



Quelle régulation des crypto-actifs et de la blockchain applicable à l'activité bancaire ?

Mémoire présenté par **Timothée FOURNIÉ-TAILLANT**

Sous la direction de Madame la Professeure Valérie NICOLAS ainsi que
Madame Virginie VIGNON-PRIAM et Monsieur Martin PAILHES

Année universitaire 2019 - 2020

Remerciements

Je tiens à remercier Madame la Professeure Valérie NICOLAS, en tant que Directrice de mémoire, pour le grand intérêt qu'elle a porté à ce sujet, ainsi que pour son encadrement.

Je tiens également à exprimer ma profonde gratitude à Madame Virginie VIGNON-PRIAM et à Monsieur Martin PAILHES, mes Maîtres de stage, pour la confiance qu'ils m'ont accordée, pour leur grande patience ainsi que pour les connaissances apprises à leurs côtés.

Je tiens enfin à remercier Madame la Professeure Catherine PREBISSY-SCHNALL ainsi que Monsieur le Professeur Sébastien RAIMOND, en qualité de Directeurs de Master, pour m'avoir accordé la chance d'intégrer le Master 2 Droit des Technologies Numériques et Société de l'Information de l'Université Paris Nanterre.

Contexte

Dans le cadre de ma formation au sein du Master 2 DTNSI, j'ai eu la chance et l'immense honneur d'effectuer un stage en droit du numérique au sein de BNP Paribas de janvier à juin 2020. J'ai ainsi intégré l'équipe « Legal IT/IP » en tant que stagiaire au sein du LEGAL, la fonction juridique du Groupe. L'une de mes principales missions chez BNP Paribas en tant que juriste stagiaire a consisté en l'apport d'une expertise juridique et technique en matière de régulation des crypto-actifs du point de vue de l'activité de la banque.

BNP Paribas est une grande multinationale présente au sein de 74 pays avec plus de 190 000 collaborateurs. La Banque y accompagne l'ensemble de ses clients : particuliers, associations, entrepreneurs, PME, grandes entreprises et institutionnels. Le Groupe les aide à réaliser leurs projets personnels et professionnels en leur proposant des services de financement, d'investissement, d'épargne et de protection. Il s'agit du leader de services bancaires et financiers en Europe, et de la première banque de la zone euro en termes de dépôts.

Le LEGAL, présidé par Monsieur Georges DIRANI depuis octobre 2010, rassemble quant à lui 1800 juristes sur cinq continents. 1390 d'entre eux exercent en Europe et 615 uniquement en France. Ces juristes forment une équipe indépendante et collaborative d'experts juridiques. Ils soutiennent et protègent le groupe BNP Paribas dans un environnement économique internationalisé et dont la réglementation est en constante évolution.

Les opinions exprimées dans la présente sont propres à leur auteur, qui s'exprime en son propre nom, et n'engagent ni l'Université Paris Nanterre, ni BNP Paribas.

Mémoire : Quelle régulation des crypto-actifs et de la blockchain applicable à l'activité bancaire ?

INTRODUCTION :

« L'accumulation de désastres monétaires tout au long du XXème siècle suggère que, contrairement à l'idée reçue, la monnaie est une chose trop importante pour être laissée à l'État. Comme le montre l'école de pensée autrichienne, les cycles économiques sont essentiellement créés par les manipulations monétaires des autorités publiques, avec des conséquences sociales et économiques catastrophiques. »¹

Historique :

La publication en 2008 du document scientifique « Bitcoin: A Peer To Peer Electronic Cash System »² par Satoshi Nakamoto³, décrivant une nouvelle monnaie décentralisée exploitant la cryptographie, est tombé à pic à une époque de défiance envers un système financier mondial en crise. L'essor des crypto-actifs qui s'en est suivi au début des années 2010, notamment en premier lieu dans leur rôle de monnaie d'échange, a constitué un grand espoir pour les libéraux souhaitant l'émergence d'un système monétaire horizontal, notamment ceux se réclamant de l'école autrichienne portée par des économistes comme Friedrich August von Hayek. Dès 1976, ce dernier appelait à la mise en concurrence de monnaies en dehors du monopole et du contrôle des États, ce qui constituait selon lui la meilleure parade contre le risque d'inflation⁴. C'est précisément en réponse à ce risque qu'il a été prévu qu'il n'existera à terme que 21 millions de Bitcoins, pas un de plus⁵.

¹ Yorick de Mombynes, Institut Sapiens, "Bitcoin, totem & tabou, que presage l'essor des cryptomonnaies ?" <https://www.institutsapiens.fr/wp-content/uploads/2018/02/Bitcoin-totem-et-tabou-f%C3%A9vrier-2018.pdf>

² « White paper » du Bitcoin <https://bitcoin.org/bitcoin.pdf>

³ Satoshi Nakamoto est le pseudonyme utilisé par la ou les personnes qui ont développé le Bitcoin.

⁴ Friedrich August von Hayek, The denationalization of money <https://nakamotoinstitute.org/static/docs/denationalisation.pdf>

⁵ Le protocole du Bitcoin prévoit qu'il n'en sera émis que 21 millions au maximum. Personne ne peut modifier ce protocole, pas même un Etat <https://www.coinhouse.com/fr/apprendre/bitcoin/pourquoi-21-millions-de-bitcoins/>

Les plus grandes institutions financières ont tout d’abord fermement rejeté les crypto-actifs, ce qui pouvait porter à croire que l’avènement de ces nouvelles monnaies les menaçaient et qu’elles en avaient peur. Jamie Dimon, PDG de JPMorgan Chase & Co et personnalité notable de la finance américaine, avait même qualifié en 2017 le Bitcoin d’escroquerie⁶. Mais ces dernières années les choses ont bien changé et les institutions de la finance classique ne se sont jamais autant intéressées aux crypto-actifs ainsi qu’à leur technologie sous-jacente, la blockchain. Il semble que, contrairement aux espoirs des libéraux et autres crypto-anarchistes⁷, *l’establishment* ne souhaite plus être à l’écart et cherche désormais à intégrer ces technologies dans ses produits et services, voire en créer de nouveaux. Difficile à croire il y a quelques années, JPMorgan compte désormais certaines plateformes d’échange de crypto-actifs parmi ses clients, et a même lancé le sien – le JPM Coin – l’année passée⁸. Le mouvement s’accélère : de nombreux instituts monétaires, notamment 80% des banques centrales⁹, réfléchissent à un projet de monnaie numérique par l’intermédiaire de crypto-actifs¹⁰.

Cet intérêt de nombreux acteurs « traditionnels » de l’industrie pour les crypto-actifs et pour la blockchain constitue une désillusion pour les enthousiastes de la première heure qui voyaient en cette technologie l’annonce du retour d’un internet décentralisé, comme le voulaient les fondateurs du *world wide web*¹¹ ; bien que cet aspect soit devenu de plus en plus contestable pour le réseau Bitcoin¹².

Les crypto-anarchistes, les internautes puis la sphère financière avaient commencé à s’intéresser aux crypto-actifs pour leur usage en tant que monnaie d’échange, d’où le terme erroné de « *cryptomonnaie* ». Mais l’usage des crypto-actifs en tant que monnaie d’échange

⁶ Bloomberg, *Jamie Dimon Slams Bitcoin as a ‘Fraud’* <https://www.bloomberg.com/news/articles/2017-09-12/jpmorgan-s-ceo-says-he-d-fire-traders-who-bet-on-fraud-bitcoin>

⁷ Communauté souhaitant la réalisation dans l’espace numérique d’une forme d’anarchie par l’usage de la cryptographie.

⁸ Forbes, *JPMorgan - Bitcoin’s ‘Biggest Enemy’ - Suddenly Appears To Be Going All In On Crypto* <https://www.forbes.com/sites/billybambrough/2020/05/30/jp-morgan-bitcoins-biggest-enemy-suddenly-appears-to-be-going-all-in-on-crypto/>

⁹ La Tribune avec AFP, « *Monnaie digitale : 80% des banques centrales planchent sur le sujet* » <https://www.latribune.fr/entreprises-finance/banques-finance/monnaie-digitale-80-des-banques-centrales-planchent-sur-le-sujet-837966.html>

¹⁰ Banque des Règlements Internationaux, « *Impending arrival – a sequel to the survey on central bank digital currency* » <https://www.bis.org/publ/bppdf/bispap107.pdf>

¹¹ Le Monde Informatique, « *Les pères de l’Internet plaident pour un web plus décentralisé* » <https://www.lemondeinformatique.fr/actualites/lire-les-peres-de-l-internet-plaident-pour-un-web-plus-decentralise-65119.html>

¹² The Coin Tribune, « *La décentralisation de Bitcoin face à un danger inédit et la solution... c’est vous* » <https://www.thecointribune.com/actualites/la-decentralisation-de-bitcoin-face-a-un-danger-inedit-et-la-solution-cest-vous/>

n'en est qu'un parmi d'autres qui sont permis par la blockchain : l'industrie connaît un intérêt croissant pour ces différents usages, y compris appliqués à l'activité bancaire. Par ailleurs, bien que la terminologie porte là aussi à confusion, les crypto-actifs ne doivent surtout pas être confondus avec la monnaie électronique¹³ – qui est un simple composant de la masse monétaire de banque centrale aux côtés de la monnaie fiduciaire et de la monnaie scripturale.

Nous laisserons donc le terme de monnaie à son rôle régalien traditionnel¹⁴. Ainsi, c'est le terme général et neutre de crypto-actif, voire de jeton numérique, qu'il conviendra d'employer par la suite.

Définitions¹⁵ :

L'activité bancaire peut être considérée comme constituée par les opérations de banque. Le code monétaire et financier dispose des termes suivants¹⁶ : « *Les opérations de banque comprennent la réception de fonds du public, les opérations de crédit, ainsi que les services bancaires de paiement* ». Si la loi en distingue donc essentiellement trois, il convient pour cette étude d'appréhender cette notion de manière large.

Crypto-actif : Forme d'actif numérique exploitant la cryptographie et existant au sein d'un registre distribué.

Technologie de registre distribué / Distributed Ledger Technology (DLT) : Moyen de sauvegarder des informations par le biais d'un registre distribué, c'est-à-dire une copie numérique répétée de données disponibles à plusieurs endroits. La DLT est basée sur la cryptographie asymétrique, un système utilisant des paires de clés : des clés publiques, qui sont publiquement connues et essentielles pour l'identification, et les clés privées, qui sont gardées secrètes et sont utilisés pour l'authentification et le chiffrement.

¹³ Telle que définie à l'article L315-1 du code monétaire et financier.

¹⁴ Telle que définie aux articles L111-1 et suivants du code monétaire et financier.

¹⁵ Définitions récentes issues du document de la Commission européenne « *Public consultation on an EU framework for markets in crypto-assets* »

https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-crypto-assets-consultation-document_en.pdf

¹⁶ Article L311-1 du code monétaire et financier

Cryptographie : Conversion de données en code privé à l'aide d'algorithmes de chiffrement, généralement destinée à leur transmission sur un réseau public.

Blockchain : Technologie de registre distribué (DLT) au sein duquel les détails des transactions sont conservés sous forme de blocs d'informations successifs. Un bloc d'informations nouvelles est rattaché à la chaîne de blocs préexistants par un processus informatisé permettant la validation des transactions.

À travers ces définitions il est possible de déduire trois choses essentielles :

- un crypto-actif s'appuie sur une technologie de registre distribué (DLT) ;
- une DLT n'est régie par aucune autorité centrale ;
- une blockchain est un type spécifique de DLT ayant comme son nom l'indique essentiellement la particularité de fonctionner par chaîne de blocs d'informations.

Délimitation :

L'objet de cette étude concernera uniquement la blockchain et les crypto-actifs exploitant cette technologie. De plus, la présente contribution n'adressera la question de la régulation des crypto-actifs et de la blockchain qu'exclusivement en lien avec l'activité bancaire. Ainsi ne sera pas évoquée la régulation de ces technologies innovantes se rapportant par exemple à la fiscalité, au droit des sociétés ou encore à la propriété intellectuelle, bien que ces matières soient connexes. Enfin, il va sans dire que cette étude se limitera à la régulation européenne et française en la matière.

Le terme de *régulation*, et non de réglementation, comme objet de cette étude, présente une importance particulière. En français, la confusion et l'assimilation des deux termes à la définition de réglementation provient d'un anglicisme. Si la réglementation est un ensemble de mesures coercitives qui imposent des obligations aux agents économiques, la régulation est une notion plus subtile et globale. La régulation peut être définie comme un ensemble de mécanismes permettant d'ajuster l'offre et la demande sur différents marchés. Elle peut être fondée sur les mécanismes de marché tels que le prix ou être étatique dans quel cas l'État intervient pour corriger les déséquilibres. La réglementation peut donc être considérée comme n'étant qu'une part de la régulation, aux côtés de mécanismes de marché ou encore du droit

mou¹⁷. Cela se matérialise en l'espèce par la règle de droit, mais aussi par le comportement des différents régulateurs ou plus concrètement encore par l'influence exercée sur le marché par l'établissement de régimes juridiques optionnels.

Il conviendra dans une première partie de s'intéresser à la régulation des crypto-actifs ainsi que celle des plateformes d'échanges s'y rapportant. Y seront traitées les problématiques se rapportant à la qualification juridique de ces actifs, ainsi qu'aux responsabilités des plateformes exploitant ce nouveau marché. Dans la seconde partie de la présente sera traitée la régulation de la blockchain : cette technologie sous-jacente pose de nouveaux défis en matière de gouvernance décentralisée, tout en présentant un fort aspect de sécurité des systèmes d'informations mêlant juridique et technique.

PARTIE I – LES BALBUTIEMENTS D'UNE RÉGULATION PRAGMATIQUE DES CRYPTO-ACTIFS ET DE LEURS PLATEFORMES D'ÉCHANGE

Un cadre juridique complexe est en formation en France, tout comme au sein des autres États membres de l'Union Européenne. L'un de ses enjeux concerne la nécessaire qualification des crypto-actifs tenant compte de leurs spécificités comme de leur diversité, notamment afin de définir le régime des services qui s'y rapportent. Une question cruciale se pose alors : peut-on y appliquer la réglementation financière existante ?

Chapitre 1^{er} : La difficile qualification juridique des jetons

La qualification juridique des crypto-actifs est cruciale pour l'application de la réglementation existante – ainsi que pour la création d'une régulation efficace là où le droit n'existe pas – aux contrats et acteurs s'y rapportant.

Section 1 : Une forte diversité de types de crypto-actifs impliquant une pluralité de régimes souhaitables

¹⁷ Dr Pier-Pascale Boulanger, Université de Concordia, « *Régulation ou réglementation ?* » <http://odft.nt2.ca/blogue/r%C3%A9gulation-ou-r%C3%A9glementation>

L'une des difficultés de la qualification des crypto-actifs vient de la diversité de leurs caractères en fonction de leur fonctionnement technique mais aussi en fonction de l'actif sous-jacent dont ils sont la représentation.

