par la suite, nous nous somme étendus sur le concept technologique de *smart contract.* Maintenant nous allons présenter, rapidement, ce qu'est une *DAO* ou *Decentralized Autonomous Organisation.*

Les DAO sont des organisations où tout est réglé par l'intermédiaire de *smart contracts*[106]. En vulgarisant à l'extrême, les DAO sont l'ensemble des applications formées par des *smart contracts* et reposant sur la technologie d'une blockchain, applications gouvernées de façon mi-algorithmique, mi-humaine, mi-communautaire, mi-automatisée[107]. L'ensemble des applications formées par les DAO forme ce que l'on appelle des « écosystèmes ».

Au sein des écosystèmes, on retrouve tout un tas d'applications comme des *wallet* permettant de conserver une crypto-monnaie, des jeux, ou encore des plateformes dites « de finances décentralisées ». Toutes ces applications ont la particularité d'être propre à une blockchain et de fonctionner avec une crypto-monnaie spécifique. L'étape suivante est la possibilité de venir connecter l'ensemble de ces écosystèmes entre eux. Cette étape s'appelle l'interopérabilité entre les blockchains.

4) Nouveau paradigme idéologique et juridique

Avec la technologie blockchain, le changement de paradigme se retrouve tant au niveau économique et sociétal que juridique. Pour les besoins de cette contribution, nous analyserons spécifiquement les mutations au sein du monde juridique. En effet, les changements que la technologie opère tant dans l'économie que dans notre société pourraient faire l'objet d'analyses distinctes qui sortiraient du cadre que nous nous sommes fixé, à savoir l'analyse de quelques aspects juridiques.

Nous l'avons vu, la décentralisation qu'opère la technologie blockchain supprime *de facto* l'utilité d'un tiers de confiance. Quid alors du rôle des professions juridiques, qui sont par essence des tiers de confiance ?

Idéologiquement et initialement, la technologie Bitcoin est le produit d'un mouvement libertarien qui prend racine dans les années 1990 avec la communauté dit des « cypherpunks ».

---

[105] J., SÉNÉCHAL, *op. cit.*, p. 51.
[106] A., BEELEN, *op. cit.*, p. 42.
[107] J., SÉNÉCHAL, *op. cit.*, p. 74.

Communauté largement composée de mathématiciens, cryptographes, informaticiens ou encore de hackers, elle défend les idées de protection de la vie privée en ligne et surtout tend à réduire au maximum le pouvoir d'intrusion, dans la vie des individus, qu'ont les états et les entreprises privées[108].

Concrètement, la « désintermédiation », qui peut être définie comme « le phénomène économique favorisé par l'émergence d'internet et de l'économie des plateformes et se traduisant par la réduction, voire la suppression des intermédiaires dans un circuit de distribution »[109] est, selon Madame Leveneur, « le but annoncé et recherché du recours à la blockchain ». Par conséquent « la digitalisation et l'utilisation de blockchains pourraient ainsi avoir pour effet de supprimer certaines professions, par exemples les greffes qui délivrent des documents sans aucune prestation de conseil ou de contrôle concret des situations. De manière générale, toute activité du marché du droit consistant à gérer des registres ou certifier qu'un document est conforme à un original (ou délivrer la copie d'un original) pourrait être utilement remplacée par un cas d'usage de blockchain, permettant à la fois des gains de temps et d'argent pour les usagers. »[110]

Néanmoins, il y a lieu de relativiser ce concept de désintermédiation en y apportant deux remarques. D'une part, il s'avère que la philosophie libertarienne prône plutôt une désinstitutionalisation qu'une véritable désintermédiation. D'autre part et en pratique, on voit finalement apparaître des intermédiaires propres aux blockchains. En effet, vous l'aurez compris, l'utilisation concrète de cette technologie n'est rendue possible que par l'implication de programmateurs qui rendent accessibles les applications permises par la blockchain. De plus, ces applications sont *in fine* conçues et détenue par des start up qui pour la plupart ressemblent déjà bien plus à de grandes entreprises privées qu'à des petits acteurs isolés[111].

Prenons un exemple pour illustrer nos dires. Il existe deux façons de se procurer une crypto-monnaie : soit en minant celle-ci et en étant donc récompensé par le protocole de consensus qui vous reverse un certain montant crypto-monnaie, soit en passant par une plateforme d'échange qui vous propose de convertir votre argent ayant cours légal en une crypto-monnaie. Cette plateforme, ou *exchange* en anglais, est créée par des entreprises privées et détient en plus les fonds que vous avez déposés dessus (il existe des moyens pour vous rendre entièrement détenteur de vos crypto-monnaie). Finalement, par l'implication (nécessaire) de nouveaux intermédiaires dans l'écosystème des blockchains, la désintermédiation tend à être relativisée.

Lorsque nous avons présenté la fonction d'exploitation ainsi que l'utilisation des *smart contracts*, nous avons également mentionné la notion d'« Oracle ». Pour rappel, le *smart contract* est un programme informatique automatique, déployé sur une blockchain, qui se réalise suivant différentes conditions. La réalisation des conditions est dûe à l'inscription d'informations, ces informations étant soit directement inscrites dans le programme du *smart contract* (on parlera de données *on-chain*), soit produites par les fameux oracles qui doivent

---

[108] C., LEVENEUR, *op. cit.*, p. 82.
[109] C. E., « Puissance publique et plateformes numériques : accompagner l'«ubérisation» », Étude annuelle 2017, 13 juillet 2017, p. 26.
[110] C., LEVENEUR, *op. cit.*, p. 82.
[111] *Op. cit.*, p. 83-84.

faire le lien entre le *smart contract* et l'information provenant du monde extérieur (on parlera de données *off-chain*).

Il est donc légitime de croire que l'ensemble des informations proprement juridiques soit délégué à des oracles ayant les capacités juridiques nécessaires et la formation de juriste adéquate pour attester et contrôler la véracité des informations inscrites sur un *smart contract*.

Les notaires avec leur rôle de certification se placent au premier plan avec une technologie comme celle-ci. L'inscription testamentaire et la réalisation de celle-ci par la concrétisation de conditions prédéfinies en est un exemple concret. L'authentification d'un acte de vente en est un autre[112]. Les huissiers pourraient également être « les gardiens de la viabilité numérique de l'entrée des données lors de l'ancrage du smart contract. »[113] Nous pensons également que les avocats dans leur rôle de construction contractuelle auront sans aucun doute la lourde tâche d'être rédacteur de *smart contract* quand celui-ci est enclin à être plus complexe que la simple réalisation de conditions chiffrées. L'on pourrait dès lors se demander si, pour les contrats les plus complexes, il est utile de les rendre entièrement programmables.

Quoi qu'il en soit, à l'heure actuelle, il est déjà rendu possible d'allier blockchain et profession juridique. En droit de la propriété intellectuelle, la blockchain permet d'enregistrer la preuve d'existence d'une création quelle qu'elle soit et cela à n'importe quelle étape du processus de création. Le travail précontentieux est alors facilité pour l'avocat par l'apport de preuves infalsifiables jusque-là inexistantes. En cas de contentieux, le recours à un huissier permettrait de démontrer au juge que les fichiers numériques qui lui sont présentés correspondent bien aux empreintes numériques enregistrées sur une blockchain[114].

De façon encore plus innovante, Madame Leveneur pense qu'il serait possible de programmer des *smart contracts* pour assurer l'exécution automatique des décisions de justice, à condition, cependant, que l'exécution soit faite de manière dématérialisée.

En définitive, c'est donc bien dans la conception et la compréhension inévitable des *smart contracts* que se trouve (très) certainement l'avenir des professions juridiques. Cette révolution juridique et technique, comme toutes les révolutions d'ailleurs, ne sera pas réalisée en un temps mais sera construite par l'alliance progressive entre les juristes et leurs capacités d'analyse ainsi que la compréhension de la technologie par ceux-ci.

5) Perspectives et domaines d'application

Si, à notre sens, il est certain que la complexité technique de la technologie blockchain est utile pour comprendre la complexité pratique de son utilisation mais que notre lecteur s'obstine à refuser toute explication, nous invitons les plus pragmatiques d'entre vous à lire ce petit tour d'horizon sur ce que permet concrètement la technologie blockchain.

---

[112] *Op. cit*., p. 86. La société ContractChain réalise déjà ce type d'opération.
[113] *Op. cit*., p. 85.
[114] *Op. cit.*, p. 86.

De manière générale, la blockchain a donc comme fonction centrale d'être une base de données décentralisée avec un niveau de sécurité élevé. Cela lui permet d'être une alternative fiable pour tous les métiers qui enregistrent et authentifient des documents comme les notaires, huissiers, ou encore assureurs. Elle permettrait également de rendre obsolètes des institutions centralisées comme les administrations publiques et donc tous les prestataires de services publics fournissant des besoins de première nécessité comme la distribution de l'eau, du gaz et de l'électricité. Enfin, ce qui change avec la blockchain, c'est qu'elle met directement en relation les personnes et qu'il n'est donc plus nécessaire d'avoir des plateformes centralisées comme Airbnb, Uber ou encore Ebay qui ont comme unique plus-value de mettre en relation les gens entre eux[115]. Comme l'a très bien résumé Vitalik Buterin[116] : « Au lieu de mettre le chauffeur de taxi hors de son emploi, la blockchain met Uber hors du travail et laisse le chauffeur de taxi travailler directement avec le client »[117].

Dans le milieu éducationnel, la technologie pourrait être utilisée pour la certification des diplômes et, dans une plus large mesure, des *curriculum vitae.* Par conséquent, cela veut dire une plus grande vérifiabilité des données et également une diminution des coûts par rapport à l'archivage des données. Sans compter qu'avec la blockchain, on reste propriétaire de l'ensemble de ces données avec un certain niveau de contrôle sur celles-ci[118].

Dans le domaine de l'énergie nucléaire, la technologie de la chaine de blocs peut être utilisée pour sécuriser la réalisation de pièces constituant un réacteur nucléaire. En effet, chaque pièce pourrait être réalisée selon les normes internationales les plus élevées en suivant les indications inscrites sur une blockchain et pourrait ensuite être vérifiée. C'est d'ailleurs ce que fait déjà une entreprise active dans le milieu, du nom de *Nuclearis*[119]. Cette logique fonctionne également avec le secteur alimentaire, médical, automobile, etc.[120]

Tout ce qui touche aux secteurs de l'approvisionnement et notamment la *supply-chain* (la logistique)[121] peut également bénéficier de la techologie blockchain.

Le domaine politique pourrait également être impacté par cette nouvelle technologie. En effet, la possibilité de pouvoir voter sur une blockchain n'est certainement pas quelque chose d'illusoire. Elle existe d'ailleurs déjà en Russie[122]. Ici, la vraie question à se poser est de savoir si nous voulons un changement total de notre façon d'être gouverné. En effet, la capacité du vote sur blockchain remettrait très certainement en balance les pouvoirs étatiques d'aujourd'hui. À notre sens, il s'agit dès lors d'une question politique plutôt que technologique.

---

[115] J.-P., PINTE, *op. cit.,* p. 37.
[116] Fondateur de la blockchain Ethereum.
[117] J.-P., PINTE, *op. cit*., p. 35 ; D., TAPSCOTT et A., TAPSCOTT, « blockchain Revolution : how the technology Behind Bitcoin Is Changing Money », Business, and the World, 2016.
[118] J.-P., PINTE, *op. cit.,* p. 38 ; https://www.silicon.fr/avis-expert/blockchain-vers-une-transformation-inattendue-du-secteur-de-leducation.
[119] J.-P., PINTE, « La blockchain : nouveau paradigme économique et sociétal » in Cotiga-Raccah, A. et al. (dir.), Les blockchains et les smart contracts à l'épreuve du droit, 1e édition, Bruxelles, Larcier, 2020, p. 38 ; https://www.reddit.com/r/rootstock/comments/idzbzs/nuclearis_developed_the_first_blockchain/.
[120] A., BEELEN, *op. cit*., p. 65.
[121] A., BEELEN, *op. cit*., p. 65-66.
[122] https://fr.cryptonews.com/news/tout-savoir-sur-le-vote-via-la-blockchain-7477.htm; https://fr.cryptonews.com/news/mixed-feelings-as-russia-readies-for-landmark-blockchain-vot-6751.htm .

Outre ses applications concrètes dans différents secteurs, il y a bien lieu de comprendre que cette technologie peut également être à l'aune d'une révolution anthropologique et sociétale complète.

L'alliance entre l'intelligence artificielle (IA) et la technologie blockchain nous réserverons également beaucoup de surprises pour l'avenir. Avec sa capacité de stockage ainsi que son haut niveau de vérifiabilité, la blockchain permettrait de faire accélérer l'évolution de l'IA.

On peut encore penser à la blockchain pour tout ce qui touche à la cybersécurité vu son haut niveau de sécurité, ainsi que comme outil visant à combattre la fraude. N'oublions pas que la blockchain permet de résoudre deux problèmes fondamentaux d'internet : « le fait que les informations peuvent être copiées sans effort, ce qui les dévalue, et la perte de confiance qui en résulte lorsque les relations économiques migrent dans le cyberespace. »[123] D'où l'invention des *NFT* (*Non Fungible Token*)[124].

Néanmoins, c'est bien le monde financier qui est actuellement le secteur le plus impacté par la technologie blockchain. C'est pourquoi nous avons décidé de vous offrir un petit aperçu juridique entourant deux domaines d'application de cette technologie, propres au secteur financier : les crypto-actifs et la DeFi.

CHAPITRE 2 : LES CRYPTOS-ACTIFS ET LA DEFI : DEUX DOMAINES D'APPLICATION

Section 1 : Qu'est-ce qu'un crypto-actif ?

C'est par abus de langage ou bien par méconnaissance que nous utilisons le terme « crypto-monnaie » pour parler d'un des sujets entourant ce phénomène. Or, les crypto-monnaies ne sont qu'une des catégories d'actifs avec une utilité propre et ce parmi tant d'autres. Dans un premier temps, nous répondrons à la question de la qualification juridique d'une crypto-monnaie (*1)*). Dans un second temps, nous tenterons de donner un aperçu global des différents actifs qu'il est possible de rencontrer avec la blockchain ainsi que leurs différentes utilités (*2)*).

1) Qualification « juridique » de la crypto-monnaie ?

Une crypto-monnaie (ou jeton de paiement) est un actif natif d'une blockchain dont la finalité est d'être une valeur d'échange pour l'exécution des transactions *on chain* (réalisées sur la

[123] J.-P., PINTE, *op. cit.*, p. 31.
[124] Voyez p. 34.

blockchain)[125]. Par exemple, le bitcoin est la crypto-monnaie native de la blockchain Bitcoin. L'ensemble des transactions sur cette blockchain porte sur l'envoi et la réception de bitcoins avec comme finalité la réalisation de paiements[126]. Pour être tout à fait précis, on ne peut dire à l'heure actuelle que le bitcoin remplisse cette fonction. En effet, de par son histoire et ses caractéristiques, il tendrait plus à être une réserve de valeur comme l'or mais en version numérique.

L'unique but des crypto-monnaies est donc de permettre des transactions sans avoir à recourir à une monnaie ayant cours légal (*fiat money* en anglais), l'euro ou le dollar, par exemple. Elles n'ont donc aucune autre fonction et remplissent parfaitement leur rôle tant qu'ils sont acceptés par les deux parties[127].

Cependant, tant sur le plan économique que sur le plan juridique, la question de leur qualification comme monnaie ayant cours légal est loin d'être admise. Pour tenter une définition juridique, nous procéderons *a contrario* de ce qu'est une crypto-monnaie.

D'une part, elle ne peut être considérée comme une monnaie fiduciaire (billets et pièces, ayant cours légal). En effet, le problème majeur est la non-possibilité pour les états de pouvoir émettre une telle monnaie[128] et par conséquent avoir un contrôle sur celle-ci, surtout lorsque l'on sait comme la création monétaire est un instrument parfois plus politique qu'économique.

D'autre part, elles ne peuvent pas non plus être qualifiées de monnaies scripturales (la « vraie » monnaie électronique)[129], tout simplement car elles ne répondent pas aux conditions de ce qu'est une monnaie électronique au sens de la directive 2009/10[130]. Ces conditions manquantes sont l'absence d'un « émetteur » et le fait que les crypto-monnaies ne sont pas sous-tendues (par l'apport de fonds initiaux) par une monnaie ayant elle-même cours légal[131].