Paragraphe 1 : L'actif sous-jacent, critère logique de classification des crypto-actifs

Différents types de crypto-actifs permettent des usages variés ce qui complique grandement la création d'une régulation adaptée à chacun d'entre eux. L'apparition d'une sous-catégorie de crypto-actifs, communément nommés crypto-actifs programmables (programmable crypto-asset) ou jeton (token), complique les choses et nécessite des définitions précises.

En voici une liste non-exhaustive :

Jeton de paiement (payment token) : crypto-actif servant de moyen de paiement ou d'échange.

Jeton d'utilité (utility token) : crypto-actif donnant accès à un produit ou à un service spécifique.

Jeton de titre (security token) : crypto-actif qualifié d'instrument financier¹⁸ au sens du CMF.

Jeton d'investissement (investment token) : crypto-actif ouvrant droit à des bénéfices.

Jeton stable (stablecoin) : type de jeton dont l'usage souhaité est le même qu'un jeton de paiement, et dont la valeur est supposée rester stable dans le temps. Sa valeur est généralement garantie par d'autres actifs – par exemple une monnaie « *fiat* » comme l'euro, ce qui en fait un type spécifique de jeton de titre qualifié d'instrument financier – ou alors par un algorithme blockchain régissant leur nombre de manière dynamique afin de maîtriser leur inflation.

¹⁸ Les instruments financiers sont soit des titres financiers, soit des contrats financiers.

	Cryptocurrencies	Tokens or programmable crypto-assets		
		Utility tokens (access to a service run on blockchain)	Digital representation of one real asset (e.g a luxury bag)	Stablecoins
Fungible	✓	✓ or ✗	✗	✓
Native	✓	✓	✗	✓ ² or ✗ ³
Control	-	- à +++	++	+++
Complexity	+	++	++	+++

19

À travers ce prisme, les crypto-actifs « classiques » dont le Bitcoin est un digne représentant sont donc des jetons de paiement qui correspondent à la mal-nommée cryptomonnaie. Leur qualification juridique est déjà relativement avancée.

Paragraphe 2 : Une qualification juridique avancée du Bitcoin et des jetons de paiement assimilables

Le Conseil d'État s'était déjà prononcé en 2018 sur les modalités d'imposition des gains tirés de la plus-value lors de la cession de Bitcoins par des particuliers. Estimant, comme enfonçant une porte ouverte, qu'il s'agissait là de biens meubles incorporels²⁰, caractères que l'on pourrait à priori aisément étendre à tous les crypto-actifs, de nombreuses autres questions demeurent cependant.

¹⁹ Tableau produit par l'Association pour le Développement des Actifs Numériques (ADAN), « *Consultation on a EU framework for markets in crypto-assets* »

²⁰ Conseil d'Etat, 3^e et 8^e chambres réunies, 26 avril 2018 n°417809

<https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-26-avril-2018-m.-g-et-autres>

Une décision du Tribunal de commerce de Nanterre en date du 26 février 2020²¹ a tenté de clarifier le statut juridique du Bitcoin²². Dans cet arrêt fortement structurant ont donc été établies les considérations suivantes :

- Un Bitcoin est un bien consommable et fongible tout comme la monnaie légale ;
- Donc un prêt de Bitcoin est un prêt de consommation ;
- Si une fourche intervient sur la blockchain Bitcoin lorsqu'un Bitcoin est prêté, alors les jetons nouvellement émis reviennent à l'emprunteur.

Bien qu'il ne s'agisse que d'une décision de première instance, et qu'il soit fortement improbable qu'elle puisse s'appliquer uniformément à tous les crypto-actifs, ces trois considérations qui s'en dégagent sont importantes pour l'activité bancaire. Le Bitcoin s'apparente en de nombreux points à une monnaie – tout comme l'ensemble des crypto-actifs appartenant à la catégorie des jetons de paiement – sans être reconnu comme tel par le tribunal.

En premier lieu, la décision établit la consommabilité du Bitcoin ; puisqu'il est consommé lors de son utilisation pour payer des biens, des services, ou encore pour le prêter. Elle confirme également la fongibilité des Bitcoin : bien qu'ils soient issus d'un protocole informatique permettant d'identifier chaque unique Bitcoin de manière certaine ainsi que de retracer l'historique des transactions et donc de remonter à chaque porteur successif de chacun d'entre eux ; ils sont « *de même espèce et de même qualité* » au sens du code civil. Le Bitcoin permet alors d'effectuer un paiement au sens de [l'article 1347](#) du code civil qui dispose en son second alinéa que les obligations fongibles sont celles qui ont pour objet une quantité de choses de même genre.

En second lieu, un prêt de Bitcoin constitue un prêt de consommation au sens de [l'article 1892](#) du code civil, et pas un prêt d'usage au sens du même code. Par l'effet de ce prêt, l'emprunteur devient alors propriétaire de la chose prêtée. Il est donc possible de rembourser le prêteur avec d'autres Bitcoin, puisqu'ils sont fongibles entre eux.

²¹ Tribunal de commerce de Nanterre, 6^e chambre, 26/02/2020, SDE BITSPREAD LTD contre SAS PAYMIUM <http://www.rdmf.es/wp-content/uploads/2020/03/TRIB.-COMERCIO-NANTERRE-26.02.2020-Bitcoin.pdf>

²² Louis Chochoy, Village Justice, « Bitcoin : La justice française reconnaît les propriétés d'une monnaie mais sans en avoir la qualification » <https://www.village-justice.com/articles/bitcoin-justice-francaise-reconnait-les-proprietes-une-monnaie-mais-sans-avoir,34045.html>

Enfin, le dédoublement des jeton prêtés se voit attribuer un régime ressemblant à celui des dividendes qui est prévu dans les dispositions applicables aux prêts de de titres financiers des [articles L211-22](#) et suivants du code monétaire et financier : l'emprunteur a droit aux dividendes qui seraient versés pendant la durée du prêt, comme fruit de la chose prêtée. En l'espèce, suite à une fourche²³ de la blockchain, chaque propriétaire de Bitcoin à un instant précis s'est vu reconnaître la propriété d'autant de Bitcoin Cash.

Paragraphe 3 : Une précision au demeurant incomplète corrélée par la doctrine prudente de l'AMF

Il s'agit d'une précision incomplète, puisque se pose toujours la question du sort de la logique clause de restitution du jeton nouvellement émis en cas de fourche. Une telle clause ressemblerait en de nombreux points à la classique clause stipulant que l'emprunteur d'un titre financier encaissant un coupon ou dividende issu de ce titre doit le restituer au prêteur. Le rapprochement est d'autant plus pertinent que la survenue d'une fourche, tout comme la distribution du dividende, exerce une pression reconnue à la baisse sur le cours de l'actif premier²⁴. La question de l'application de la réglementation concernant le taux d'intérêt légal²⁵ aux prêts de Bitcoin et autres jetons de paiement demeure également.

L'Autorité des Marchés Financiers, qui régule la place financière française, ses acteurs et les produits d'épargne qui y sont commercialisés, et qui n'est pas directement²⁶ compétente en matière de crypto-actifs, a estimé en avril dernier²⁷ qu'une classification légale précise des crypto-actifs était prématurée. L'AMF préconise plutôt la distinction entre les jetons qui correspondent à un instrument financier, et ceux qui n'y correspondent pas.

Si les jetons ouvrent des droits de créance ou en capital, alors ce sont des instruments financiers qui relèvent de la réglementation financière classique (notamment jetons stables et jetons de

²³ Une fourche est la création d'une chaîne secondaire gardant un tronc commun avec la blockchain principale, qui apporte des améliorations ou modifications par rapport au protocole d'origine, mais qui n'a pas fait consensus au sein du réseau premier.

²⁴ Lorsque le dividende est versé, on dit que le coupon est « détaché » et le montant du dividende est soustrait du cours de l'action en bourse.

²⁵ Articles L313-2 et suivants du CMF

²⁶ L'AMF est traditionnellement compétente en matière de traitement prudentiel du portefeuille des sociétés de gestion d'actifs. Elle est reconnue compétente en matière de crypto-actifs lorsque ceux-ci correspondent à des instruments financiers.

²⁷ AMF, "Consultation document on an EU framework for markets in crypto-assets" https://www.amf-france.org/sites/default/files/2020-04/crypto-ue-reponse-amf_1.pdf au point 6

titres) c'est-à-dire des articles [L211-1](#) et suivants du code monétaire et financier. Les jetons qui ne répondent pas à cette qualification échappent donc à la réglementation financière, notamment concernant les délits de marché dont le délit d'initié²⁸ et la manipulation de cours²⁹ sont d'éloquents représentants. Le principe d'égalité des acteurs devant l'information qui régit normalement les marchés financiers ne s'applique donc pas dans ce cas, ce qui pose problème notamment en matière de confiance et de protection des investisseurs, comme le sera exposé dans la suite de la présente.

L'AMF préconise, en outre, l'établissement d'une réglementation agile devant prendre le temps de se préciser. Il s'agit d'une position pragmatique, mais qui laisse pour le moment bien peu de visibilité aux acteurs notamment les établissements bancaires, qui développent dès aujourd'hui les services de demain.

Section 2 : Les levées de fond en crypto-actifs : vers de nouveaux marchés financiers

Les crypto-actifs sont à l'origine d'un nouveau moyen de financement des entreprises qui présente des problématiques nouvelles notamment quant à la protection des investisseurs.

Paragraphe 1 : L'innovation bienvenue des Initial Coin Offering en matière de financement des entreprises

L'un des premiers apports des crypto-actifs en matière de finance fut les « Initial Coin Offering » (ICO), ou offre au public de jetons. Il s'agit d'une méthode innovante de levée de fonds durant la phase de démarrage d'un projet, qui fonctionne via l'émission de crypto-actifs sur une blockchain, échangeables contre d'autres crypto-actifs ou contre une monnaie étatique. Elle peut être définie comme une opération de levée de fonds effectuée à travers un dispositif d'enregistrement électronique partagé (la blockchain) qui donne lieu à une émission de jetons pouvant être ensuite, selon les cas, utilisés pour obtenir des produits ou services.

L'opération a pour but, pour une entreprise, de lever du capital afin de bâtir un écosystème innovant sur une nouvelle blockchain. Le jeton d'utilité (utility token) qui y est émis aura une fonction spécifique constituant la substance de la contrepartie de l'acquéreur, lui donnant accès

²⁸ Article L564-1 CMF

²⁹ Articles L465-3-1 et L465-3-3 CMF

à un produit ou à un service – souvent logiciel – par exemple à travers une fonctionnalité innovante de cette nouvelle blockchain. La forte volatilité de ces crypto-actifs et la rapide valorisation du jeton émis pour certains projets ont également attiré de nombreux spéculateurs, ce qui constitue un certain risque financier et a fait craindre aux régulateurs l’explosion de bulles spéculatives³⁰.

L’offre initiale de jetons est parfois comparée à une introduction en bourse³¹, bien que ces deux modèles divergent sur plusieurs points. Le terme ICO est d’ailleurs inspiré du terme financier classique « Initial Public Offering » (IPO). Lors d’une de ces levées de fonds, les investisseurs reçoivent des actions en échange de leur argent. Ces actions représentent une part de la propriété du capital de l’entreprise et se négocient ensuite sur le marché secondaire par l’intermédiaire des marchés financiers traditionnels. Lors d’une ICO, les investisseurs reçoivent des jetons émis sur une blockchain, qui n’offrent pas juridiquement une part de l’entreprise, encore moins la garantie que le service promis sera bien effectif, pas plus que celle de l’existence d’un marché secondaire pour la revente de cet actif.

Les ICO posent ainsi un problème de confiance des investisseurs : il est difficile pour eux de s’informer et d’évaluer la pertinence ou la qualité d’un projet, qui n’existe souvent pas encore au moment de l’offre de jetons. Certains n’ont tout simplement aucune valeur tangible. Le flou juridique qui entoure les ICO ne permet pas aux investisseurs de se protéger, alors que les introductions en bourse sont, elles, extrêmement réglementées. L’Autorité Européenne des Marchés Financiers (ESMA) alertait les investisseurs à propos de ces risques dès 2017 et attirait leur attention sur leur exposition à des fraudes et autres activités illicites permises par l’anonymat des personnes à l’origine d’un ICO, ainsi que par leur capacité à récolter des montants d’argent élevés en de très courts laps de temps³².

Les ICO sont tout de même devenues populaires à partir de 2017 et ont permis à de nombreux projets autour de la blockchain de se développer, avec plus de 4 milliards de dollars de récoltés

³⁰ Dr Lerong Lu, “*Bitcoin: speculative bubble, financial risk and regulatory response*”

³¹ Le Monde, « *Bitcoins et autres cryptodevises agitent Wall Street* »
https://www.lemonde.fr/economie/article/2017/10/05/bitcoins-et-autres-cryptodevises-font-vaciller-le-capital-risque-et-wall-street_5196321_3234.html

³² European Securities and Market Authority, “*ESMA highlights ICO risks for investors and firms*”
<https://www.esma.europa.eu/press-news/esma-news/esma-highlights-ico-risks-investors-and-firms>

par les différents projets dans le monde. En 2018, ce sont plus de 13 milliards de dollars qui ont été levés par leur intermédiaire³³ !

Paragraphe 2 : L'apport « mou » de la Loi Pacte en matière d'ICO : le visa optionnel

La loi du 22 mai 2019 relative à la croissance et la transformation des entreprises fut l'occasion pour la France de tenter de trouver une solution à ces problèmes, sans légiférer de manière rigide et contraignante, ce qui aurait pu avoir pour effet de défavoriser les projets nationaux face à leur concurrence étrangère se trouvant hors du champ d'application de la loi française. Il s'agit donc de régulation bien plus que de réglementation, les acteurs concernés étant libres de s'y soumettre, bien que le marché les y ait fortement incités – la fameuse *soft law*.

En effet, l'une des mesures phares de la loi Pacte en matière de crypto actifs, codifiée à l'article [L.552-4](#) du code monétaire et financier, est la possibilité pour les porteurs de projets d'ICO de solliciter un visa optionnel auprès de l'AMF. Il s'agit d'un régime spécifique destiné au développement des ICO notamment en comblant le déficit de confiance des investisseurs présenté au paragraphe précédent³⁴.

Les émetteurs d'ICO peuvent se voir légitimés auprès du public par ce visa de l'AMF sous certaines conditions³⁵, notamment :

- produire un document d'information « white paper » délivrant une information claire et loyale aux potentiels souscripteurs conformément à [l'article 712-2](#) du règlement général de l'AMF ;
- être constitués sous la forme d'une personne morale établie ou immatriculée en France ;
- prévoir un mécanisme de sécurisation des fonds collectés et répondre aux exigences en matière de lutte contre le blanchiment et le financement du terrorisme.