En France, la loi PACTE de 2019 définit la notion de « jeton » comme « constitue un jeton tout bien incorporel représentant, sous forme numérique, un ou plusieurs droits pouvant être émis, inscrits, conservés ou transférés au moyen d'un dispositif d'enregistrement électronique partagé permettant d'identifier, directement ou indirectement, le propriétaire dudit bien »[132] (art. L.552-2 du Code monétaire et financier).

Cette même loi qualifie les « jetons de paiement » comme des actifs numériques et sont définis à l'article L. 54-10-1 du Code monétaire et financier. Nous reviendrons ci-dessous sur la qualification juridique de certains jetons et notamment des jetons de paiement[133].

---

[125] A., BARBET-MASSIN, F., FLEURET, A., LOURMI, W. O'RORKE et C. PION, *Droit des crypto-actifs et de la blockchain*, Paris, LexisNexis, 2020, p. 205.

[126] S. NAKAMOTO, « Bitcoin : A Peer-t-Peer Electronic Cash System », 2008, disponible sur https://bitcoin.org/bitcoin.pdf.

[127] A., BARBET-MASSIN, F., FLEURET, A., LOURMI, W. O'RORKE et C. PION, *op. cit.*, p. 205.

[128] E., SOTIRI, *op. cit.,* p. 107.

[129] A., BARBET-MASSIN, F., FLEURET, A., LOURMI, W. O'RORKE et C. PION, *op. cit.,* p. 206 ; E., SOTIRI, *op. cit.*, p. 107.

[130] Directive 2009/110/CE du parlement européen et du conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, modifiant les directives 2005/60/CE et 2006/48/CE et abrogeant la directive 2000/46/CE.

[131] E., SOTIRI, *op. cit.,* p. 108.

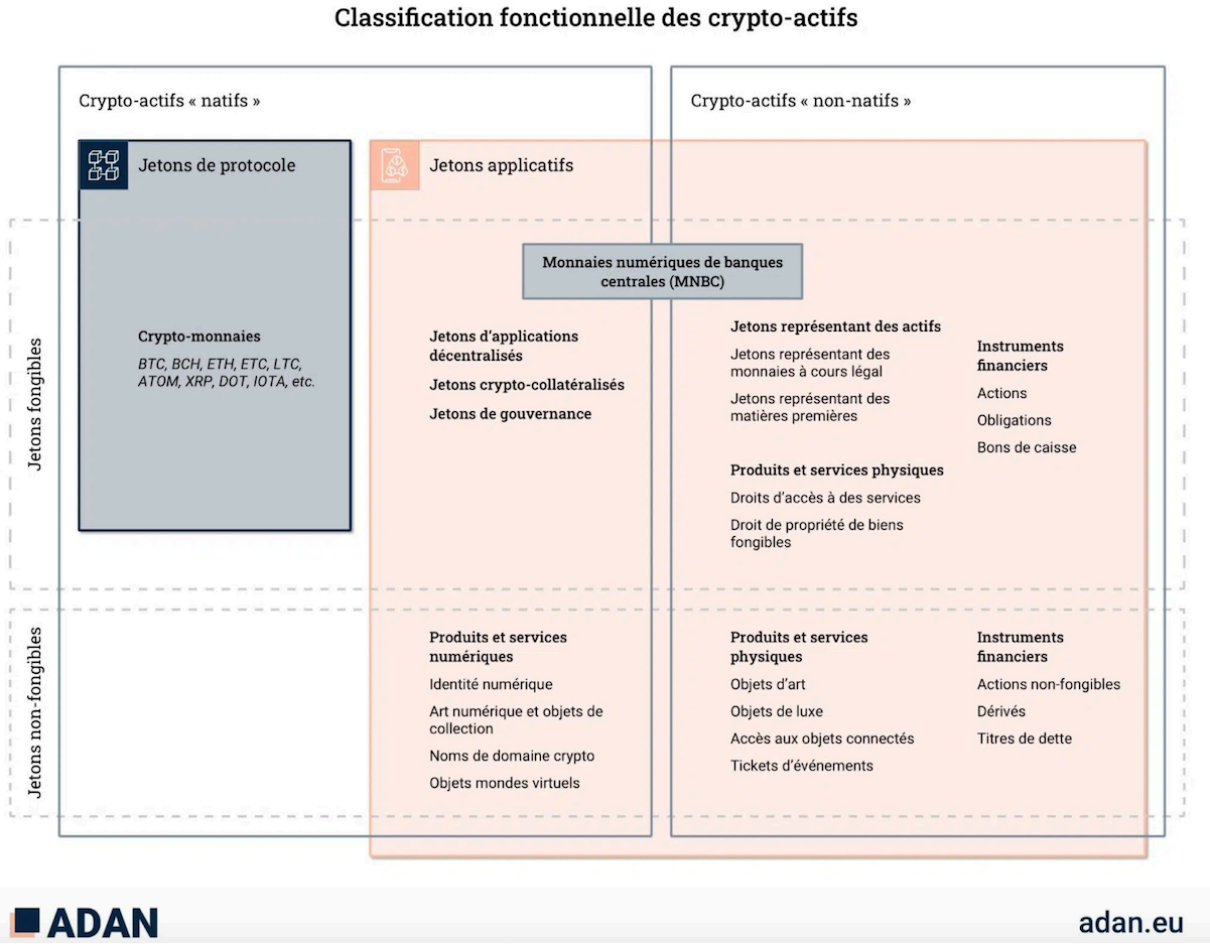
[132] LOI n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises (1), article 85.

[133] Voyez *infra*, p. 34 et 37.

2) Taxonomie des crypto-actifs sur blockchain

Par souci d'exhaustivité, nous illustrons[134] la taxonomie des crypto-actifs selon l'association française pour la défense des actifs numériques (ADAN), mais nous simplifierons notre exposé en nous focalisant juridiquement sur trois d'entre eux.

a) Suivant leurs fonctionnalités



Suivant un premier axe, on distingue les crypto-actifs « natifs » des « non-natifs ». Les premiers sont originaires d'une blockchain et tant leur utilisation que leur valeur n'a de sens que sur la blockchain à laquelle ils appartiennent. Dans notre tableau, on peut reprendre l'exemple du « jeton de gouvernance » (droit de vote) qui n'aura de sens que sur la blockchain pour laquelle il fonctionne. Un autre exemple sont les initiales *BTC* (bitcoin) qui est une crypto-monnaie propre à la blockchain Bitcoin et ne circulant que sur celle-ci. Autrement dit, les crypto-actifs

[134] Disponible sur : https://adan.eu/pedagogie/classification-crypto-actifs .

« natifs » n'ont aucune fonctionnalité en dehors de leur blockchain et ne représentent pas un droit ou un actif existant.

Les crypto-actifs « non-natifs » (ou actifs tokénisés) fonctionnent différemment : leur utilisation et leur valeur correspondent, pour une première partie, à une représentation uniquement sur blockchain et, pour l'autre partie, représentent bien un actif du « monde extérieur » donc en dehors d'une blockchain. Ce type de crypto-actif est nécessairement une représentation d'un actif ou d'un droit sous-jacent et est détenu par une personne physique ou morale. Par exemple, tous les crypto-actifs adossés à une monnaie fiduciaire ou encore ceux représentant certains droits de propriété intellectuelle voire même des biens immobiliers[135].

Suivant un deuxième axe, on distingue les « jetons de protocole » des « jetons applicatifs ». Les jetons de protocole sont également originaires d'une blockchain et sont centraux. En effet, nous avons vu *supra* qu'une blockchain fonctionnait par l'application d'un protocole de consensus quel qu'il soit et, pour faire tourner ces protocoles (par les utilisateurs), il a fallu inciter financièrement les participants d'un réseau. Les jetons de protocole sont donc des mécanismes d'incitation. Prenons l'exemple du mineur sur la blockchain Bitcoin qui vient à l'instant de résoudre le calcul demandé et donc de valider un bloc : pour le remercier de son travail, le protocole de la blockchain lui versera le montant de 6,5 *BTC*. Les jetons applicatifs sont donc tous ceux qui ne sont pas nécessaires au fonctionnement du protocole de consensus[136].

Suivant un dernier axe, on fait la distinction entre les jetons « fongibles » et « non fongibles ». Les jetons « fongibles » doivent s'entendre au sens usuel du terme à savoir interchangeable. Les « non fongible », plus connus sous le nom de *NFT (Non Fungible Token)*, sont des actifs qui ne sont pas équivalents et non interchangeables[137]. Un *NFT* est « un certificat d'authenticité numérique associé à un document numérique. »[138] Nous resterons très sommaire à ce sujet car il mériterait de faire l'objet d'une contribution à part mais ces *NFT* sont certainement l'avenir d'une des utilités de la technologie blockchain et cette fois-ci dans un sens beaucoup plus concret et pragmatique.

b) Suivant le régime juridique applicable

1. ICO

L'implication d'un cadre juridique propre et adéquat fait suite au lancement du marché des *ICO's (Initial Coins Offerings)*[139] qui connaît une croissance exponentielle en 2017-2018 avec plus de 5 milliards de dollars levés en l'espace de douze mois, contre moins de 100 millions en 2016[140].

---

[135] Disponible sur : https://adan.eu/pedagogie/classification-crypto-actifs .
[136] Disponible sur : https://adan.eu/pedagogie/classification-crypto-actifs .
[137] Disponible sur : https://adan.eu/pedagogie/classification-crypto-actifs .
[138] A., BEELEN, *op. cit.*, p. 71.
[139] Les termes d'*Initial Token Offerings* (ITO) sont également utilisés.
[140] A., BEELEN, *op. cit.*, p. 107.

Une *ICO* permet « de lever des fonds sur internet en émettant des jetons (*coins* ou *tokens*) via un dispositif d'enregistrement partagé (entendez un registre décentralisé de type blockchain, nous précisons). Elle est nommée de la sorte en raison de sa similitude avec les introductions en bourse classiques, appelées en anglais *Initial Public Offering* (IPO). Mais cette offre diffère de l'IPO en ce qui concerne la nature des droits acquis par les investisseurs. « Ainsi les détenteurs de jetons peuvent bénéficier de fruits, sous la forme de profits versés par l'émetteur et/ou d'une augmentation de la valeur de leurs jetons qu'ils pourront revendre avec une plus-value si le projet réussit ; et/ou de droit de vote ou de gouvernance ; et/ou d'un droit d'usage du bien ou du service financé [nous soulignons]. »[141].

C'est donc l'avènement des *ICO* qui a permis de faire une distinction entre, principalement, trois types de crypto-actifs voyez *infra* au point (*2.*) et se faisant, permettant une qualification juridique en fonction du crypto-actif émis par l'*ICO*.

2. Token utilitaire, de paiement ou financier

Nous avons vu *supra* la qualification juridique française du jeton qui peut être traduit littéralement en anglais par *token*. Un *token* est donc « un actif numérique émis et échangeable sur une blockchain. Trop souvent appelés « crypto-monnaies », ils n'ont pas tous vocation à devenir une monnaie. Ce sont des actifs qui permettent la représentation et l'échange de valeur sur la blockchain »[142]. Autrement dit, un jeton est un support numérique et plus précisément cryptographique qui représente un ou plusieurs droits dont peut jouir son titulaire[143]. La particularité de ce support numérique est qu'il est conservé non pas au sein d'une institution centralisée mais bien par une multiplicité de nœuds formant un registre distribué (une blockchain)[144].

C'est donc sous le vocable *token* que nous reprendrons trois catégories de crypto-actifs qu'il y a lieu d'analyser juridiquement car présentant de l'intérêt en pratique.

C'est selon la qualification de l'*International Token Standardisation Association*[145] (« ITSA ») que nous vous présentons ceux-ci.

D'abord, on retrouve les « *tokens* de paiement » (ce que l'on entend par crypto-actif « natif » et par véritable crypto-monnaie), par exemple le bitcoin. Au sein de cette catégorie, on retrouve les fameux *stablecoins* qui sont des jetons de paiement dont la spécificité est d'être adossés à un actif stable, par exemple le dollar, ce qui a pour but de limiter leur volatilité. Ces jetons

---

[141] B., FRANÇOIS, Les offres au public de jetons (Initial Coin Offerings- ICO) en droit français et en droit comparé, in « blockchain et droit des sociétés », Paris, Dalloz, 2019, p. 62.

[142] A., BEELEN, *op. cit*., p. 71.

[143] J.-M., MOULIN, M., QUINIOU, A., Gasser et G., BOUILLET-CORDONNIER (Coord.), La finance numérique : aspects juridiques et fiscaux du crowdfunding et des cryptoactifs : avec des formulaires et tutoriels digitalisés et personnalisables par Legaltech Legal Pilot, Paris, EFE Édition, 2021, p. 123.

[144] *Ibidem.*

[145] L'*International Token Standardisation Association* est une association sans but lucratif de droit allemand qui s'est fixé comme objectif de proposer une classification internationale des différents *tokens*/crypto-monnaies sur la base de quatre dimensions (économique, régulatoire, légale et technologique) (https://my.itsa.global/) ; A., BEELEN, *op. cit*., p. 107.

« stables » sont pour l'instant de nature privée (produits et adossés à des fonds privés) ce qui fait peser un risque systémique pour la stabilité financière[146]. Notons d'emblée que l'union européenne tente à son tour d'en posséder un[147].

Ensuite, on retrouve les « *tokens* utilitaires » (ou d'usage), qui permettent de recouvrir à des services proposés par une blockchain.

Enfin, on retrouve les « *tokens* financiers », ou *security tokens* en anglais, qui doivent être considérés, dans certain cas, comme de vrais instruments financiers car offrant des droits financiers (dividendes, créances...) ou politiques (votes, fonctions)[148].

Section 2 : Qu'est-ce que la finance décentralisée ou « DeFi » ?

La « finance décentralisée », ou *decentralised finance* (ci-après « DeFi », de la contraction des termes « *decentralised » et « finance »*, en anglais), devient en 2020 un pan entier et incontournable[149] du paysage blockchain[150]. Celle-ci s'oppose à la *centralised finance* (ci-après « CeFi ») qui est tout ce que l'on peut rattacher à la finance classique.

Concrètement, il ne s'agit plus comme dans la CeFi de détenir des actions, obligations placées sur un compte titre ou dans un portfolio mais bien des *tokens* (jetons), ceux-ci déposés dans un portefeuille numérique[151], appelé *wallet* en anglais. La DeFi propose également des solutions de paiement, des applications de dépôt et de prêt et même des fonds d'investissement.

Les avantages sont multiples. D'abord et principalement, on vient supprimer le fameux tiers de confiance propre aux institutions financières centralisées, ce qui signifie que tous les prêts, emprunts et échanges de crypto-monnaies ne sont plus soumis aux conditions, parfois subjectives, des institutions bancaires. Les conditions qui devront être à l'avenir respectées ont simplement trait à la capacité de remboursement de l'utilisateur, ce qui est compréhensible. Cela signifie également que, la plupart du temps, une identification de type *KYC* (*know your consumers*) n'est plus nécessaire, ce qui permet de supprimer les barrières à l'entrée, faisant *de facto* de la DeFi un endroit où l'innovation est maîtresse. Les plateformes offrant ce type de services s'appellent des *Dapps.*

Par exemple, un individu porteur d'une maladie grave se voyant refuser une assurance ou un prêt par une institution « classique » à dans la DeFi toutes les chances de voir sa demande être validée. Voilà ce que propose d'offrir les partisans de la DeFi.

Ensuite, on automatise les transactions (financières), basées sur des *smart contracts*, ce qui veut donc dire que d'une part, on permet de réduire les coûts, ce qui est bien entendu recherché par ce genre de secteurs. D'autre part, l'ensemble des transactions sont garanties par un haut niveau

---

[146] J.-M., MOULIN, M., QUINIOU, A., Gasser et G., BOUILLET-CORDONNIER (Coord.), *op. cit*., p. 126.
[147] A., BEELEN, *op. cit*., p. 91.
[148] A., BEELEN, *op. cit*., p. 107.
[149] L'industrie de la DeFi pesait plus de 1,6 milliard de dollars en 2020 ; Voyez https://defipulse.com/.
[150] A., FULWOOD, « La DeFi se déchaîne- La finance décentralisée, en plein essor, cherche ou s'accrocher. », Challenge, 6 janvier 2022, p. 143- 144.
[151] A., BEELEN, *op. cit*., p. 137.

de sécurité car basées sur la blockchain. Rappelez-vous, le réseau est distribué et constitué de nœuds qui vérifient l'intégralité des transactions. C'est d'ailleurs ce qui rend difficile le hack des *Dapps*[152] mais également le contrôle de celles-ci par la loi.