Ces critères, qui demandent un peu d'organisation pour les porteurs de projets, sont extrêmement simples à remplir pour les établissements bancaires, qui ne sont pas étrangers à

³³ Charlie Perreau, Journal du Net, « ICO : définition, liste, situation en France » <https://www.journaldunet.com/economie/finance/1195462-ico-definition-liste-la-situation-en-france-decembre-2019/>

³⁴ Georges Tchikaidze, Village Justice, « L'encadrement réglementaire des ICOs par la loi Pacte » <https://www.village-justice.com/articles/encadrement-reglementaire-des-icos-par-loi-pacte-contenu-enjeux,31308.html>

³⁵ AMF, « Obtenir un visa pour une offre au public de jetons (ICO) » <https://www.amf-france.org/fr/espace-professionnels/fintech/mes-relations-avec-lamf/obtenir-un-visa-pour-une-ico/preparer-une-ico>

ce type d'obligations issues de la finance classique. Tout comme le *crowdfunding*, les ICO pouvaient être jusqu'ici considérées comme une forme de concurrence déloyale au capital-risque classique, puisque non régulées, bien que les enjeux soient différents³⁶. Ce régime optionnel consiste finalement pour les porteurs de projets en une forte incitation à se conformer aux obligations issues de la finance classique. En outre l'AMF vérifiera que les jetons proposés ne tombent pas sous la réglementation existante en matière d'instruments financiers : ce visa ne concerne donc que les ICO proposant des jetons d'utilité qui n'empiètent pas sur l'activité bancaire.

Il s'agit là d'un modèle de régulation très intéressant : bien qu'il s'agisse d'un visa optionnel, il aura une influence importante sur le marché. Les acteurs qui ne souhaitent pas s'y conformer sont libres de ne pas le faire, mais prennent le risque d'être décrédibilisés face à leur concurrents qui le font, voire d'être directement soupçonnés de fraude.

La loi Pacte a également permis d'apporter des définitions en la matière, notamment celle des jetons numériques et des ICO, qu'elle a codifié respectivement au sein des articles [L552-2](#) et [L552-3](#) du code monétaire et financier. À noter que la blockchain y est également définie de manière indirecte³⁷.

Paragraphe 3 : Une transition en cours vers une forme nouvelle d'offre au public de jetons : les Security Coin Offering

Une nouvelle forme de levée de fonds en crypto-actifs est en train de connaître un attrait croissant de la part des émetteurs et investisseurs, notamment au sein des milieux financiers traditionnels. Il s'agit d'offres au public de jetons de titre (security token) présentant cette fois des caractéristiques d'instrument financier au sens du code monétaire et financier. En effet, l'actif sous-jacent du jeton est un titre financier existant, qui donne droit de créance ou de capital – avec les droits de gouvernance et dividendes associés.

³⁶ Caroline Lamaud, « Les ICOs : une menace pour le capital risque ? » <https://www.anaxago.com/aller-plus-loin/blog/les-icos-une-menace-pour-le-capital-risque>

³⁷ L'article L552-2 du CMF dispose des termes suivants : « dispositif d'enregistrement électronique partagé permettant d'identifier, directement ou indirectement, le propriétaire dudit bien »

Ces jetons offrent de nouvelles possibilités car ils sont soumis à la réglementation financière classique qui protège les investisseurs de manière efficace. Il s'agit donc d'une forme hybride de levée de fonds qui tente d'allier le meilleur des deux mondes entre les avantages technologiques de la blockchain et ceux de la finance régulée³⁸.

Les jetons de titres permettent de mettre en place un vaste éventail de nouvelles capacités d'investissement. Par leur intermédiaire, un STO permet par exemple pour l'entrepreneur d'émettre de la dette classique – l'actif sous-jacent du jeton étant alors une obligation – afin de capitaliser sur la construction d'un projet basé sur un nouveau protocole blockchain. Les propriétaires de certains jetons de titre pourront choisir de vendre soit une partie de leurs intérêts, soit une partie des dividendes de la totalité de leurs actions sur un marché secondaire, tout en automatisant ce type d'opération grâce aux capacités de la blockchain. Les établissements bancaires classiques n'ont donc jamais eu une si belle occasion de jouer un rôle dans la finance par l'intermédiaire des crypto-actifs³⁹.

Il existe également des interactions complexes avec le droit des sociétés : par exemple, il est par principe interdit aux SAS de procéder à une offre au public de titres financiers⁴⁰ ; la liquidité offerte par l'émission jetons de titres sur une blockchain ne devrait donc pas leur permettre de contourner cette interdiction. Là encore, les établissements bancaires ont un rôle fort à jouer, les levées de fonds en crypto-actifs et leurs interactions avec le droit existant devenant une nouvelle discipline d'expertise financière.

Chapitre 2^e : La responsabilité renforcée des plateformes d'échanges de crypto-actifs

Depuis l'avènement des crypto-actifs, de nombreuses *exchanges*⁴¹ spécialisés en la matière se sont développés. Leur nouveau rôle, semblable à celui des plateformes de trading, mène logiquement aux problématiques juridiques bien connues des opérateurs des marchés financiers classiques. Des obligations héritées de la finance classique, voire seulement la possibilité de

³⁸ Adrien Ahmadi Kermanshahani et Henri Nalbandyan, Village Justice, « *Security Token Offerings : Plongée au cœur de la finance régulée* » <https://www.village-justice.com/articles/security-token-offering-plongee-coeur-finance-regulee,30971.html>

³⁹ Jonathan Chester, Forbes, « *Will Security Token Offerings Be The Future Of Raising Money?* » <https://www.forbes.com/sites/jonathanchester/2019/02/19/will-security-token-offerings-be-the-future-of-raising-money/>

⁴⁰ Article L227-2 du code de commerce

⁴¹ Les exchanges sont les plateformes de rencontre entre vendeurs et acheteurs de crypto-actifs.

s'y soumettre, incombent donc désormais à ces nouvelles places de marché proposant l'échange de crypto-actifs.

Section 1 : L'apport de la Loi Pacte pour les échanges de crypto-actifs

La loi Pacte s'intéresse aux projets de financement en crypto-actifs, mais également directement aux acteurs les plus critiques de ce nouvel univers. Elle leur propose un agrément optionnel ainsi qu'une licence obligatoire pour l'exercice de deux activités.

Paragraphe 1 : La possibilité d'obtenir l'agrément PSAN

La loi Pacte a proposé une solution intelligente de visa optionnel afin de combler le manque de confiance⁴² dans les projets de levée de fonds par offre au public de jetons, et propose en son article 86 un agrément optionnel pour les acteurs de ce marché. Mais elle apporte également des solutions contraignantes pour réguler certaines activités exercées par les échanges. La loi Pacte a donc créé un nouveau cadre juridique pour les « *prestataires de services sur actifs numériques* » (PSAN), codifié au sein d'un nouveau chapitre du même nom dans le code monétaire et financier⁴³.

L'article L54-10-2 du même code couvre désormais cinq types de services distincts, pour lesquels les acteurs des places de marché de crypto-actifs peuvent demander d'être licenciés et placés sous la supervision de l'AMF.

Le terme « actifs numériques » comprend ici l'ensemble des crypto actifs, les fameux jetons issus des offres publiques sont donc compris. Les instruments financiers sont cependant là encore exclus du régime.

Les services sur actifs numériques que couvrent ces nouvelles dispositions sont définis dans le CMF comme étant les suivants :

- la conservation d'actifs numériques pour le compte de tiers ;
- l'achat ou la vente d'actifs numériques contre une monnaie ayant cours légal ;

⁴² Yanis-Said Khadiri, Village Justice, « *Loi Pacte : Blockchain et crypto-actifs, une histoire de confiance* » <https://www.village-justice.com/articles/blockchain-les-crypto-actifs-une-histoire-confiance,30426.html>

⁴³ Aux nouveaux articles L54-10-1 et suivants du code monétaire et financier.

- l'achat ou la vente d'actifs numériques contre d'autres actifs numériques ;
- l'exploitation d'une plateforme de négociation d'actifs numériques ;
- la fourniture d'autres services connexes tels que la transmission d'ordres pour le compte de tiers ou le conseil aux souscripteurs d'actifs numériques.

L'obtention et le bénéfice de cette licence de PSAN sont optionnels et impliquent le respect de quelques obligations générales comme la transparence de la tarification, la sécurité des systèmes d'information ainsi que des contrôles internes, ou encore la fourniture d'un système de gestion des conflits d'intérêts. La souscription à une assurance responsabilité civile professionnelle ou la disposition d'un certain niveau de fonds propres est également requise.

Paragraphe 2 : Un enregistrement obligatoire auprès de l'AMF pour deux services

Si l'obtention de la licence PSAN est optionnelle, l'exercice des deux premières activités définies implique un enregistrement obligatoire auprès de l'AMF. Il s'agit de la conservation d'actifs numériques pour le compte de tiers ainsi que les services d'achat/vente d'actifs numériques contre une monnaie ayant cours légal. Le premier service consiste techniquement à stocker pour des clients les clés de chiffrement leur conférant le contrôle de leurs crypto-actifs sur une blockchain (une notion qui sera approfondie au sein de la Partie II de la présente). Le second service pour sa part consiste en fait à exploiter le très sensible « passage » entre le monde des crypto-actifs et celui des monnaies étatiques.

Pour avoir le droit de fournir ces deux services, il est donc nécessaire de s'enregistrer auprès de l'AMF, qui statuera après sollicitation de l'avis conforme de l'Autorité de Contrôle Prudentiel et de Résolution⁴⁴. Le règlement général de l'AMF⁴⁵ impose alors aux entreprises de fournir certaines informations à l'autorité conformément à l'article [L-54-10-3](#) du code monétaire et financier. Elles doivent notamment fournir des informations sur l'identité et l'honorabilité des actionnaires, attestant du caractère suffisant de leurs connaissances et compétences notamment grâce à leur formation et expérience professionnelle démontrant de leur capacité respecter les exigences applicables ; sans toutefois être sujets aux interdictions énoncées à l'article [L500-1](#) du CMF – il leur faut essentiellement ne pas avoir fait l'objet de certaines condamnations.

⁴⁴ AMF, « *Obtenir un agrément PSAN* » <https://www.amf-france.org/fr/espace-professionnels/fintech/mes-relations-avec-lamf/obtenir-un-enregistrement-un-agrement-psan>

⁴⁵ Article 721-1 RGAMF

Enfin, l'AMF dispose de six mois à compter du dépôt de dossier pour notifier l'entreprise de sa décision.

Il s'agit en fait d'une procédure très classiques issue de l'univers de la finance qui existe déjà pour l'obtention des nombreux agréments bancaires délivrés par l'ACPR⁴⁶. Bien que les différents agréments soient tous associés à un périmètre d'activités bien défini, il est très aisé pour les banques de tous les obtenir afin de couvrir toutes leurs activités⁴⁷, ce qui complexifie l'accès de la concurrence au marché, contrairement à l'intention initiale du législateur, notamment pour les petites structures pour lesquelles cette procédure représente un certain coût. Ces conditions d'enregistrement auprès de l'AMF après avis de l'ACPR, permettant d'avoir le droit d'exercer ces deux premiers services relevant des PSAN, sont similaires et pourraient là aussi avantager les établissements bancaires face aux plus petites structures, notamment les exchanges, pour l'accès à ce marché.

Paragraphe 3 : La reconnaissance salvatrice d'une forme de droit au compte bancaire pour les entreprises du monde des crypto-actifs

En revanche, de nombreux refus d'ouverture de compte essayés par les porteurs de projets autour de la blockchain⁴⁸ ont poussé le législateur à tenter d'améliorer leur situation. Les émetteurs ayant obtenu l'agrément AMF pour les ICO, et les PSAN ayant été enregistrés ou ayant obtenu un agrément⁴⁹ se sont alors vu garantir par la loi Pacte d'une forme spécifique de droit au compte bancaire⁵⁰.

Les établissements de crédit doivent alors fixer en toute transparence des règles qui incombent à ces acteurs ; en particulier concernant l'ouverture de compte. Un décret⁵¹ permet de rendre ce droit au compte effectif en donnant la possibilité aux entreprises concernées de saisir l'ACPR si elles estiment le refus par la banque d'ouvrir un compte contraire aux règles édictées elles-

⁴⁶ Article L511-10 et suivants du CMF

⁴⁷ D'après le cours de Droit Bancaire de Monsieur le Professeur Laurent Ruet (M1 Droit des affaires 2018-2019 ; au sein du chapitre 1 : l'agrément bancaire).

⁴⁸ Grégory Raymond, Capital, « *Les banques qui interdisent à leurs clients d'acheter des Bitcoins... et les plus ouvertes* » <https://www.capital.fr/votre-argent/les-banques-qui-interdisent-a-leurs-clients-dacheter-des-bitcoins-et-les-plus-ouvertes-1358960>

⁴⁹ Respectivement aux articles L552-4, L54-10-3 et L54-10-5 du CMF

⁵⁰ Gaëlle Marraud Des Grottes, Actualités du droit, « *Prestataires de services sur actifs numériques : le décret est paru !* » <https://www.actualitesdudroit.fr/browse/tech-droit/blockchain/24813/prestataires-de-services-sur-actifs-numeriques-le-decret-est-paru>

⁵¹ Décret codifié à l'article D312-23 du CMF

mêmes par la banque, ou si le refus est fondé sur des règles édictées par la banque qui seraient elles-mêmes contraires à la réglementation. Ce droit au compte garanti aux PSAN et autres porteurs de projets ICO ne favorise pas tellement l'intérêt des établissements bancaires qui jusqu'ici témoignaient, à tort ou à raison, d'une volonté de se tenir éloignées des entreprises de ce secteur. Il s'agit donc là d'une limitation de la liberté contractuelle des banques, d'autant plus que la relation bancaire implique un fort *intuiti personae*, mais qui se justifie par un besoin de promotion de la liberté d'entreprendre dans le domaine des crypto-actifs.

Section 2 : L'application logique aux échanges des exigences en matière de lutte contre le blanchiment et le terrorisme et de protection des investisseurs

Le « passage » entre le monde des crypto-actifs et celui des monnaies étatiques précédemment cité, se trouve au cœur des problématiques de lutte contre le financement du terrorisme ainsi que contre le blanchiment de capitaux, tout comme celles concernant la protection des investisseurs. Mais il reste des cas où la réglementation actuelle ne s'applique pas, ce qui ouvre le débat quant à son adaptation.