Enfin, la DeFi offre des services non-offerts par la finance classique. En permettant notamment de venir fractionner des titres, en achetant, par exemple, une partie d'action sans devoir acheter l'action en entier[153]. De plus, elle solutionne le risque de défaillances entre les parties en bloquant, au travers des *smart contracts*, la somme faisant l'objet soit d'une transaction de prêt ou d'emprunt.

Attention cependant : même si la DeFi offre des solutions intéressantes sous couvert d'une philosophie égalitaire entre tous, elle n'en est qu'à ses débuts et doit être manipulée avec précautions. En effet, les fameuses plateformes *Dapps* sont certes sous-tendues par la technologie blockchain mais leur programmation initiale est faite en dehors de celles-ci par des programmeurs parfois peu scrupuleux. Il est donc primordial qu'un certain contrôle soit opéré au minimum vis-à-vis du consommateur.

Il est également utile de souligner que l'entièreté des services dont nous parlons ne sont rendus possibles qu'avec à la base l'utilisation d'une crypto-monnaie. Sur ce point, l'on connaît la méfiance du système bancaire classique lorsqu'il s'agit de venir rapatrier certains fonds produits par la DeFi.

Mais l'argument étant le plus en sa défaveur est le fait que la DeFi ne rend aucun service à l'économie réelle. Néanmoins, il tendrait à s'estomper car, premièrement, la DeFi pourrait venir supplanter le système financier traditionnel avec l'adoption d'un jeton comme moyen de paiement. Deuxièmement, en fusionnant avec la finance traditionnelle. Troisièmement, lorsqu'une économie réelle aura su se développer sur les blockchains alors la DeFi aura trouvé son économie réelle[154].

Cependant, avant de pouvoir se prononcer sur ces différentes questions, il y a lieu de s'interroger sur les différentes qualifications juridiques qu'offrent ces nouveaux instruments financiers et, par conséquent, de voir quelles réglementations appliquer.

II. ASPECTS JURIDIQUES

Nous focaliserons notre analyse sur les cadres légaux existant autour des deux domaines d'applications dont nous venons de parler et donc, comme nous le verrons, principalement vis-à-vis d'un droit financier numérique propre.

---

[152] Cela est pourtant déjà arrivé et se produit toujours.
[153] A., BEELEN, *op. cit*., p.137.
[154] A., FULWOOD, « La DeFi se déchaîne- La finance décentralisée, en plein essor, cherche ou s'accrocher. », Challenge, 6 janvier 2022, p. 144.

Une première approche *de lege lata* sera opérée, en offrant une analyse supranationale du point de vue européen.

Une deuxième approche *de lege ferenda* sera ensuite proposée afin de proposer une évaluation critique de la situation.

CHAPITRE 1 : APPROCHE *DE LEGE LATA* EUROPÉENNE

S'il y avait, il y a encore quelque mois, lieu d'opérer l'analyse juridique des crypto-actifs de façon nationale et comparative, cela n'est dorénavant plus le cas suite aux récentes évolutions dans le domaine[155]. En effet, quatre textes ont été proposés par l'Union Européenne dans ce qu'il a été décidé d'appeler le « *digital finance package* »[156].

Section 1 : La proposition de règlement dit « MiCA »

Le 30 juin 2022 le Conseil de l'union européenne ainsi que le Parlement européen sont parvenus à un accord provisoire concernant la proposition de règlement du Parlement européen et du conseil sur les marchés de crypto-actifs, modifiant la directive (UE) 2019/1937 du 24 septembre 2020 (ci-après dénommé « MiCA » pour *Market in Crypto-Assets*)[157].

1. Objectifs

Avec un titre I, MiCA propose raisonnablement de présenter son objet ainsi que son champ d'application mais surtout de donner un cadre européen unifié sur la plupart des notions dont nous avons parlé jusqu'à présent.

Le règlement MiCA distingue, en définitive, les « crypto-actifs autres que des jetons se référant à des actifs ou que des jetons de monnaie électronique » dans son titre II des « jetons se référant à des actifs » dans son titre III et des « jetons de monnaie électronique » dans son titre IV.

Suivant cette typologie et suivant la définition que le règlement donne aux « jetons se référant à un ou des actifs »[158], nous pouvons en conclure que les crypto-actifs visés au titre II concernent les *tokens* de paiement et les *tokens* utilitaires que nous avons analysés *supra*. *De facto*, les titres III et IV visant respectivement les fameux *stablecoins* (jetons stable) et les « vrais » jetons de monnaie électronique, il peut également être dit que le règlement MiCA ne

---

155 L'analyse juridique est à jour jusqu'au 13 juillet 2022.

156 https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

157 Disponible sur : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52020PC0593

158 Article 3, paragraphe 1er , point (3) du règlement MiCA : « un type de crypto-actif qui vise à conserver une valeur stable en se référant à la valeur de plusieurs monnaies fiat qui ont cours légal, à une ou plusieurs matières premières ou à un ou plusieurs crypto-actifs, ou à une combinaison de tels actifs ».

vise pas les *tokens* financiers ou *Security token*. De plus, le champ d'application du règlement exclut clairement les crypto-actifs rentrant sous la définition des instruments financiers au sens de l'article 4, paragraphe 1, point 15), de la directive 2014/65/UE[159].

Le titre V offrira les différentes conditions d'agrément et d'exercice pour les prestataires de services sur crypto-actifs, ce qui amènera plus de transparence et de contrôle visant à prévenir les abus vis-à-vis du consommateur. Concernant les abus, un sixième titre a entièrement été dédié à cet effet.

Enfin, le dernier titre pertinent du règlement MiCA est le titre VII définissant les prérogatives des autorités compétentes.

2. Crypto-actifs visés

Le crypto-actif reçoit, finalement, une définition européenne comme étant : « une représentation numérique d'une valeur ou de droits pouvant être transférée et stockée de manière électronique, au moyen de la technologie des registres distribues ou d'une technologie similaire »[160].

MiCA régulera à l'avenir la vie des jetons utilitaires définis comme suit : « un type de crypto-actif destiné à fournir un accès numérique à un bien ou à un service, disponible sur la DLT, et uniquement accepté par l'émetteur de ce jeton »[161]. Le règlement aborde également (et surtout) les jetons de paiement (dit jetons stables) sous son titre II, vu l'importance systémique[162] de ces jetons vis-à-vis du secteur financier.

3. Les émetteurs de crypto-actifs

Avec MiCA, un plus grand contrôle sera opéré dans le domaine des crypto-actifs ; ce contrôle passe aussi par une plus grande responsabilisation des émetteurs[163] de crypto-actifs. D'une part, en ayant l'obligation de transmettre un livre blanc (*white paper* en anglais) à l'autorité des marchés nationaux[164]. Ce livre blanc aura pour but de renseigner au mieux le consommateur lors du lancement d'une *ICO*. En son article 7, l'émetteur justifiera la qualification juridique qu'il entend donner au jeton émis tout en l'excluant des autres qualifications que d'autres instruments législatifs pourraient lui donner. Cet article 7 donne également aux autorités compétentes le droit d'interdire l'offre ainsi que le droit d'obliger l'émetteur à modifier son livre blanc. Un article 12 permettra sous certaines conditions un droit de rétractation vis-à-vis du consommateur.

---

159 Article 2, paragraphe 2, point (a).
160 Article 3, paragraphe 1er, point (2) du règlement MiCA.
161 Article 3, paragraphe 1er, point (5) du règlement MiCA.
162 Voyez en ce sens l'article 39 du règlement MiCA.
163 Voyez la définition donnée par le règlement à l'article 3, paragraphe 1er, point (6) du règlement MiCA.
164 Article 5 du règlement MiCA.

D'autre part, en responsabilisant l'émetteur et en donnant par exemple un droit d'indemnisation aux clients victimes d'un préjudice[165].

4. Les prestataires de services sur crypto-actifs

En son article 3, §1, point (8), le règlement propose de définir les prestataires de services sur crypto-actifs comme « toute personne dont l'occupation ou l'activité consiste à fournir un ou plusieurs services sur crypto-actifs à des tiers à titre professionnel ». Les services en question sont listés de manière exhaustive au point (9) du même article.

Ceux-ci devront faire une demande d'agrément[166] pour les services proposés. L'agrément sera différent en fonction du jeton que l'émetteur proposera d'offrir et, en ce qui nous concerne, tous services sur les crypto-actifs seront concernés par les articles 53 à 58 dudit règlement. L'agrément fera office de passeport puisque valable sur tout le territoire européen[167].

On notera également, l'apparition d'un registre contenant l'intégralité des informations (juridiques) sur les jetons émis par un prestataire de service sur crypto-actifs européen[168].

Section 2 : Le règlement sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués

À la différence des autres textes européens, ce Règlement[169]sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués vient tout juste d'être voté (ci-après dénommé règlement DLT).

Ce règlement aura comme objectif l'encadrement de la technologie reposant sur des registres distribués (ou *distributed ledger technology* en anglais), autrement dit des infrastructures fonctionnant avec la technologie blockchain ainsi que de leurs exploitants ; on y retrouve d'ailleurs un certain nombre de conditions pour l'exploitation de tels registres[170].

Ce régime pilote vise l'ensemble des acteurs (économiques) du marché et permettrait à ceux-ci, après avoir reçu l'autorisation d'exploitation (art. 7), de pouvoir contourner certaines règlementations du droit financier classique. L'on sait en effet ce dernier plus contraignant mais parfois pas toujours adapté à certaines innovations technologiques comme les jetons financiers

---

165 Article 5 du règlement MiCA.
166 Article 53, 54 et 55 du règlement MiCA.
167 J.-M., MOULIN, M., QUINIOU, A., Gasser et G., BOUILLET-CORDONNIER (Coord.), *op. cit*., p. 163.
168 Article 57 du règlement MiCA.
169 Règlement (UE) 2022/858 du Parlement européen et du Conseil du 30 mai 2022 sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués, et modifiant les règlements (UE) no 600/2014 et (UE) no 909/2014 et la directive 2014/65/UE.
170 Article 7 et 8 du règlement DLT.

ou *security token* qui restent, suivant leurs caractéristiques, parfois soumis aux réglementations financières comme MIFID II[171] par exemple.

Section 3 : La proposition de règlement dit « TFR »

Le paquet sur la finance numérique contient également une proposition de règlement[172] visant à encadrer le rapatriement et le transfert de fonds sur crypto-actifs tout en luttant efficacement contre le blanchiment d'argent. Cette proposition aura comme objectif principal « d'imposer aux prestataires de services sur crypto-actifs l'obligation de recueillir et de rendre accessibles des données complètes sur le donneur d'ordre et le bénéficiaire des transferts d'actifs virtuels ou de crypto-actifs qu'ils traitent. C'est ce que font actuellement les prestataires de services de paiement pour les virements électroniques. Le but est d'assurer la traçabilité des transferts de crypto-actifs, afin de pouvoir mieux détecter les éventuelles transactions suspectes et, le cas échéant, de les bloquer. »[173]

Cette réglementation s'inscrit dans la même mouvance que les différentes directives concernant la prévention du délit de blanchiment d'argent.

Section 4 : La proposition de règlement sur la résilience opérationnelle numérique du secteur financier

Cette proposition[174] de règlement a pour objectif de proposer une sorte de *lex specialis* pour le secteur de la finance numérique[175]. Visant, notamment, en son article 2, « les prestataires de services sur crypto-actifs, les émetteurs de crypto-actifs, les émetteurs de jetons se référant à un ou des actifs et les émetteurs de jetons se référant à un ou des actifs et revêtant une importance significative ».

De plus, la proposition entend par « résilience opérationnelle numérique » la « capacité d'une entité financière à développer, garantir et réévaluer son intégrité opérationnelle d'un point de vue technologique en assurant directement, ou indirectement par le recours aux services de tiers prestataires de services informatiques, l'intégralité des capacités liées à l'informatique

---

[171] Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE (refonte).

[172] Proposition de règlement du Parlement européen et du Conseil du 20 juillet 2021 sur les informations accompagnant les transferts de fonds et de certains crypto-actifs (refonte).

[173] https://www.consilium.europa.eu/fr/press/press-releases/2021/12/01/anti-money-laundering-council-agrees-its-negotiating-mandate-on-transparency-of-crypto-asset-transfers/ .

[174] Proposition de règlement du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014 et (UE) no 909/2014.

[175] J.-M., MOULIN, M., QUINIOU, A., Gasser et G., BOUILLET-CORDONNIER (Coord.), *op. cit*., p. 157.

nécessaires pour garantir la sécurité des réseaux et des systèmes d'information qu'elle utilise, et qui sous-tendent la fourniture continue de services financiers et leur qualité »[176].

Par conséquent, ce cadre règlementaire vise la protection du secteur financier lorsque celui-ci peut être impacté par la défaillance du secteur financier mais numérique.

CHAPITRE 2 : APPROCHE *DE LEGE FERENDA*

Section 1 : Position de la finance traditionnelle face aux Fintechs

Dans un premier acte, a pu être constatée l'inefficacité de la réglementation spontanée du secteur *fintechs* par les régulateurs, en particulier ceux du milieu financier, ainsi que la dangerosité de la situation si le secteur *fintechs* venait à être régulé de façon bureaucratique. Par conséquent, la technique juridique utilisée était de répliquer les instruments législatifs propres au droit financier et essayer de faire correspondre ceux-ci au monde des crypto-actifs, ce qui ne pouvait être suffisant pour un secteur aussi disruptif. Néanmoins, cette absence législative est, spécialement dans le secteur des technologies, nécessaire pour pouvoir laisser à celles-ci le temps de se déployer[177], afin de ne pas tuer dans l'œuf la révolution qui était en train de se produire.

Dans un second acte, après avoir tout doucement perçu les applications que pouvait rendre possible la blockchain, principalement dans le secteur financier numérique et donc de la finance décentralisée, une période de crainte s'est installée. Déjà sous l'administration de Barack Obama, on se rendait compte du défi que serait la réglementation de l'activité des sociétés de technologies financières sous tendue par la blockchain. Aucune règle propre n'était encore définie et l'inclusion d'un cadre solide permettrait sans aucun doute l'expansion d'applications sur blockchain[178].

Dans un troisième acte, on pouvait lire dans un article publié sur le blog de Christine Lagarde en 2018, qu'« il est aussi possible de mettre en place des réglementations internationales pour les crypto-actifs, y compris les Initial Coin Offerings (ICO). L'objectif devrait être d'exploiter le potentiel des technologies sous-jacentes, tout en assurant la stabilité financière et en réduisant les risques liés au blanchiment des capitaux et au financement du terrorisme. »[179]

Dans un acte final, nous avons fait état, au niveau européen, des différents règlements et propositions de loi adoptés ou en cours de réception. Nous en déduisons deux choses : premièrement, le phénomène n'est pas ignoré et il est même pris très au sérieux par nos institutionnelles. Le choix de règlements plutôt que de directives en est un exemple.

---

[176] Article 3, point (1), de la proposition de règlement sur la résilience opérationnelle numérique.
[177] E., SOTIRI, *op. cit.*, p. 111-112.
[178] J.-P., PINTE, op. cit., p. 50.
[179] A., CASSART, « 2. - FinTech : l'art délicat de la disruption » in Cassart, A. (dir.), Le droit des MachinTech (FinTech, LegalTech, MedTech...), 1e édition, Bruxelles, Larcier, 2018, p. 80.

Deuxièmement, en plus d'être petit à petit encadré juridiquement, on peut percevoir la création d'un droit propre pour le secteur financier numérique et donc pour la technologie blockchain.