Paragraphe 1 : La nécessité d'appliquer les règles LCB-FT pour les services d'achat/vente de crypto-actifs contre de la monnaie ayant cours légal

L'Autorité Bancaire Européenne (EBA) estimait dès juillet 2014⁵² qu'il était nécessaire d'inclure les services sur crypto-actifs dans le champ d'application des dispositions légales pour la lutte contre le blanchiment et contre le financement du terrorisme, notamment concernant la fourniture de service d'échanges de crypto-actifs contre des monnaies étatiques.

Les échanges, entreprises proposant la mise en relation d'acheteurs et de vendeurs de crypto-actifs, exploitent fréquemment ce marché de l'achat/vente de ces actifs numériques contre de la monnaie ayant cours légal telle que définie dans l'article [L111-1](#) du CMF. Elles exploitent également de tels marchés portant sur l'achat/vente de crypto-actifs qui répondent à la qualification d'instrument financier.

⁵² European Banking Authority, "EBA Opinion on 'virtual currencies'" <https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1>

L'activité de ces plateformes se situe donc dans le champ d'application⁵³ de la cinquième directive européenne sur le blanchiment de capitaux ([5AMLD](#)) ainsi que de la seconde directive européenne sur les marchés d'instruments financiers ([MiFID II](#)) qui sont entrées en vigueur en 2018. Ces directives fixent les règles auxquelles les établissements financiers qui fournissent des services d'investissement doivent se plier. Ces établissements doivent notamment dresser un profil de l'investisseur, et vérifier qu'ils disposent des connaissances nécessaires pour l'utilisation de certains produits d'investissement. Il s'agit de l'application au monde des crypto-actifs du principe de la connaissance du consommateur (KYC, Know Your Customer) bien connu des banques et déjà largement pratiqué dans la finance classique. Ils doivent également mettre en place des procédures et mesures adaptées de contrôle interne permettant entre autres l'évaluation des risques ou encore l'identification des bénéficiaires effectifs des mouvements de capitaux⁵⁴. Il faudra finalement que la plateforme soit régulée et supervisée en tant que système multilatéral de négociation⁵⁵.

Les investisseurs, lors de leur inscription sur un échange, doivent donc désormais décliner leur identité à la plateforme pour avoir accès aux services de base, ceci afin de permettre aux enquêteurs de remonter jusqu'à eux, le cas échéant, dans le cadre d'affaires de blanchiment de capitaux ou de financement du terrorisme. De plus, les investisseurs doivent obligatoirement répondre correctement à un questionnaire que leur présentera l'échange pour avoir accès à certains services financiers avancés et risqués, comme des produits dérivés. Par exemple, Kraken, l'un des échanges les plus importants, respecte rigoureusement ces exigences et expose de manière transparente les services auxquels il est possible d'avoir accès selon trois niveaux distincts de vérification de compte client⁵⁶.

Paragraphe 2 : Un flou juridique persistant pour les services d'achat/vente « crypto vers crypto »

⁵³ Comme en dispose l'article L561-2 CMF

⁵⁴ DGCCRF et Tracfin, « Lignes directrices conjointes sur les obligations relatives à la LCB-FT » https://www.economie.gouv.fr/files/files/directions_services/tracfin/pdf/LD-Societes-Domiciliation-2019.pdf

⁵⁵ Me Thibault Verbiest, Planet-Fintech, « Plateformes d'échange de crypto-actifs : quelle régulation ? » https://www.planet-fintech.com/Plateformes-d-echange-de-crypto-actifs-quelle-regulation_a861.html

⁵⁶ Kraken, Payward Inc, "Verification levels explained" <https://support.kraken.com/hc/en-us/articles/360001395743-Verification-levels-explained>

L'Autorité Européenne des Marchés Financiers (ESMA) estime⁵⁷ cependant qu'il persiste un flou juridique sur la manière d'appliquer la réglementation. Pour l'Autorité, il persiste notamment un certain nombre de crypto-actifs qui ne relèvent pas du cadre réglementaire actuel, ce qui pose toujours un problème de risques pour les investisseurs qui ne bénéficient alors que d'une protection limitée voire nulle lorsqu'ils investissent dans ces crypto-actifs.

Il s'agit d'une problématique logique : la réglementation actuelle du LCB-FT pour les échanges ne s'applique que pour les services d'échanges de crypto-actifs qualifiés d'instruments financiers – donc en particulier les jetons de titres (security token) – ou les services d'échanges de crypto-actifs contre des monnaies « fiat ». Il reste donc une zone grise concernant les services d'échanges de crypto-actifs contre d'autres crypto-actifs, qui ne répondent pas ni l'un ni l'autre à une telle qualification ou qui ne réalisent pas de conversion depuis ou vers une monnaie légale, et qui échappent donc logiquement au champ de la réglementation.

Paragraphe 3 : Un débat en cours sur la question de l'extension du régime des PSAN aux échanges « crypto vers crypto »

Ce que note l'ESMA est directement lié au débat auquel se livrent actuellement les acteurs du monde des crypto-actifs en France concernant la possibilité d'une modification du régime français des prestataires de services sur actifs numériques (PSAN). Il est question de rendre obligatoire l'enregistrement des acteurs proposant des services d'échange de crypto-actifs contre d'autres crypto-actifs, et de les soumettre à de nouvelles obligations.

Il s'agirait du troisième type de services sur actifs numériques relevant du régime des PSAN pour lequel l'enregistrement auprès de l'AMF deviendrait obligatoire (c'est actuellement optionnel). Pour rappel, les deux services pour lesquels l'enregistrement est déjà obligatoire, comme décrit précédemment dans la présente, sont la conservation d'actifs numériques pour le compte de tiers ainsi que l'achat/vente de crypto-actifs contre monnaie ayant cours légal.

Il s'agit donc d'imposer aux acteurs proposant des services « crypto vers crypto » de respecter l'ensemble des règles en matière de LCB-FT qui incombent aux établissements bancaires et financiers.

⁵⁷ ESMA, “*Advice: Initial Coin Offerings and Crypto-Assets*”
https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf

L'Association pour le Développement des Actifs Numériques a récemment publié une lettre ouverte⁵⁸ dans laquelle son Président Simon Polrot, qui salue la souplesse et l'ambition du cadre français actuel, plaide pour qu'une telle extension des obligations des PSAN n'ait pas lieu. Selon lui, la réglementation actuelle n'est pas adaptée au cas de figure de l'achat/vente de crypto-actifs vers d'autres crypto-actifs.

« De manière générale, le dispositif LCB-FT “traditionnel” est, sous de nombreux aspects, inadapté aux spécificités des marchés des actifs numériques, et par là même inefficace en matière de prévention et gestion des risques de blanchiment de capitaux et de financement du terrorisme : son application en l'état n'est donc ni raisonnable ni souhaitable. Une rapide observation des dispositions prises au niveau de nos pays voisins permet de confirmer ce constat. Au Luxembourg par exemple, les règles LCB-FT ont été allégées pour s'adapter aux spécificités du secteur et la vérification des mesures LCB-FT est réalisée a posteriori via des audits. Ceci semble déjà plus raisonnable tout en préservant la sécurité financière dont ce dispositif se veut le garant. »

En outre, le Président de l'ADAN soutient que les risques associés à l'échange de crypto-actifs entre eux sont très faibles, comme l'a souligné le ministère de l'économie dans son rapport sur la lutte contre le blanchiment de capitaux et la lutte contre le terrorisme⁵⁹. Il est donc nécessaire selon lui de laisser le temps de la réflexion avant d'assujettir les acteurs exploitant ce type de services à ces lourdes obligations, d'autant plus que l'UE pourrait créer elle-même un cadre harmonisé et adapté à ces services dans les prochains trimestres.

PARTIE II – LA BLOCKCHAIN, NOUVEAU MODE DE GOUVERNANCE DES DONNÉES BANCAIRES

⁵⁸ Simon Polrot, ADAN, « Lettre aux députés sur l'extension du régime des PSAN » <https://www.adan.eu/actualites/lettre-deputes-extension-regime-psan>

⁵⁹ Conseil d'orientation de la lutte contre le blanchiment de capitaux et le financement du terrorisme, Ministère de l'Économie et des Finances, « Analyse nationale des risques de blanchiment de capitaux et de financement du terrorisme en France » https://www.economie.gouv.fr/files/files/directions_services/tracfin/analyse-nationale-des-risques-lcb-ft-en-France-septembre-2019.pdf

La technologie sous-jacente des crypto-actifs, la blockchain, est un condensé d'innovation permettant un nouveau moyen de stocker l'information qui laisse entrevoir de nombreuses nouvelles applications dans le monde bancaire et financier⁶⁰. Les principales difficultés que pose la blockchain en matière de réglementation sont dues à son caractère décentralisé, qui implique une gouvernance sans organe central de contrôle, ainsi qu'à son caractère transparent qui est une conséquence directe du premier.

Chapitre 1^{er} : Un défi de gouvernance posé par le caractère décentralisé de la blockchain

La révolution du Bitcoin, porté par la toute première blockchain, est qu'il s'agit d'une technologie permettant d'envoyer de la valeur à une autre personne en se passant entièrement de tout tiers de confiance. Il s'agit là d'une application pratique d'un système monétaire horizontal. Les milliers de nouveaux crypto-actifs qui depuis ont vu le jour⁶¹, portés par des technologies de blockchain innovantes, tentent d'exploiter plus profondément cette possibilité – y compris au-delà du rôle de monnaie d'échange.

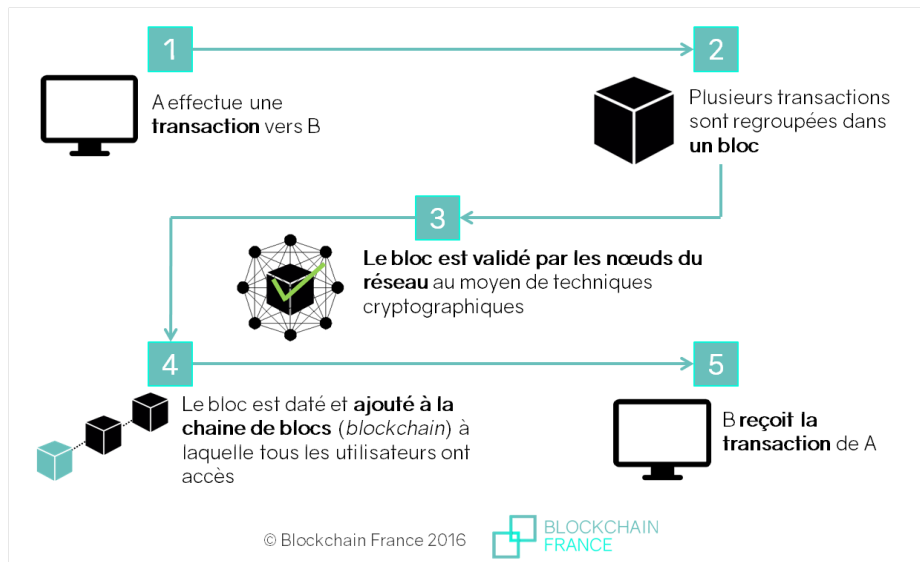
Section 1 : La possibilité nouvelle de se passer du tiers de confiance centralisé

L'innovation apportée par les technologies de registres distribués (DLT) dont la blockchain fait partie est la suppression du tiers de confiance comme source de vérité judiciaire faisant autorité – on peut penser bien-sûr la banque mais aussi au notaire. Cette source d'informations traditionnelle et de confiance est alors remplacée par le consensus obtenu par les différents administrateurs de « nœuds », les multiples systèmes d'information qui enregistrent et sécurisent les informations. Ils possèdent chacun leur propre copie de la chaîne de blocs, qui est ainsi accessible à tous les membres de ce réseau de pair à pair⁶².

⁶⁰ Observatoire des métiers de la banque, « *Impact de la blockchain sur les métiers et compétences de la banque* » http://www.observatoire-metiers-banque.fr/f/etudes/sf/plus/s/impact_blockchain_metiers_banque

⁶¹ Le Ministère de l'économie dénombrait 1600 crypto-actifs différents en 2018. Il est probable qu'il en existe plus de 3000 aujourd'hui <https://www.economie.gouv.fr/particuliers/cryptomonnaies-cryptoactifs>

⁶² Le pair à pair ou peer to peer (P2P) est un modèle d'échange en réseau où chaque entité est à la fois client et serveur ; évitant le recours à un serveur central. L'application la plus répandue du P2P est le partage de fichiers sur internet.

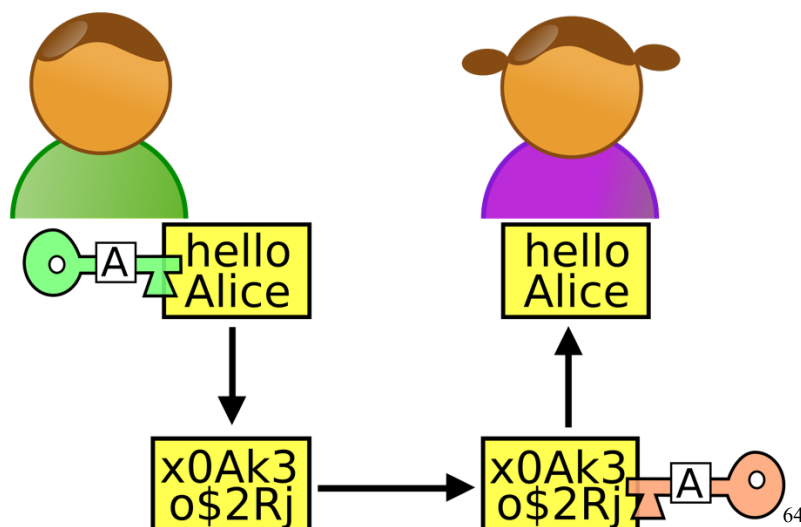


Cette chaîne de blocs qui s'empilent est la majeure innovation apportée par la blockchain aux DLT : chaque bloc est interdépendant du précédent, notamment parce qu'il contient son empreinte électronique, de telle sorte qu'il est impossible de falsifier les précédentes transactions sans que cela ne soit visible.

Paragraphe 1 : Une opacité partielle des informations sur la Blockchain, conséquence de l'absence d'organe central d'identification

La blockchain utilise la technologie du chiffrement asymétrique pour identifier les membres du réseau.

⁶³ Schémas produits par Blockchain France <https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/>



La clé publique est le moyen d'identification sur la blockchain : c'est à celle-ci que sont rattachées les informations liées à une personne. Sa dérivée constitue l'adresse publique d'une personne sur la blockchain, par l'intermédiaire de laquelle il est notamment possible de lui transmettre des jetons. En revanche, la clé privée est le moyen d'authentification pour la personne pour prouver qu'elle « possède » les crypto-actifs associés à son adresse publique, lui permettant d'en prendre le contrôle. Elle peut alors notamment envoyer des fonds (payment token) à l'adresse publique de son choix sur la blockchain. La clé publique, comme la clé privée, sont deux chaîne de lettres et de chiffres uniques représentant l'utilisateur. Elles sont unies par une relation mathématique.

Ainsi, les membres du réseau bénéficient d'une forme de pseudonymat⁶⁵ : ils ne sont identifiés sur la blockchain que par leurs adresses publiques. Cette adresse est comparable à un numéro de compte en banque, bien qu'il ne soit directement relié à aucune identité. Il est possible de pousser jusqu'à l'analogie avec le système du RIB et du PIN⁶⁶ : le premier est destiné à la communication au public afin de recevoir des fonds, et le second sert à l'inverse à les retirer, et doit être gardé secret. Une différence réside alors dans le fait que la blockchain ne fait pas appel à un tiers de confiance pour connaître l'identité qui se cache derrière un de ces « comptes ». Il est donc difficile de savoir qui contrôle quelles données, où et quand, et ainsi déterminer qui

⁶⁴ Schéma provenant de Wikipédia (chiffrement asymétrique).

⁶⁵ Le pseudonyme identifie un propriétaire, c'est-à-dire une ou plusieurs personnes le possédant mais qui ne divulguent pas leurs propres noms (leurs identités légales).

⁶⁶ Clément Tequi, François Hiault et Martin Della Chiesa, « *Blockchain : Vers de nouvelles chaînes de valeur* » pages 89 et 90

est responsable légalement. Une conséquence de ce fonctionnement est également la difficulté de déterminer la loi applicable à une transaction ou encore la juridiction compétente pour un litige⁶⁷.

C'est bien pour cela que la régulation, comme exposé précédemment dans la présente, a tenté d'appliquer les règles de LCB-FT aux plateformes d'échange de crypto-actifs ; ceci afin d'identifier les personnes qui échangent des crypto-actifs contre des actifs répondant à la qualification d'instruments financiers.

Paragraphe 2 : Les « smart contracts », nouveaux concurrents du droit financier ?

Il ne faut pas traduire la fameuse expression *code is law*⁶⁸ au sens propre⁶⁹ ! Les *smart contracts* consistent à former et mettre en œuvre automatiquement les termes pouvant provenir d'un réel contrat en les traduisant en langage informatique. Il s'agit de programmes du type « if ... then » (« si telle condition, telle conséquence »). Lorsque ces termes arrivent à échéance, les smart contracts les exécutent de manière totalement automatique ; ceci par l'intermédiaire des nœuds sécurisant la blockchain⁷⁰.

Aujourd'hui ces mal nommés *contrats intelligents* ne peuvent pas être assimilés à des contrats : les conditions classiques de la formation d'un contrat ne sont que rarement vérifiables, et l'un des défis consiste à savoir si le cocontractant a véritablement compris le code développé dans le programme. Il ne s'agit pour le moment que de programmes informatiques exécutant des transactions, entre autres. Ces programmes ne sont donc pour le moment que des modalités d'exécutions d'accords préalablement conclus⁷¹. Néanmoins l'évolution de cette technologie

⁶⁷ Plisson, Claire Fénéron. « *La blockchain, un bouleversement économique, juridique voire sociétal* », *I2D – Information, données & documents*, vol. 54, no. 3, 2017, pp. 20-22.

⁶⁸ *Code is law* est une expression de Lawrence Lessig, un juriste américain de notoriété internationale et professeur de droit au Harvard Law où il a fondé le *Center for Internet and Society*. Lessig est l'auteur d'un article « Code is law » paru en 2000 dans lequel il énonce l'idée que le cyberspace constitue une réelle menace pour les libertés.

⁶⁹ Mustapha Mekki, Dalloz Etudiant Actu, « *Droits(s) et algorithmes : de la blockchain à la justice prédictive* » <https://actu.dalloz-etudiant.fr/le-billet/article/droitss-et-algorithmes-de-la-blockchain-a-la-justice-predictive/h/d66e9db5333715c8ff6d88221cf44721.html>

⁷⁰ Elise Huber, Village Justice, « *Les smart contracts : contrats non identifiés ?* » <https://www.village-justice.com/articles/les-smart-contracts-contrats-non-identifies,28893.html>

⁷¹ Simon Polrot, Blockchain Partner, « *Panorama des enjeux juridiques de la blockchain* » <https://blockchainpartner.fr/wp-content/uploads/2017/06/Enjeux-juridiques-de-la-blockchain-Etude-Blockchain-Partner.pdf>

pourrait amener les acteurs économiques à programmer des contrats intelligents de plus en plus complexes se plaçant comme de réels accords.

Une accumulation minimale d'actions pourrait donner accès à divers avantages du système ou constituer une adhésion à une sorte de club. Il est possible de créer des organisations autonomes décentralisées, des sociétés qui existent entièrement dans le cadre de contrats intelligents sur une chaîne de blocs, qui pourraient avoir des mécanismes de gouvernance incluant des actionnaires humains codant les préférences de vote directement dans le « contrat ».

Tel est le cas d'une nouvelle technologie blockchain nommée DAO (Decentralized Autonomous Organization). Il s'agit comme son nom l'indique d'une organisation autonome et décentralisée dont les règles de gouvernance sont automatisées et inscrites de façon immuable et transparente dans la blockchain. Un fond d'investissement nommé TheDAO a pour la première fois mis en œuvre cette technologie par l'intermédiaire d'une ICO ayant permis de lever 120 millions de dollars en 2016⁷².

Paragraphe 3 : La finance décentralisée (DeFi), une insaisissable atteinte au monopole bancaire

Les contrats intelligents et les fonctionnalités de plus en plus avancées que la blockchain permet de mettre en œuvre sont en train de révolutionner la finance d'une toute autre manière que ce qui existe avec les ICO/STO. Il s'agit de la *finance décentralisée* (Decentralized Finance, DeFi), aussi appelée finance ouverte (à ne pas confondre avec l'open banking), dont les usages sont variés et promettent de révolutionner de nombreuses activités classiques de banque.

La finance décentralisée s'appuie sur trois principes clés – notamment mis en œuvre par cette fameuse DAO sur la blockchain d'Ethereum⁷³ – afin de débloquer des liquidités, accroître la sécurité et la transparence financières et exploiter un système économique intégré et normalisé⁷⁴. Ces principes sont la *programmabilité* (la capacité de pouvoir être programmé ou établi à l'avance), *l'immutabilité* (ce qui par nature demeure identique et ne peut subir de

⁷² Financial Times, « *Automated company raises equivalent of \$120m in digital currency* » <https://www.ft.com/content/600e137a-1ba6-11e6-b286-cddde55ca122>

⁷³ Ethereum est un protocole blockchain créé en 2015 par Vitalik Buterin. Cette blockchain supporte des échanges décentralisés permettant la création par les utilisateurs de contrats intelligents grâce à un langage Turing-complet. <https://ethereum.org>

⁷⁴ Alethio Analytics, Everett Muzzy, Danning Sui, Bogdan Gheorge, « *Ethereum Decentralized Finance Report* » <https://pages.consensys.net/ethereum-decentralized-finance-report-alethio>

changement) et *l'interopérabilité* (capacité d'un système à fonctionner sans restriction avec d'autres systèmes existants ou futurs).

Grâce à la finance décentralisée, il devient notamment possible, pour un membre du réseau, d'emprunter tout ce qu'il souhaite tant qu'il est en mesure de placer une certaine quantité d'un crypto-actif prédéfini en garantie⁷⁵ (soit une forme de collatéral⁷⁶). Il est donc concrètement proposé aux membres du réseau d'accéder à de la liquidité en mettant des actifs en garantie, ce qui représente un des cœurs de métiers de la banque d'investissement. Dans ce système, les décisions sont entièrement dépolitisées : il n'y a pas de discrimination des emprunteurs car l'opération est entièrement exécutée sur la blockchain par le programme informatique du contrat intelligent. Il s'agit en fait du déclenchement de prêts de pair à pair dont les modalités (montant en jetons, garantie, échéance, taux d'intérêts, etc.) sont définies au sein-même de cette organisation décentralisée, sans distinction entre les personnes ; les adresses publiques sur la blockchain masquant les identités des bénéficiaires effectifs. Ces modalités sont calculées à la volée selon le contexte du marché, notamment en fonction du rapport entre l'offre et la demande formé par la rencontre des offreurs et des demandeurs de ce type de service à un instant précis sur la blockchain. Il existe également de nombreux services inexistant dans la finance classique, qui sont accompagnés de mécanismes de diminution des risques, notamment les « *flash loans* » : il s'agit de prêts d'une durée de quelques secondes permettant d'effectuer une série prédéterminée d'opérations à la condition d'être immédiatement en capacité de rembourser les fonds prêtés. Les mouvements des fonds sont alors calculés à l'avance de manière instantanée et effectivement prêtés si les conditions sont réunies⁷⁷.

Ainsi, il n'y a pas d'interlocuteur unique établissant un profil de l'emprunteur et du risque que son projet comporte pour l'établissement bancaire – bien que les emprunts effectués par l'intermédiaire de ce nouveau système ne soient pas sans risque non plus, ce risque étant compensé par le taux d'intérêt et le collatéral, selon les liquidités disponibles. Les barrières classiques de l'accès au crédit tombent alors, notamment vis-à-vis de la situation personnelle de l'emprunteur (situation professionnelle, projet objet du financement sollicité, etc.).

⁷⁵ Coinhouse, « *Qu'est-ce que la finance décentralisée ?* »

<https://www.coinhouse.com/fr/apprendre/blockchain/la-finance-decentralisee/>

⁷⁶ Le collatéral est un actif déposé en garantie par le débiteur au prêteur lors d'un emprunt. Si le débiteur est défaillant, le prêteur a le droit de conserver les actifs remis en collatéral en dédommagement.

⁷⁷ Grégory Raymond, Brice Berdah, Podcast 21 Millions, Capital, « *La finance décentralisée (DeFi), une banque sans banquiers* » à la 27^e minute <https://soundcloud.com/21millions>

Un aspect important de la finance décentralisée est qu'elle s'appuie tout particulièrement sur des jetons stables : par exemple, l'un des jetons stables les plus populaires est le DAI⁷⁸, un crypto actif garanti par des dollars américains (USD). La finance décentralisée permet ainsi chacun d'effectuer des opérations de crédit à titre habituel, ce qui contrevient directement au monopole bancaire⁷⁹, exposant alors en principe les personnes s'y adonnant à de lourdes sanctions⁸⁰. Cependant, aucun organe central n'exploite ces services de pair à pair – contrairement aux activités des échanges ou encore celles des porteurs de projets ICO. Le droit actuel régissant le monopole bancaire semble alors inapplicable : bien que les personnes juridiques (les membres du réseau) contrevenant à ce monopole via la finance décentralisés se situent manifestement dans son champ d'application, elles semblent hors d'atteinte puisqu'anonymes et à distance du circuit financier classique. En effet, les entreprises qui exploitent les services de conversion de crypto-actifs en monnaie « fiat », qui sont des personnes morales et sujets aisément accessibles pour la régulation présentée jusque-là (notamment avec le régime des PSAN décrit en Partie I), n'entrent pas ici directement en jeu. Il semble donc que les établissements bancaires aient alors tout intérêt à ce que la régulation actuelle évolue afin protéger leur monopole d'activité historique, bien que la tâche semble ardue.

Section 2 : Le renouvellement du rôle de tiers de confiance avec la blockchain, une opportunité des établissements bancaires

Le fonctionnement décentralisé de la blockchain a en apparence éliminé le tiers de confiance, tout au moins, dans ses rôles classiques des systèmes centralisés que nous connaissons. La blockchain offre de nouvelles opportunités pour le tiers de confiance, notamment concernant les aspects pour lesquels la blockchain a besoin d'un lien avec la « réalité ».

Paragraphe 1 : Les banques, possibles garantes des clés privées (wallet)

⁷⁸ Les jetons de DAI, qui correspondent à des instruments financiers au sens du code monétaire et financier, sont générés sur la blockchain via l'établissement d'un contrat intelligent lors du dépôt d'Ethers (les jetons de la blockchain Ethereum) en garantie. <https://makerdao.com/fr/>

⁷⁹ L'article L511-5 du CMF dispose des termes suivants : « *Il est interdit à toute personne autre qu'un établissement de crédit ou une société de financement d'effectuer des opérations de crédit à titre habituel.* »

⁸⁰ L'article L571-3 du CMF punit de trois ans d'emprisonnement et de 375 000 euros d'amende le non-respect de l'interdiction édictée à l'article L511-5 du même code.

C'est la clé privée de chiffrement, reliée par une fonction cryptographique à l'adresse publique correspondante sur la blockchain, permet de signer les transactions et de prouver son identité aux pairs sur le réseau. Cette clé est donc le seul moyen permettant de s'authentifier afin de disposer des crypto-actifs associés à un « compte » (*wallet*) de la blockchain. Sans la clé privée, les jetons sont immobilisés sur l'adresse publique dans la blockchain, visibles aux yeux de tous les membres du réseau, mais sans possibilité d'utilisation et donc perdus à jamais.

La mort du patron de l'échange canadien QuadrigaCX en décembre 2018, qui était l'unique personne en possession des clés privées des adresses blockchain de son service, fut une cruelle leçon pour ses 100 000 clients : l'équivalent de 125 millions d'euros en crypto-actifs leur appartenant était alors devenu inaccessible. L'entreprise, en faillite et croulant sous les demandes de retrait des fonds de ses créanciers, avait été placée sous la protection de la loi⁸¹.

La perte des clés privées – ou leur divulgation au public – est la hantise de tout propriétaire de crypto-actifs et cristallise la réalité technique de la blockchain : aucune autorité centrale ne peut « décider » de débloquer des fonds perdus, ou de rapatrier des fonds volés. Il n'existe pas de fonction comparable à une réinitialisation du mot de passe ou encore à une réécriture comptable dans cet univers.

La garde des clés privées, qui ne peuvent être raisonnablement confiées à un seul homme, pourrait alors constituer une nouvelle activité pour un tiers de confiance. Les établissements bancaires pourraient alors jouer ce rôle de tiers garde des clés privées, comme une évolution moderne de leur rôle historique de garde physique de fonds. Ils pourraient alors proposer à leurs clients des solutions de garde des clés cryptographiques dont il existe déjà différentes sortes⁸². Autant si ce n'est plus que pour n'importe quel autre type de mot de passe, le maintien de la sécurité et du secret d'une clé privée d'une adresse blockchain s'annonce comme un enjeu absolument critique, et pourrait s'apparenter comme une nouvelle activité de banque.