Ces fameuses *Fintechs* (de la contraction entre *Financial Technology* ou Technologies financières) sont « des entreprises visant à s'accaparer un marché économique lié aux fonctions traditionnellement dévolues aux acteurs historiques de la finance, en mettant en place des stratégies de rupture appuyées sur des développements technologiques et généralement facilitées par un carcan réglementaire plus léger. »[180] C'est donc naturellement que l'on y retrouve les services entourant les crypto-actifs et par conséquent le phénomène DeFi.

L'avènement des fintechs est, selon M. Cassart, du fait de la conjoncture de trois éléments : « des acteurs traditionnels aux positions verrouillées par les contraintes règlementaires et par la difficulté de faire advenir l'innovation en leur sein ; de nouveaux acteurs souhaitant mettre en place des stratégies inédites pour attaquer un pan de ces acteurs ; la facilité d'accès et l'abondance des technologies permettant à ces nouveaux acteurs d'implémenter leurs nouvelles stratégies. » [181]

Du point de vue économique et sectoriel, les fintechs se sont incontestablement implantées dans le paysage financier. De par les investissements massifs entrepris, les technologies utilisées (blockchain), les offres qu'elles proposent, leur utilisation dans les domaines de la finance classique, etc.[182]

Du point de vue juridique, et particulièrement en ce qui concerne nos propos, nous avons vu que l'Europe est en train de donner une accise juridique solide aux fintechs utilisant la technologie des registres distribués et donc des cryptos-actifs.

Section 2 : La résilience du droit face aux nouvelles technologies

Appréhender juridiquement une technologie nouvelle est quelque chose de particulièrement mal aisé. D'abord, il y aura lieu de se poser la question de l'intérêt de légiférer et voir si nos institutions juridiques ne sont pas déjà assez fortes pour réguler la nouvelle technologie. Ensuite, il est important d'envisager dans quelle proportionnalité il faudra encadrer une technologie et endéans quel délai. En effet, une intervention trop forte et trop précoce aura pour conséquence de venir casser l'innovation avant même qu'elle puisse se rendre utile. Enfin, et spécialement en ce qui nous concerne, il faut se demander comment légiférer une technologie qui a été pensée pour justement être décentralisée et donc ne pas se soucier des frontières ou d'un pouvoir souverain. Telles sont les questions que le droit devra résoudre afin d'offrir un cadre juridique adéquat.

Selon nous, deux types de règles pourraient coexister afin de donner le cadre juridique le plus pertinent qui soit pour la technologie blockchain. Nous appellerons ces règles des « règles internes » et des « règles externes ».

---

[180] A., CASSART, *op. cit.*, p. 85.
[181] A., CASSART, *op. cit.*, p. 82.
[182] https://www.ey.com/en_lu/assurance/fintechs-de-nouvelles-opportunites-pour-le-secteur-bancaire .

Comme nous l'avons expliqué, la gouvernance d'une blockchain est composée d'un protocole de consensus qui, une fois lancé, se régule par lui-même. Par conséquent, une blockchain est son propre régulateur, ce qui nous fait penser à la célèbre phrase de Lawrence lessing : « *Code Is Law* »[183]. Il serait donc vain de proposer un cadre législatif à la blockchain, étant auto-suffisante et ayant comme fondement philosophique la non-centralisation par des acteurs uniques. Une certaine analogie peut être faite entre l'ère d'internet et la technologie blockchain en ce sens qu'il ne s'agit pas tant de réguler la technique mais bien les activités déployées grâce à cette technique[184].

Le problème de la régulation des règles internes d'une blockchain est particulièrement vite résolu lorsque cette blockchain est privée. Rappelons-le, une blockchain privée a comme particularité d'avoir été négociée contractuellement entre ses différents acteurs[185]. Cela nous permet d'avancer que le fondateur d'une blockchain n'a finalement qu'à s'en remettre aux concepts de « supplétivité » et « impérativité » des normes ainsi qu'au droit des contrats lorsqu'il lie des participants à sa blockchain.

Cela nous amène dès lors à des règles régulant les activités que nous dénommerons « règles externes ». Nous nous efforcerons simplement d'expliquer un principe qui peut être utilisé pour la création d'une série de règles propres à une myriade de secteurs différents.

Circonscrire l'ensemble des activités déployées sur une blockchain avec des règles *sui generis* précises aurait pour effet de devoir légiférer dès qu'un changement majeur dans un procédé technique viendrait à être modifié ou découvert. C'est le concept de « neutralité technologique » qui doit être utilisé et cela sur la base de grands principes plutôt que sur des régulations précises, difficiles à comprendre et trop réfractaires aux changements[186].

La réglementation européenne actuelle a, à notre sens, laissé le temps à la technologie blockchain de se développer pour ensuite venir, dans une première réaction législative, encadrer les activités les plus importantes et donc les crypto-actifs principalement.

---

[183] L. Lessig, Code and Other Laws of Cyberspace, New York, Basic Books, 1999, p. 24 et s.
[184] E., TREPPOZ, Quelle régulation internationale pour les blockchain ? Code is Law v. Law will become Code, in *Blockchain et droit des sociétés* , Paris, Dalloz, 2019, p. 57.
[185] E., TREPPOZ, *op. cit.*, p. 55.
[186] A., CASSART, *op. cit.*, p. 99.

CONCLUSION

Au travers de cette contribution, nous avons tenté de rendre le plus simplement possible la compréhension d'une technologie qui peut, à certains égards, être complexe. Nous avons également essayé de rendre cette technologie la plus accessible en vous présentant deux domaines d'application que nous rencontrons en pratique, c'est-à-dire les crypto-actifs et la finance décentralisée. Pour ce faire, il fallait évidemment proposer un tour d'horizon technique afin de pouvoir distinguer chaque concept, les uns à la suite des autres. De ce fait, notre première grande partie doit être analysée à la lumière d'une blockchain, comme une grande chaine de blocs conceptuelle dans laquelle chaque concept (bloc) devait nécessairement précéder les blocs nouvellement expliqués/créés.

Ensuite, un rapide tour juridique s'imposait afin, et surtout, de prouver aux lecteurs que le phénomène blockchain n'est pas sur le point de s'estomper. Certes, nous sommes qu'au début de la prise en compte par le droit de cette technologie, mais cette prise en compte est déjà bien présente et promet à l'avenir d'être en constante évolution.

Ce sont, à notre sens, les caractéristiques principales des blockchains qui ont permis de mettre en avant l'utilité de cette technologie car, si initialement elle n'était qu'un moyen de conserver de l'information, elle est devenue une façon de re-concevoir, re-façonner, re-penser nos sociétés. En effet, la décentralisation permettrait de replacer l'individu au centre sans toujours devoir passer par un tiers de confiance et, *de facto*, le mot confiance, qui manque aujourd'hui cruellement à nos sociétés, pourrait être utilisé à sa juste valeur.

Finalement, le retour en arrière n'apparait pas possible ; nous pensons sincèrement que cette technologie a du potentiel et continuera à faire parler d'elle notamment en étant prise en considération par nos institutions juridiques. Par contre, à la question de savoir si la blockchain influencera beaucoup ou peu nos vies, il conviendrait de laisser le temps passer pour y répondre.

Pour conclure, à l'instar des grands conférenciers qui ont coutume de dire que toutes les révolutions passent par trois stades, à savoir le stade du ridicule, le stade de la dangerosité et puis finalement le stade de l'évidence, nous aimerions poser la question : à quel stade pensez-vous que nous soyons après en avoir appris un peu plus sur la technologie blockchain ?

BIBLIOGRAPHIE

DOCTRINE

ANDRE-DUMONT, A.-P., « Les services de paiement à l'épreuve des évolutions technologiques » in *La révolution digitale et les start-ups*, Bruxelles, Editions Larcier, 2016, 83-102 p.p.

ARMSTRONG, D., HYDE, D. ET THOMAS, S., « Blockchain and Cryptocurrency: International Legal and Regulatory Challenges », *Conveyancer & property lawyer*, 2019, vol. 1, pp. 109-111.

ARTZT, M. ET RICHTER, T., *Handbook of blockchain law : a guide to understanding and resolving the legal challenges of the blockchain technology* , Alphen aan den Rijn, The Netherlands, Kluwer Law International, 2020.

ATTIA, J.-J. ET VERBIEST, T., « Partie II. - 2010-2020 – Technologie blockchain » in *Un nouvel Internet est-il possible ?*, 1e édition, Bruxelles, Bruylant, 2020, p. 61-106.