⁸¹ Gregory Barber, Wired, "A Crypto Exchange CEO Dies—With the Only Key to \$137 Million"
<https://www.wired.com/story/crypto-exchange-ceo-dies-holding-only-key/>

⁸² Journal Du Net, « *Wallet : qu'est-ce qu'un wallet et comment le choisir ?* »
<https://www.journaldunet.fr/patrimoine/guide-des-finances-personnelles/1208977-wallet/#:~:text=Un%20%22wallet%22%2C%20dont%20la,physique%20ou%20num%C3%A9rique%2C%20de%20cryptomonnaies.>

Paragraphe 2 : Les banques, possibles « oracles » fournissant l'information extérieure à la blockchain

Le services d'« Oracle » est comme une « passerelle » entre la blockchain et le monde réel. Tout comme dans la mythologie grecque ancienne, un oracle relie deux royaumes : tout en étant lui-même un contrat intelligent, l'oracle est utilisé par d'autres contrats intelligents afin de récupérer des informations du « monde réel », c'est-à-dire toute information extérieure et nécessaire qui n'est pas encore stockée sur la Blockchain. En effet, l'oracle, service exploité par un tiers de confiance, est nécessaire aux ordinateurs du réseau d'une blockchain qui ne peuvent pas récupérer des informations externes par eux-mêmes – une pratique qui introduirait un aléa dans la qualité de l'information récupérée et empêcherait tout consensus des nœuds du réseau⁸³.

Cette information est parfois nécessaire au dénouement de certains contrats intelligents : par exemple, dans le cadre d'un pari sur le résultat d'un match sportif, c'est l'oracle qui injectera dans la blockchain, en temps voulu, ledit résultat nécessaire à l'exécution du contrat intelligent. L'oracle est rémunéré pour jouer ce rôle, et doit l'être assez pour éviter toute tentation de corruption : une information erronée injectée dans la blockchain fausserait le résultat de nombreux contrats intelligents. Paradoxalement, il s'agit là d'un élément nécessairement centralisé et à l'opposé de la philosophie et du fonctionnement des crypto-actifs et de la blockchain. Le détournement de ce dernier « maillon » de la chaîne anéantirait ainsi tout l'intérêt de cette technologie.

Dans l'univers de la finance, la fourniture dans des délais extrêmement courts d'une information précise et exacte représente un enjeu élevé, tout particulièrement concernant les marchés financiers. Un acteur éminent du domaine est Bloomberg⁸⁴, qui exerce une activité d'information financière qui répond aux mêmes besoins que ceux de la finance décentralisée. Ainsi, il est aisément concevable que les établissements financiers exercent cette activité d'oracle, en tant que tiers de confiance privilégié, afin d'injecter dans la blockchain des informations cruciales et extérieures, à propos de taux d'intérêts ou encore des informations

⁸³ Legal Tech Blog, “*The Problem of Blockchain Oracles – Interview with Alexander Egberts*” <https://legal-tech-blog.de/the-problem-of-blockchain-oracles-interview-with-alexander-egberts>

⁸⁴ Bloomberg est un groupe financier américain spécialisé dans les services aux professionnels des marchés financiers.

relatives à la valorisation précise d'un crypto actif en monnaie fiat. En outre, la conformité de nombreux services financiers requiert l'application de valeurs variables dans le temps, par exemple celle du taux d'intérêt légal⁸⁵ qui est fixé par décret : il pourrait bien s'avérer nécessaire à l'avenir d'injecter ce type d'information dans la blockchain.

Paragraphe 3 : Les banques, possibles garantes des actifs sous-jacents des jetons

Les jetons stables (stablecoin) sont des crypto-actifs particulièrement pertinents pour la création de systèmes de paiement, qui nécessitent une faible volatilité de la valeur de l'actif. Comme leur nom l'indique leur valeur a pour vocation d'être stable dans le temps. Si leur valeur est garantie par une monnaie ayant cours légal comme l'euro, les jetons stables pourraient représenter une certaine prolongation des politiques monétaires de banque centrale profitant en pratique des avantages de la blockchain. Il faudra alors pour le législateur européen trancher entre le régime des instruments financiers⁸⁶ – comme le préconise l'AMF – ou le régime de la monnaie électronique⁸⁷.

Des études quant à la possibilité de créer un jeton stable officiel de banque centrale sont évoquées partout dans le monde notamment en Chine et aux États-Unis. L'UE n'est pas en reste : Christine Lagarde a récemment rappelé que la Banque Centrale Européenne, dont elle est la Présidente, avait créé un groupe de travail expert afin d'étudier l'intérêt et la faisabilité d'un jeton numérique de banque centrale. Elle a également déclaré qu'il ne serait pas fait « *barrage aux initiatives privées* »⁸⁸ ce qui est un signe encourageant pour les établissements bancaires. Ces derniers pourraient, tenir dans ce cadre un nouveau rôle de garant en administrant la monnaie sous-jacente du jeton stable pour le compte de la banque centrale – en assurant la *tokenisation*⁸⁹ des jetons émis sur la blockchain – en plus de proposer leurs propres services commerciaux associés. Par ailleurs, les établissements bancaires pourraient également assurer la tokenisation des jetons émis par des titres financiers, afin d'émettre sur une blockchain des jetons de titres (security token). Les banques pourraient en fait jouer le rôle de

⁸⁵ Au sens des articles L313-2 et suivants du CMF.

⁸⁶ Article L211-1 CMF

⁸⁷ Article L315-1 CMF

⁸⁸ European Central Bank, « *Christine Lagarde: Interview with "Challenge" Magazine* » <https://www.ecb.europa.eu/press/inter/date/2020/html/ecb.in200108~f3ba434000.en.html>

⁸⁹ En informatique, la tokenisation est le procédé permettant de remplacer une donnée critique par un élément équivalent qui n'aura aucune valeur intrinsèque ou signification exploitable une fois sortie du système (définition Wikipédia). Dans le monde des crypto-actifs, il s'agit de lier un actif à son équivalent, qui est un jeton sur la blockchain. D'où le terme « crypto-actif ».

lien entre un actif (notamment une monnaie étatique ou un titre financier) et sa représentation sur une blockchain (crypto-actif, donc).

La surnommée « *Ordonnance Blockchain*⁹⁰ » traite des titres de capital et les titres de créance qui ne sont pas négociés sur une plateforme de négociation relevant de MiFID II⁹¹ et qui ne sont pas admis aux opérations d'un dépositaire central. La tenue du registre des titres entre dans le champ d'application de cette ordonnance ainsi que la livraison desdits titres. Ces activités peuvent déjà s'effectuer sous forme de jeton de titre par l'intermédiaire d'une blockchain, sans tiers de confiance donc, et ne posent pas actuellement de difficulté juridique⁹².

De nombreuses personnes estiment que les prochains systèmes de paiements massivement adoptés utiliseront la blockchain – qui n'a pas les défauts des systèmes centralisés actuels – ce qui provoquerait même la fin du paiement en espèces⁹³. C'est notamment le cas de David Marcus, ancien président de Paypal⁹⁴ et cofondateur de Libra⁹⁵, un projet de jeton stable initialement conçu pour être garanti par un panier de plusieurs monnaies étatiques – et qui relèverait donc de la compétence de plusieurs régulateurs simultanément ; ce qui semble en l'espèce extrêmement délicat. Le projet, dont le lancement est toujours prévu pour 2020, a d'ailleurs reçu un accueil glacial de la part de différents gouvernements, rappelant les réticences de nombreuses institutions aux crypto-actifs jusqu'à récemment. En France, le ministre des finances Bruno Lemaire avait catégoriquement refusé l'autorisation du projet Libra sur le sol européen, arguant que la souveraineté des États était en jeu⁹⁶.

⁹⁰ Ordonnance n° 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers
<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000036171908>

⁹¹ Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers ; déjà évoquée en Partie I

⁹² AMF, « *État des lieux et analyse relative à l'application de la réglementation financière aux security tokens* »
https://www.amf-france.org/sites/default/files/2020-03/analyse-juridique-security-tokens-amf-fr_2.pdf

⁹³ Le Monde, « *La fin du paiement cash : Pour David Marcus, « Des services vont se développer autour de l'argent programmable et de Libra »* » https://www.lemonde.fr/economie/article/2020/06/07/la-fin-du-paiement-cash-les-crisis-renforcent-les-tendances-deja-en-cours_6042071_3234.html

⁹⁴ Paypal est une entreprise américaine offrant un service de paiement en ligne utilisant la monnaie électronique – qui est à distinguer des crypto-actifs – dans le monde entier.

⁹⁵ Libra est le projet de jeton stable porté par Facebook ainsi que d'autres entreprises et institutions partenaires issues notamment du monde de la finance. <https://libra.org/>

⁹⁶ Antonio Rodriguez et AFP, La Tribune, « *Cryptomonnaie : la France ne veut pas du Libra de Facebook sur le sol européen* » <https://www.latribune.fr/entreprises-finance/banques-finance/cryptomonnaie-la-france-ne-veut-pas-du-libra-de-facebook-sur-le-sol-europeen-828007.html>

Chapitre 2^e : Une application complexe de la régulation de la protection et de la sécurité des données à la blockchain

La blockchain est un concentré de technologies comportant de nombreux aspects qui concernent la gouvernance des données. Ces aspects relèvent essentiellement de l'application à la blockchain du droit des données personnelles et du droit relatif à la cybersécurité.

Section 1 : Une apparente difficile conciliation du RGPD et de la blockchain

La blockchain est d'abord une technologie de registre distribué (DLT) : son objet premier est le stockage de données au sein de systèmes d'information. Il s'agit notamment d'informations assimilables à des données bancaires, qui sont particulièrement sensibles. Cette technologie est donc un sujet d'application du droit des données, notamment du RGPD⁹⁷. Il apparaît alors essentiellement deux points de tension : l'absence de contrôle centralisé des données de la blockchain ainsi que sa directe conséquence sur leur gouvernance⁹⁸.

Paragraphe 1 : Le responsable de traitement, une notion peu pertinente vis-à-vis des DLT

Le RGPD repose sur l'hypothèse selon laquelle pour chaque donnée à caractère personnel, il existe au moins une personne physique ou morale – le responsable du traitement – à laquelle les personnes concernées peuvent s'adresser pour faire appliquer leurs droits. Cependant, la blockchain est une grande base de données distribuée qui remplace l'acteur unitaire par de nombreux acteurs différents, ce qui entrave la répartition des responsabilités et donc l'attribution de l'obligation de rendre compte.

Selon une analyse de la CNIL⁹⁹, les responsables de traitement au sein de la blockchain sont toutes les personnes ayant droit d'écriture sur la chaîne – qui disposent donc d'une clé privée reliée à une adresse publique – pouvant ainsi soumettre des données à validation par les nœuds

⁹⁷ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

⁹⁸ Dr Michèle Fink, European Parliament, “*Blockchain and the General Data Protection Regulation : Can distributed ledgers be squared with European data protection law?*”
[https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)634445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf)

⁹⁹ CNIL, « *Premiers éléments d'analyse de la CNIL : blockchain* »
https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf

du réseau. Elle écarte d'emblée de cette qualification les personnes contrôlant les nœuds du réseau, qui ne font que valider les transactions et n'exercent pas directement de contrôle sur les données produites. Par opposition, ces personnes administrant des nœuds du réseau, ou encore les développeurs de contrats intelligents devraient pouvoir être qualifiés de sous-traitants au sens du RGPD, ce qui est un régime favorable à la création de services de finance décentralisée par les établissements bancaires.

La CNIL précise également dans son analyse que le participant devrait être considéré comme responsable de traitement s'il s'agit d'une personne morale, ou s'il s'agit d'une personne physique agissant dans le cadre d'une activité professionnelle ou commerciale. La CNIL précise de plus son analyse jusqu'à l'activité de bancaire : « *Si une banque inscrit les données de ses clients dans une blockchain dans le cadre de ses traitements de gestion des clients, elle est responsable de traitement* ». Cela pourrait s'appliquer à l'une des nouvelles potentielles activités de tiers de confiance à la blockchain que pourraient exercer les établissements bancaires : le service d'oracle précédemment décrit.

En outre, cette doctrine de la CNIL concerne tout particulièrement à la gestion des banques de leurs fichiers clients. La blockchain pourrait en effet représenter une solution¹⁰⁰ à la problématique de connaissance du consommateur (KYC), un classique de l'activité de banque exploré en Partie I. La blockchain était alors le problème en lui-même (KYC et échanges), mais elle pourrait être également représenter une solution efficace pour optimiser et simplifier la connaissance du consommateur requise par la réglementation financière – et, plus largement, représenter un puissant outil décentralisé en réponse à la problématique d'identité numérique¹⁰¹.

Paragraphe 2 : Une conciliation entre l'immutabilité des données dans la blockchain et le RGPD matériellement impossible

C'est l'articulation entre ce droit à l'effacement et le fonctionnement d'une chaîne de blocs, délibérément conçue afin de rendre la modification unilatérale des données difficile, voire impossible. Ceci est bien sûr difficile à concilier avec les exigences du RGPD selon lesquelles

¹⁰⁰ Adlen Bouchenafa, Nofel Goulli, « La blockchain pour optimiser le KYC », article initialement publié dans la Revue Banque n°841 (février 2020) <http://www.revue-banque.fr/management-fonctions-supports/article/blockchain-pour-optimiser-kyc>

¹⁰¹ Blockchain Partner, « Vers une identité numérique « private by design » » <https://blockchainpartner.fr/vers-une-identite-numerique-private-by-design/>

les données à caractère personnel doivent être modifiées (article 16 du RGPD) et effacées (article 17 du RGPD) dans des circonstances spécifiques.

En effet, personne n'est en capacité de rectifier ou de supprimer ces informations sur la blockchain, qui sont comme inscrite dans le marbre suite au consensus trouvé à un instant précis par les nœuds du réseau. Cette technologie permet alors de retracer toutes les transactions ayant eu lieu depuis le début de la chaîne. La chaîne de blocs permet également de connaître de manière certaine toutes les adresses publiques par lesquelles sont passés tous les crypto-actifs ; ce qui lui fait ressembler à un immense historique de virements bancaires. Les transactions passées donc, mais également aussi toutes les traces laissées par les services blockchain, sont comme condamnés à rester visibles aux yeux de tous les membres du réseau, sans espoir d'être un jour effacées ou rectifiées.

Au contraire, le droit à l'information, le droit d'accès tout comme le droit à la portabilité ne posent pas de difficultés lors de l'utilisation de la blockchain, qui est en conformité *by design* sur ces points. La blockchain est en effet accessible à tous, interopérable avec d'autres technologies et entièrement transparente ; bien que les utilisateurs soient masqués par le pseudonyme que sont leurs adresses publiques.

Une actualité récente¹⁰² illustre parfaitement ce phénomène : en mai 2020, 40 Bitcoins (d'une valeur d'environ 400 000 USD au moment des faits) ont été déplacés pour la première fois. Ces Bitcoins avaient été créés durant le premier mois de l'existence de la blockchain du Bitcoin (2009), ce qui avait alimenté de nombreuses spéculations à propos d'un possible retour du légendaire Satoshi Nakamoto.