AZAN, W., CAVALIER, G.A. ET BIDAN, M., *Des systèmes d'information aux blockchains : convergence des sciences juridiques, fiscales, économiques et de gestion* , Bruxelles, Bruylant, 2021.

BARBET-MASSIN, A., FLEURET, F., LOURMI, A., O'RORKE, W, et PION, C., *Droit des crypto-actifs et de la blockchain* , Paris, LexisNexis, 2020.

BEELEN, A., *Tout sur la blockchain et ses applications*, Limal, Anthemis, 2021.

BOUCHARD, C., (Dir.), *Comment la chaîne de blocs va transformer le droit ?*, Montréal, Éditions Yvon Blais, 2020.

CASSART, A., *Le droit des machintechs (FinTech, LegalTech, MedTech...) : état des lieux et perspectives*, Bruxelles, Larcier, 2018.

CASSAR, B. et DEFFAINS, B., *La transformation numérique du droit : les enjeux autour des LegalTech*, Bruxelles, Bruylant, 2021.

CHIU, I.H.-Y., *Regulating the crypto economy : business transformations and financialisation, Oxford*, Hart, 2021.

CUVELIER, F. ET NIEUWENHUYSE, H., « Risques et responsabilités en matière de blockchain » in Cuvelier, F. et al. (dir.), *Responsabilité, risques et progrès*, 1e édition, Bruxelles, Larcier, 2021, p. 57-100.

DUBOIS, J., « La régulation des crypto-monnaies et leurs plateformes de conversion », *R.I.S.F.-I.J.F.S.*, 2014/2, p. 77-82.

FULWOOD, A., « La DeFi se déchaîne- La finance décentralisée, en plein essor, cherche ou s'accrocher. », Challenge, 6 janvier 2022, p. 143- 144.

GAUTRAIS, V., *Neutralité technologique : rédaction et interprétation des lois face aux changements technologiques*, Montréal, Éditions Thémis, 2012.

GOUPY, M. et KOLIFRAT, G., « Blockchain : les enjeux en droit français », *R.I.S.F.-I.J.F.S.*, 2017/4, 19 p.

HOUSSA, C., STANDAERT, L., « La nouvelle frontière de la finance », in *L'économie du futur. Le futur de l'économie / Economie van de toekomst. Toekmst van de economie*, Bruxelles, Bruylant, 2016, 153-197 p.p.

HUTCHINSON, A.C., *Cryptocurrencies and the regulatory challenge*, London, Routledge, 2022.

JACQUEMIN, H., COTIGA, A. et POULLET, Y., *Les blockchains et les smart contracts à l'épreuve du droit*, Bruxelles, Larcier, 2020.

JOHNSTONE, S., *Rethinking the regulation of cryptoassets : cryptographic consensus technology and the new prospect, Cheltenham*, UK, Edward Elgar Publishing, 2021.

KRAUS, D., OBRIST, T. et HARI, O., *Blockchains, smart contracts, decentralised autonomous organisations and the law*, Cheltenham, UK, Edward Elgar Publishing, 2019.

LESSIG, L., *Code and Other Laws of Cyberspace*, New York, Basic Books, 1999.

MADIR, J., *FinTech: Law and Regulation*, Cheltenham, Gloucestershire, Edward Elgar Publishing, 2019.

MAGNIER, V., et BARBAN P., *Blockchain et droit des sociétés*, Paris, Dalloz, 2019.

MARMOZ, F., *Blockchain et droit* , Paris, Dalloz, 2018.

MOULIN, J.-M., QUINIOU, M., GASSER, A. et BOUILLET-CORDONNIER, G., (Coord.), *La finance numérique : aspects juridiques et fiscaux du crowdfunding et des cryptoactifs : avec des formulaires et tutoriels digitalisés et personnalisables par Legaltech Legal Pilot*, Paris, EFE Édition, 2021.

MORTON, J., « Alternative Finance in the United Kingdom », in *Droit de la Finance alternative*, Bruxelles, Bruylant, 2017, 369-400 p.p.

POLLICINO, O. ET DE GREGORIO, G., *Blockchain and public law : global challenges in the era of decentralisation* , Cheltenham, Edward Elgar Publishing, 2021.

POULLET. Y., et JACQUEMIN H., « Blockchain : une révolution pour le droit ? », *J.T.*, 2018, p. 801 à 819.

PREDA, R., « Les monnaies virtuelles, enjeux de régulation » in *Droits et souveraineté numérique en Europe*, Bruxelles, Bruylant, 2016, p. 73-79.

QUEMENER, M. et BENSOUSSAN, A., *Le droit face à la disruption numérique : adaptation des droits classiques : émergence de nouveaux droits*, Issy-les-Moulineaux, Gualino éditeur, 2018.

SOTIRI, E., *Précis sur les crypto-monnaies*, Bertrange, Luxembourg, Legitech, 2018.

TAPSCOTT, D et TAPSCOTT, A., « Blockchain Revolution : how the technology Behind Bitcoin Is Changing Money », Business, and the World, 2016.

TORDEURS A., « Une approche pédagogique de la blockchain », *Rev. int. serv. fin.,* 2017, p. 8 à 18.

VERCAMMEN, J., « Blockchain and the potential benefits for the financial market », *R.B.F.-B.F.W*, 2017/1, 67-71 p.p.

VERSLYPE K. et VERHEYE B., *Blockchain et contrats intelligents*, 1e édition, Bruxelles, Larcier, 2019.

WERY, P., « Monnaie fiduciaire, monnaie scripturale et monnaie électronique », *Rép.not.*, Tome IV, in *Les obligations extracontractuelles et le régime général des obligations*, Bruxelles, Larcier, 2016, n°659, 551 p.

LÉGISLATION

Règlement (UE) 2022/858 du Parlement européen et du Conseil du 30 mai 2022 sur un régime pilote pour les infrastructures de marché reposant sur la technologie des registres distribués, et modifiant les règlements (UE) no 600/2014 et (UE) no 909/2014 et la directive 2014/65/UE

Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE

Proposition de règlement du Parlement européen et du Conseil du 20 juillet 2021 sur les informations accompagnant les transferts de fonds et de certains crypto-actifs

Proposition de règlement du Parlement européen et du Conseil sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) no 1060/2009, (UE) no 648/2012, (UE) no 600/2014 et (UE) no 909/2014

Proposition de règlement du Parlement européen et du Conseil sur les marchés de crypto-actifs, modifiant la directive (UE) 2019/1937 du 24 septembre 2020

Article 1101 de la loi du 21 mars 1804, ancien Code Civil , *M.B.,* 21 mars 1804

INTERNET

https://www.ey.com/en_lu/assurance/fintechs-de-nouvelles-opportunites-pour-le-secteur-bancaire

https://www.consilium.europa.eu/fr/press/press-releases/2021/12/01/anti-money-laundering-council-agrees-its-negotiating-mandate-on-transparency-of-crypto-asset-transfers/

https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52020PC0593

https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

https://defipulse.com/

https://my.itsa.global/

https://adan.eu/pedagogie/classification-crypto-actifs

https://bitcoin.org/bitcoin.pdf

https://fr.cryptonews.com/news/tout-savoir-sur-le-vote-via-la-blockchain-7477.htm

https://fr.cryptonews.com/news/mixed-feelings-as-russia-readies-for-landmark-blockchain-vot-6751.htm

https://www.reddit.com/r/rootstock/comments/idzbzs/nuclearis_developed_the_first_blockchain/

https://www.silicon.fr/avis-expert/blockchain-vers-une-transformation-inattendue-du-secteur-de-leducation

https://www.ethereum-france.com/livre-blanc-white-paper-ethereum-traduction-francaise/

https://www.ecb.europa.eu/paym/digital_euro/html/index.fr.html

https://goo.gl/RHG1t1

https://goo.gl/sg4MzW

https://cryptoast.fr/ethereum-selon-nouveau-calendrier-merge-attendue-19-septembre/

https://doi.org/10.1145/2382196.2382292

https://www.reuters.com/article/crypto-currencies-criminals-idUSKBN28J1IX

https://cryptoforinnovation.org/resources/Analysis_of_Bitcoin_in_Illicit_Finance.pdf

www.etherscan.com