Paragraphe 3 : L'adresse publique sur une blockchain, une donnée personnelle riche éclipsant le secret bancaire

L'adresse publique n'identifie pas directement la personne qui détient les crypto-actifs associés, d'où une certaine opacité concernant les bénéficiaires effectifs des transactions sur une blockchain, qui est paradoxalement transparente. Cependant, l'adresse publique la rend

¹⁰² Zoe De La Roche, The Coin Tribune, « *Jusqu'où le Syndrome Satoshi tirera-t-il le Marché ?* » <https://www.thecointribune.com/actualites/bitcoin-le-21-mai-2020-jusquou-le-syndrome-satoshi-tirera-t-il-le-marche/>

identifiable si elle est associée à une autre information, notamment telle que l'identité de l'utilisateur contenue dans le fichier KYC d'un échange. L'adresse publique répond alors à la qualification de donnée personnelle au sens du RGPD¹⁰³. Une fois une adresse publique reliée à une identité, l'opacité tombe et il devient possible de retracer toutes les transactions effectuées par la personne par l'intermédiaire de cette adresse. Dans le cadre d'une activité de banque, cette transparence semble à priori impossible à concilier avec le secret bancaire¹⁰⁴.

Pour contrecarrer ceci, le « White paper »¹⁰⁵ du Bitcoin, recommandait dès 2008, encore une fois en précurseur, qu'une nouvelle paire de clés soit utilisée pour chaque transaction afin d'éviter qu'elles ne soient liées à un propriétaire commun tout en admettant qu'il s'agit simplement d'une technique de sécurité plutôt que d'une réelle anonymisation : « *Certains liens sont encore inévitables dans le cas de transactions à entrées multiples, qui révèlent nécessairement que leurs entrées appartiennent au même propriétaire. Le risque est que si le propriétaire d'une clé est révélé, le lien pourrait tout de même révéler toutes les autres transactions ayant appartenu au même propriétaire.* »

Ce phénomène doit cependant être relativisé : lorsque des entreprises comme les échanges utilisant leur propre adresse publique sur la blockchain pour stocker les crypto-actifs de leurs clients, les clés publiques se rapportent à l'entité qui est une personne morale. Les clés publiques ne correspondent pas aux utilisateurs finaux personnes physiques – qui sont reliés à leurs crypto-actifs par le système d'information centralisé de l'échange – et donc dans ce cas, ne répondent à priori pas à la qualification de donnée personnelle. Cela ressemble aux comptes que possèdent les banques commerciales auprès de la banque centrale : ceux-ci ne donnent aucune information concernant la répartition des fonds entre les clients de la banque.

Section 2 : Des innovations de la blockchain en matière de sécurité des systèmes d'information déjà fortement réglementées

La blockchain repose sur différentes technologies de cryptographie ainsi que de protocoles de sécurité afin d'assurer sa gouvernance : chiffrement symétrique, asymétrique ou encore

¹⁰³ L'article 4 du RGPD dispose des termes suivants : « Aux fins du présent règlement, on entend par « données à caractère personnel » toute information se rapportant à une personne physique identifiée ou identifiable. ».

¹⁰⁴ Les règles concernant l'étendue du secret bancaire sont codifiées au sein des articles L511-33 et suivants du code monétaire et financier.

¹⁰⁵ « White paper » du Bitcoin <https://bitcoin.org/bitcoin.pdf>

fonction de hashage¹⁰⁶. Il s'agit d'une exploitation innovante de technologies bien connues de l'industrie, notamment bancaire, dont l'utilisation est déjà fortement réglementée.

Paragraphe 1 : La nécessaire reconnaissance de la force probante des données (bancaires) de la blockchain

La blockchain repose sur des techniques de cryptographie afin d'assurer l'intégrité des transactions. Cependant, bien qu'il soit possible de prouver mathématiquement que les transactions d'une chaîne de blocs sont valables, de prouver leur horodatage ou de savoir qui est associé aux données ; cela n'assure en rien la possibilité de démontrer que ces données n'ont pas été altérées afin de les rendre juridiquement contraignantes¹⁰⁷.

L'une des conditions requises pour que les données de la blockchain puissent acquérir un statut juridique est la reconnaissance des signatures en chaîne (qui a effectué la transaction) ; l'horodatage (quand la transaction a-t-elle été effectuée) ; les validations (qui a validé le transactions) ; et les données de fonds (c'est-à-dire les données contenues dans la transaction ou dans le contrat intelligent).

En premier lieu, l'[article 1366](#) du code civil dispose des termes suivants : « *L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.* ». La loi française n'est donc pas hostile par principe à la potentielle valeur probante des données de la blockchain. Mais ces questions sont traitées de manière plus approfondies au niveau européen, notamment par le Règlement [eIDAS](#)¹⁰⁸. Tout d'abord, selon ce règlement européen, la force juridique des documents ne peut être refusée simplement parce qu'ils sont sous forme électronique. Ce règlement établit donc là aussi un cadre favorable à la potentielle reconnaissance du statut juridique des données contenues dans un registre basé sur une chaîne de blocs. Cependant, la situation est plus

¹⁰⁶ De l'anglais hash function : fonction particulière qui, à partir d'une donnée fournie en entrée, calcule une empreinte numérique servant à identifier rapidement la donnée initiale, au même titre qu'une signature pour identifier une personne.

¹⁰⁷ Les Huissiers de Justice de Paris, « *L'authenticité électronique : ne pas confondre la technique et le droit !* » <https://www.huissiersdeparis.com/lauthenticite-electronique-ne-pas-confondre-la-technique-et-le-droit/>

¹⁰⁸ Règlement n° 910/2014/UE du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

complexe lorsqu'il s'agit de signatures. L'eIDAS reconnaît trois niveaux différents de signatures électroniques : simple, avancée et *qualifiée*.

La Blockchain semblerait répondre aux critères techniques pour les deux premiers niveaux. Mais pour être juridiquement contraignant ils doivent répondre à la norme la plus élevée : la signature électronique qualifiée. Ceci requiert le recours aux services d'un organisme tiers de confiance reconnu (Trust Service Provider ; TSP), ou se soumettant à la procédure pour en devenir un. C'est le cas des établissements bancaires qui ont besoin de faire signer les transactions électroniques de manière qualifiée afin de se mettre en conformité avec la seconde directive sur les services de paiement ([DSP2](#))¹⁰⁹.

Ainsi, pour une parfaite reconnaissance juridique du caractère probant des informations contenues dans la blockchain, il semble selon les textes qu'il faille là encore faire appel à un tiers de confiance. Ce choix du législateur ne semble pas opportun puisque l'on peut considérer qu'il s'éloigne des réalités techniques. Cependant, en attendant des précisions explicites concernant la blockchain, le caractère probant de cette technologie est soumis à la libre appréciation du juge lorsque la preuve est libre. Les opérations bancaires de montants élevés opérées sur une blockchain ne sauraient donc revêtir d'autre force juridique que celle que les participants acceptent de leur donner¹¹⁰ – en la précisant au sein d'un contrat cadre par exemple.

Paragraphe 3 : Une conciliation possible entre l'authentification forte et les systèmes de paiement blockchain

La DSP2 rend obligatoire la mise en place d'une authentification forte¹¹¹ pour les services de paiement en ligne de plus de 30 euros. La directive oblige les prestataires de services de paiement à activer l'authentification forte lorsque de leurs clients, lorsque le payeur « *accède à son compte de paiement en ligne, initie une opération de paiement électronique ou exécute une action, grâce à un moyen de communication à distance, susceptible de comporter un risque de*

¹⁰⁹ Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur

¹¹⁰ Boris Barraud. Les blockchains et le droit. Revue Lamy Droit de l'immatériel, Lamy (imprimé) / Wolters Kluwer édition électronique 2018, pp.48-62. fihal-01729646

¹¹¹ L'authentification forte impose deux facteurs différents pour l'authentification parmi les suivants : un code secret, un appareil que l'on possède, une donnée biométrique (empreinte digitale, iris, reconnaissance faciale, etc.).

fraude en matière de paiement ou de toute autre utilisation frauduleuse »¹¹². Une question se pose alors : comment rendre les systèmes de paiement via blockchain conformes à cette exigence ?

Pour s'authentifier, la blockchain impose nativement l'utilisation d'une clé privée. Mais cette nouvelle obligation légale pourrait être une occasion pour les établissements bancaires de créer un service renforçant la sécurité du portefeuille de leurs clients. Dans le cadre d'une nouvelle activité de garde des clés privées des clients (telle que présentée précédemment dans la présente) ; les prestataires de service de paiement pourraient proposer une nouvelle couche de sécurité. L'utilisateur pourrait être amené à s'identifier auprès de l'établissement bancaire par l'intermédiaire de deux facteurs, ce qui lui donnerait accès à l'authentification sur la blockchain via sa clé privée ; ceci afin d'effectuer un paiement en jetons sur une blockchain. Ainsi, l'intervention de l'établissement bancaire aura pour effet d'ajouter une couche supplémentaire de sécurité à la blockchain, sans que la clé privée ne sorte de son contrôle et ne soit directement entre les mains de l'utilisateur qui pourrait se la faire voler.

Paragraphe 3 : Un important vide juridique concernant la gouvernance et la sécurité de la blockchain

Il existe deux grands types de modes de gouvernance d'une blockchain : la *preuve de travail* (Proof of Work, PoW) et la *preuve d'enjeu* (Proof of Stake, PoS). Il s'agit du procédé selon lequel un nœud du réseau ou un ensemble de nœuds du réseau obtient le « droit » de sécuriser les transactions (le fameux « minage ») qui ont lieu sur la blockchain en y ajoutant un nouveau bloc. Ils assurent ainsi son fonctionnement en échange d'une récompense en jetons nouvellement émis ou provenant d'une forme de taxe sur les transactions (aussi appelée *gas*). La preuve de travail met en compétition la puissance de calcul nœuds du réseau, qui doivent résoudre des formes d'énigmes mathématiques ; alors que la preuve d'enjeu met en compétition les nœuds du réseau en fonction du montant de leur investissement en crypto-actifs – ce qui ressemble beaucoup à une gouvernance d'entreprise par actions. Il existe même une version améliorée de ce protocole appelée preuve d'enjeu liquide (Liquid Proof of Stake, LPoS) qui permet de déléguer ses « voix » de gouvernance à un nœud de son choix sans avoir besoin de transférer les précieux jetons, ce qui peut même faire l'objet d'une rémunération.

¹¹² Article 97 de la DSP2

Dans le cas de la preuve de travail, lorsque des nœuds du réseau collaborent et obtiennent le droit de sécuriser les transactions de la blockchain, ils peuvent en prendre le contrôle. Il s'agit d'une cyberattaque qu'il est possible de mener si l'on dispose d'une puissance de calcul importante à un instant précis, dépassant de loin celle des autres membres du réseau. Dans le cadre de la preuve d'enjeu, il s'agit pour les attaquants de contrôler assez de crypto-actifs à un instant précis afin d'obtenir le droit de valider les transactions sur la blockchain. Dans les deux cas, on parle alors d'attaque des 51%¹¹³ – en réalité, 50% plus une unité (de puissance de calcul ou de droits de gouvernance), comme pour une décision d'assemblée sur un vote à la majorité simple. Parfois une partie de la communauté souhaite continuer la chaîne de blocs avec d'autres règles techniques de fonctionnement, provoquant alors une fourche ayant pour conséquence, comme exploré précédemment dans la présente, de dédoubler la chaîne de blocs et ainsi diminuer la valeur des actifs de la chaîne première. Le droit ne règle actuellement pas la question de la responsabilité des membres de la communauté ayant provoqué la fourche, s'ils sont identifiables.

Il n'existe cependant aucun droit régissant la prise de contrôle « sauvage » de la blockchain par la concurrence de puissance de calcul (preuve de travail), qui là encore est un fonctionnement autorégulé – qui a démontré jusqu'ici une forte résilience – qui ne repose que sur la réalité technique. Il n'existe pas plus de droit régissant l'acquisition de crypto-actifs afin de prendre le contrôle d'une blockchain par preuve d'enjeu, comme ce qui existe avec les franchissements de seuils – notamment de droits de vote – lors de l'achat d'actions sur les marchés financiers dans le cadre de la réglementation sur les offres publiques d'achat et d'échange (OPA et OPE)¹¹⁴. Seuls les jetons de titres (dont l'actif sous-jacent est déjà régulé de cette manière) pourraient entrer dans le champ de la réglementation, ce qui laisse un vide béant pour les autres types de crypto-actifs.

Il est possible que le contrôle de la blockchain, dont l'aspect décentralisé présente un intérêt maintes fois démontré, devienne un enjeu majeur du système financier de demain. Les établissements bancaires, s'ils établissent des services autour de la blockchain, auront tout intérêt à ce que leurs structures soient protégées juridiquement. En effet, la prise de contrôle de

¹¹³ Joe Pinasi, The Coin Tribune, « *Qu'est-ce qu'une attaque des 51%, le pire cauchemar de Bitcoin ?* » <https://www.thecointribune.com/actualites/quest-ce-quune-attaque-des-51-le-pire-cauchemar-de-bitcoin/>

¹¹⁴ Au sens des articles L433-1 et suivants du code monétaire et financier

la blockchain par des personnes malveillantes pourrait avoir des conséquences économiques et financières désastreuses¹¹⁵. Cette question du contrôle de la gouvernance de la blockchain nécessitera alors peut-être la création d'une régulation incitante, contraignante, et établissant clairement les responsabilités des différents acteurs sur le réseau ; à défaut pour les forces de l'ordre de pouvoir rétablir matériellement ce type de situation.

¹¹⁵ Malik Bensalem, Véronique Moussu-Baj, AiYO Group, « *La sécurité financière des blockchains* » <https://aiyo.fr/2019/07/08/la-securite-financiere-des-blockchains/>

BIBLIOGRAPHIE

Textes normatifs :

Code civil

Code de commerce

Code monétaire et financier (CMF)

Règlement Général de l'AMF (RGAMF)

Loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises (Loi Pacte)

Ordonnance n° 2017-1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers (Ordonnance « Blockchain »)

Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (5AMLD)

Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers (MiFID II)

Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur (DSP2)

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. (RGPD)

Règlement 910/2014/UE du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur. (eIDAS)

Décisions de Justice :

Conseil d'Etat, 3^e et 8^e chambres réunies, 26 avril 2018 n°417809

Tribunal de commerce de Nanterre, 6^e chambre, 26/02/2020, SDE BITSPREAD LTD contre SAS PAYMIUM

Articles de doctrine et issus de revues :

Adrien Ahmadi Kermanshahani et Henri Nalbandyan, Village Justice, « *Security Token Offerings : Plongée au cœur de la finance régulée* » <https://www.village-justice.com/articles/security-token-offering-plongee-coeur-finance-regulee,30971.html>

Boris Barraud. « *Les blockchains et le droit. Revue Lamy Droit de l'immatériel* », Lamy (imprimé) / Wolters Kluwer édition électronique 2018, pp.48-62. fihal-01729646

Malik Bensalem, Véronique Moussu-Baj, AiYO Group, « *La sécurité financière des blockchains* » <https://aiyo.fr/2019/07/08/la-securite-financiere-des-blockchains/>

Adlen Bouchenafa, Nofel Goulli, « La blockchain pour optimiser le KYC », article initialement publié dans la Revue Banque n°841 (février 2020) <http://www.revue-banque.fr/management-fonctions-supports/article/blockchain-pour-optimiser-kyc>

Dr Pier-Pascale Boulanger, Université de Concordia, « Régulation ou réglementation ? » <http://odft.nt2.ca/blogue/r%C3%A9gulation-ou-r%C3%A9glementation>

Louis Chochoy, Village Justice, « Bitcoin : La justice française reconnaît les propriétés d'une monnaie mais sans en avoir la qualification » <https://www.village-justice.com/articles/bitcoin-justice-francaise-reconnait-les-proprietes-une-monnaie-mais-sans-avoir,34045.html>

Claire Fénéron, Plisson « La blockchain, un bouleversement économique, juridique voire sociétal », *I2D – Information, données & documents*, vol. 54, no. 3, 2017, pp. 20-22.

Friedrich August von Hayek, The denationalization of money <https://nakamotoinstitute.org/static/docs/denationalisation.pdf>

Elise Huber, Village Justice, « Les smart contracts : contrats non identifiés ? » <https://www.village-justice.com/articles/les-smart-contracts-contrats-non-identifies,28893.html>

Yanis-Said Khadiri, Village Justice, « Loi Pacte : Blockchain et crypto-actifs, une histoire de confiance » <https://www.village-justice.com/articles/blockchain-les-crypto-actifs-une-histoire-confiance,30426.html>

Dr Lerong Lu, “Bitcoin: speculative bubble, financial risk and regulatory response”

Gaëlle Marraud Des Grottes, Actualités du droit, « Prestataires de services sur actifs numériques : le décret est paru ! » <https://www.actualitesdudroit.fr/browse/tech-droit/blockchain/24813/prestataires-de-services-sur-actifs-numeriques-le-decret-est-paru>

Mustapha Mekki, Dalloz Etudiant Actu, « Droits(s) et algorithmes : de la blockchain à la justice prédictive » <https://actu.dalloz-etudiant.fr/le-billet/article/droitss-et-algorithmes-de-la-blockchain-a-la-justice-predictive/h/d66e9db5333715c8ff6d88221cf44721.html>

Simon Polrot, ADAN, « Lettre aux députés sur l'extension du régime des PSAN » <https://www.adan.eu/actualites/lettre-deputes-extension-regime-psan>

Clément Tequi, François Hiault et Martin Della Chiesa, « Blockchain : Vers de nouvelles chaînes de valeur » pages 89 et 90

Georges Tchikaidze, Village Justice, « L'encadrement réglementaire des ICOs par la loi Pacte » <https://www.village-justice.com/articles/encadrement-reglementaire-des-icos-par-loi-pacte-contenu-enjeux,31308.html>

Me Thibault Verbiest, Planet-Fintech, « Plateformes d'échange de crypto-actifs : quelle régulation ? » https://www.planet-fintech.com/Plateformes-d-echange-de-crypto-actifs-quelle-regulation_a861.html

Cours universitaire :

Cours de Droit Bancaire de Monsieur le Professeur Laurent RUET (Université Paris Nanterre, M1 Droit des Affaires, année universitaire 2018-2019).

Podcast :

Grégory Raymond, Brice Berdah, Podcast 21 Millions, Capital, « *La finance décentralisée (DeFi), une banque sans banquiers* »

Articles issus de la presse et de divers sites web :

Yorick de Mombynes, Institut Sapiens, “*Bitcoin, totem & tabou, que presage l’essor des cryptomonnaies ?*”
<https://www.institutsapiens.fr/wp-content/uploads/2018/02/Bitcoin-totem-et-tabou-f%C3%A9vrier-2018.pdf>

« White paper » du Bitcoin <https://bitcoin.org/bitcoin.pdf>

Bloomberg, *Jamie Dimon Slams Bitcoin as a ‘Fraud’* <https://www.bloomberg.com/news/articles/2017-09-12/jpmorgan-s-ceo-says-he-d-fire-traders-who-bet-on-fraud-bitcoin>

Forbes, *JPMorgan - Bitcoin’s ‘Biggest Enemy’ - Suddenly Appears To Be Going All In On Crypto*
<https://www.forbes.com/sites/billybambrough/2020/05/30/jp-morgan-bitcoins-biggest-enemy-suddenly-appears-to-be-going-all-in-on-crypto/>

La Tribune avec AFP, « *Monnaie digitale : 80% des banques centrales planchent sur le sujet* »
<https://www.latribune.fr/entreprises-finance/banques-finance/monnaie-digitale-80-des-banques-centrales-planchent-sur-le-sujet-837966.html>

Le Monde Informatique, « *Les pères de l’Internet plaident pour un web plus décentralisé* »
<https://www.lemondeinformatique.fr/actualites/lire-les-peres-de-l-internet-plaident-pour-un-web-plus-decentralise-65119.html>

The Coin Tribune, « *La décentralisation de Bitcoin face à un danger inédit et la solution... c’est vous* »
<https://www.thecointribune.com/actualites/la-decentralisation-de-bitcoin-face-a-un-danger-inedit-et-la-solution-cest-vous/>

Le Monde, « *Bitcoins et autres cryptodevises agitent Wall Street* »
https://www.lemonde.fr/economie/article/2017/10/05/bitcoins-et-autres-cryptodevises-font-vaciller-le-capital-risque-et-wall-street_5196321_3234.html

Charlie Perreau, Journal du Net, « *ICO : définition, liste, situation en France* »
<https://www.journaldunet.com/economie/finance/1195462-ico-definition-liste-la-situation-en-france-decembre-2019/>

AMF, « *Obtenir un visa pour une offre au public de jetons (ICO)* » <https://www.amf-france.org/fr/espace-professionnels/fintech/mes-relations-avec-lamf/obtenir-un-visa-pour-une-ico/preparer-une-ico>

Caroline Lamaud, « *Les ICOs : une menace pour le capital risque ?* » <https://www.anaxago.com/aller-plus-loin/blog/les-icos-une-menace-pour-le-capital-risque>

Jonathan Chester, Forbes, “*Will Security Token Offerings Be The Future Of Raising Money?*”
<https://www.forbes.com/sites/jonathanchester/2019/02/19/will-security-token-offerings-be-the-future-of-raising-money/>

AMF, « *Obtenir un agrément PSAN* » <https://www.amf-france.org/fr/espace-professionnels/fintech/mes-relations-avec-lamf/obtenir-un-enregistrement-un-agrement-psan>

Grégory Raymond, Capital, « *Les banques qui interdisent à leurs clients d’acheter des Bitcoins... et les plus ouvertes* »
<https://www.capital.fr/votre-argent/les-banques-qui-interdisent-a-leurs-clients-dacheter-des-bitcoins-et-les-plus-ouvertes-1358960>

Kraken, Payward Inc, “*Verification levels explained*” <https://support.kraken.com/hc/en-us/articles/360001395743-Verification-levels-explained>

Financial Times, « *Automated company raises equivalent of \$120m in digital currency* »
<https://www.ft.com/content/600e137a-1ba6-11e6-b286-cddde55ca122>

Coinhouse, « *Qu'est-ce que la finance décentralisée ?* » <https://www.coinhouse.com/fr/apprendre/blockchain/la-finance-decentralisee/>

Gregory Barber, Wired, « *A Crypto Exchange CEO Dies—With the Only Key to \$137 Million* » <https://www.wired.com/story/crypto-exchange-ceo-dies-holding-only-key/>

Journal Du Net, « *Wallet : qu'est-ce qu'un wallet et comment le choisir ?* » <https://www.journaldunet.fr/patrimoine/guide-des-finances-personnelles/1208977-wallet/#:~:text=Un%20%22wallet%22%2C%20dont%20la.physique%20ou%20num%C3%A9rique%2C%20de%20cryptomonnaies.>

Legal Tech Blog, « *The Problem of Blockchain Oracles – Interview with Alexander Egberts* » <https://legal-tech-blog.de/the-problem-of-blockchain-oracles-interview-with-alexander-egberts>

European Central Bank, « *Christine Lagarde: Interview with "Challenge" Magazine* » <https://www.ecb.europa.eu/press/inter/date/2020/html/ecb.in200108~f3ba434000.en.html>

Le Monde, « *La fin du paiement cash : Pour David Marcus, « Des services vont se développer autour de l'argent programmable et de Libra »* » https://www.lemonde.fr/economie/article/2020/06/07/la-fin-du-paiement-cash-les-crisis-renforcent-les-tendances-deja-en-cours_6042071_3234.html

Antonio Rodriguez et AFP, La Tribune, « *Cryptomonnaie : la France ne veut pas du Libra de Facebook sur le sol européen* » <https://www.latribune.fr/entreprises-finance/banques-finance/cryptomonnaie-la-france-ne-veut-pas-du-libra-de-facebook-sur-le-sol-europeen-828007.html>

Blockchain Partner, « *Vers une identité numérique « private by design »* » <https://blockchainpartner.fr/vers-une-identite-numerique-private-by-design/>

Zoe De La Roche, The Coin Tribune, « *Jusqu'où le Syndrome Satoshi tirera-t-il le Marché ?* » <https://www.thecointribune.com/actualites/bitcoin-le-21-mai-2020-jusquou-le-syndrome-satoshi-tirera-t-il-le-marche/>

Les Huissiers de Justice de Paris, « *L'authenticité électronique : ne pas confondre la technique et le droit !* » <https://www.huissiersdeparis.com/lauthenticite-electronique-ne-pas-confondre-la-technique-et-le-droit/>

Joe Pinasi, The Coin Tribune, « *Qu'est-ce qu'une attaque des 51%, le pire cauchemar de Bitcoin ?* » <https://www.thecointribune.com/actualites/quest-ce-quune-attaque-des-51-le-pire-cauchemar-de-bitcoin/>

TABLE DES MATIÈRES

REMERCIEMENTS

CONTEXTE

MÉMOIRE : QUELLE RÉGULATION DES CRYPTO-ACTIFS ET DE LA BLOKCHAIN
APPLICABLE À L'ACTIVITÉ BANCAIRE ?

INTRODUCTION

Historique

Définitions

Délimitation

PARTIE I – LES BALBUTIEMENTS DE LA RÉGULATION DES CRYPTO-ACTIFS ET
DE LEURS PLATEFORMES D'ÉCHANGE

Chapitre 1^{er} : La difficile qualification juridique des jetons

Section 1 : Une forte diversité de types de crypto-actifs impliquant une pluralité de régimes
souhaitables

Paragraphe 1 : L'actif sous-jacent, critère logique de classification des crypto-actifs

Paragraphe 2 : Une qualification juridique avancée du Bitcoin et des jetons de
paiement assimilables

Paragraphe 3 : Une précision au demeurant incomplète corrélée par la doctrine
prudente de l'AMF

Section 2 : Les levées de fond en crypto-actifs : vers de nouveaux marchés financiers

Paragraphe 1 : L'innovation bienvenue des Initial Coin Offering en matière de
financement des entreprises

Paragraphe 2 : L'apport « mou » de la Loi Pacte en matière d'ICO : le visa optionnel

Paragraphe 3 : Une transition en cours vers une forme nouvelle d'offre au public de jetons : les Security Coin Offering

Chapitre 2^e : La responsabilité renforcée des plateformes d'échanges de crypto-actifs

Section 1 : L'apport de la Loi Pacte pour les échanges de crypto-actifs

Paragraphe 1 : La possibilité d'obtenir l'agrément PSAN

Paragraphe 2 : Un enregistrement obligatoire auprès de l'AMF pour deux services

Paragraphe 3 : La reconnaissance salvatrice d'une forme de droit au compte bancaire pour les entreprises du monde des crypto-actifs

Section 2 : L'application logique aux échanges des exigences en matière de lutte contre le blanchiment et le terrorisme ainsi que la protection des investisseurs

Paragraphe 1 : La nécessité du KYC pour les services d'achat/vente de crypto-actifs contre de la monnaie ayant cours légal

Paragraphe 2 : Un flou juridique persistant pour les services d'achat/vente « crypto vers crypto »

Paragraphe 3 : Un débat en cours sur la question de l'extension du régime des PSAN aux échanges « crypto vers crypto »

PARTIE II – LA BLOCKCHAIN, NOUVEAU MODE DE GOUVERNANCE DES DONNÉES BANCAIRES

Chapitre 1^{er} : Un défi de gouvernance posé par le caractère décentralisé de la blockchain

Section 1 : La possibilité nouvelle de se passer du tiers de confiance centralisé

Paragraphe 1 : Une opacité partielle des informations sur la Blockchain, conséquence de l'absence d'organe central d'identification

Paragraphe 2 : Les « smart contracts », nouveaux concurrents du droit financier ?

Paragraphe 3 : La finance décentralisée (DeFi), une insaisissable atteinte au monopole bancaire

Section 2 : Le renouvellement du rôle de tiers de confiance avec la blockchain, une opportunité des établissements bancaires

Paragraphe 1 : Les banques, possibles garantes des clés privées (wallet)

Paragraphe 2 : Les banques, possibles « oracles » fournissant l'information extérieure à la blockchain

Paragraphe 3 : Les banques, possibles garantes des actifs sous-jacents des jetons

Chapitre 2^e : Une application complexe de la régulation de la protection et de la sécurité des données à la blockchain

Section 1 : Une apparente difficile conciliation du RGPD et de la blockchain

Paragraphe 1 : Le responsable de traitement, une notion peu pertinente vis-à-vis des DLT

Paragraphe 2 : Une conciliation entre l'immutabilité des données dans la blockchain et le RGPD matériellement impossible

Paragraphe 3 : L'adresse publique sur une blockchain, une donnée personnelle riche éclipant le secret bancaire

Section 2 : Des innovations de la blockchain en matière de sécurité des systèmes d'information inégalement réglementées

Paragraphe 1 : La nécessaire reconnaissance de la force probante des données (bancaires) de la blockchain

Paragraphe 2 : Une conciliation possible entre l'authentification forte et les systèmes de paiement blockchain

Paragraphe 3 : Un important vide juridique concernant la gouvernance et la sécurité de la blockchain

BIBLIOGRAPHIE