RLDA 6531

La souscription de cryptoactifs et de jetons d'ICO : les recours des investisseurs

Jérôme BROSSET
Avocat associé
August Debouzy

Alice BARBET-MASSIN
Doctorante
Univ. Lille, CNRS, UMR 8026-CERAPS
August Debouzy

Non sans risques pour les investisseurs, l'acquisition de cryptoactifs et de jetons émis dans le cadre d'ICO tend à être encadrée par le droit spécial (notamment, le régime dérivé de la future loi Pacte) et le droit commun. Un panorama des recours pouvant être initiés par les investisseurs avec Jérôme Brosset, avocat associé, et Alice Barbet-Massin, doctorante, du Cabinet August Debouzy. .

L'écosystème mondial des cryptoactifs et des ICO(1) ou ITO (pour respectivement « Initial Coin Offerings » et « Initial Token Offerings ») connait depuis quelques années un succès remarquable, même si les montants en jeu restent relatifs. À ce jour, les cryptoactifs et les ICO échappent à une intermédiation et réglementation traditionnelles liées aux infrastructures bancaires et aux marchés financiers(2). Les souscriptions de cryptoactifs et de jetons d'ICO s'accompagnent dès lors d'incertitudes accrues pour les investisseurs(3).

Les cryptoactifs sont définis comme étant des *« actif virtuels stockés sur un support électronique permettant à une communauté d'utilisateurs les acceptant en paiement de réaliser des transactions sans avoir à recourir à une monnaie légale »* (par exemple, le bitcoin, l'ether, le ripple…)(4). Ils fonctionnent grâce à des techniques cryptographiques et un réseau pair-à-pair selon un mode de consensus qui détermine la validation des transactions(5).

(1) Ci-après, le terme ICO sera le seul utilisé.

(2) Le rapport Landau précise dans ses conclusions qu'"*une réglementation directe n'est pas souhaitable [pour les cryptoactifs], car elle obligerait à définir, à classer et donc à rigidifier des objets essentiellement mouvants et encore non identifiés*" (Rapport J.-P. Landau, Les crypto-monnaies, 4 juill. 2018., p. 3).

(3) Colloque du Conseil scientifique de l'AMF, discours de R. Ophèle, ICO, cryptoactifs : quel avenir et quelle régulation ? , le 7 juin 2018.

(4) Banque de France, L'émergence du bitcoin et autres cryptoactifs : enjeux, risques et perspectives, Focus n° 16, le 5 mars 2018 et v. aussi la définition de cybermonnaie issue du Vocabulaire de l'informatique (liste de termes, expressions et définitions adoptés) publié au JORF n° 0121 le 23 mai 2017, texte n°20 : « *Monnaie dont la création et la gestion reposent sur l'utilisation des techniques de l'informatique et des télécommunications* ».

(5) Se référer à la définition de la technologie blockchain sous-jacente : « *Mode d'enregistrement de données produites en continu, sous forme de blocs liés les uns aux autres dans l'ordre chronologique de leur validation, chacun des blocs et leur séquence étant protégés contre toute modification* » (Vocabulaire de l'informatique (liste de termes, expressions et définitions adoptés) publié au JORF n°0121 le 23 mai 2017, texte n°20).

En droit français, les cryptoactifs ne sont pas considérés comme équivalant à une monnaie légale[6]. Ils échappent, tout d'abord, à la qualification de monnaie à cours légal puisque seul l'euro est l'unité de compte officielle et permet le paiement d'une obligation de somme d'argent[7]. De plus, ils n'entrent pas dans le champ de la monnaie électronique en ce qu'ils ne sont pas émis contre la remise de fonds aux fins d'opérations de paiement[8].

La qualification de monnaie conventionnelle est avancée par certains auteurs permettant d'utiliser les cryptoactifs comme un moyen de paiement[9]. En effet, les parties sont libres de payer des obligations issues d'un contrat international dans la devise qu'ils entendent[10]. Cette position est d'ailleurs accréditée par la Cour de justice de l'Union européenne (CJUE) qui a précisé, dans son arrêt dit « *bitcoin* » du 22 octobre 2015, que « *la devise virtuelle "bitcoin" étant un moyen de paiement contractuel elle ne saurait, d'une part, être regardée ni comme un compte courant ni comme un dépôt de fonds, un paiement ou un virement...* »[11]. Il n'existe pas, par conséquent, ni de qualification certaine ni de régime idoine applicable aux cryptoactifs.

Pour ce qui est de l'offre au public de jetons (ou « *ICO* »), elle peut être définie comme une opération de levée de fonds par offre au public, donnant lieu à une émission de jetons numériques (ou « *tokens* »), destinée à financer le développement d'un projet par l'émetteur. Ce projet est accompagné d'un document à visée informative non réglementé appelé livre blanc (ou « *white paper* »).

L'article 26 du projet de loi Pacte prévoit de compléter le titre V du livre V du code monétaire et financier (CMF) d'un nouveau chapitre intitulé « *Émetteurs de jetons* » qui intégrerait sept articles au CMF (L.552-1 à L.552-7 du CMF)[12]. Au sein de ceux-ci, l'ICO serait définie comme l'opération permettant « *de proposer au public, sous quelque forme que ce soit, de souscrire à des jetons* »[13], le jeton étant défini comme « *tout bien incorporel représentant, sous forme numérique, un ou plusieurs droits, pouvant être émis, inscrits, conservés ou transférés au moyen d'un dispositif d'enregistrement électronique partagé permettant d'identifier, directement ou indirectement, le propriétaire dudit bien* »[14]. Ces jetons peuvent, par exemple, représenter un droit à des revenus, des dividendes ou encore une gouvernance... Le droit français en projet s'oriente donc vers une qualification souple des jetons selon leurs caractéristiques : droits d'usage, titres financiers, ou encore biens divers...[15]. Cette qualification du jeton sera déterminante de son régime juridique et ainsi des règles applicables à l'opération d'ICO.

Ces régimes encore incertains des cryptoactifs et des ICO sont un facteur de risque accru pour les investisseurs. À ce titre, le rapport Landau sur les cryptomonnaies remis le 4 juillet 2018 au Ministre de l'économie et des finances recense une perte de 649 millions de dollars de cryptoactifs depuis 2011 (dont 73% sur des plateformes d'échange)[16]. Ce rapport dresse aussi l'ensemble des incidents intervenus sur ces plateformes[17]. Concernant les ICO, les investisseurs potentiels s'exposent à des risques très significatifs et pour partie imprévisibles.

Le présent article a pour objet de dresser un panorama général, sinon exhaustif, des actions et recours qui pourraient être initiés par des investisseurs tant de cryptoactifs que de *tokens* émis dans le cadre d'ICO. Ces actions judiciaires et recours peuvent être initiés sur les plans du droit pénal, civil, et de la consommation. En plus de ces trois grandes familles, d'autres recours peuvent être envisagés et être mis en œuvre à la suite à de souscriptions de jetons d'ICO et de cryptoactifs.

(6) Cette position est partagée unanimement par la doctrine : L. Corbion-Condé, De la défiance à l'égard des monnaies nationales au miroir du bitcoin, RD bancaire et fin. n° 2, dossier 13, mars 2014 ; J. Lasserre-Capdeville, Le Bitcoin : JCP E 2014, act. 25 ; M. Roussille, Le bitcoin : objet juridique non identifié, Rev. Banque et droit n°159, 2015, p. 27 ; Th. Bonneau, Le bitcoin, une monnaie ?, Rev. Banque et droit 2015, p. 8.

(7) C. mon. fin., art. L. 111-1. et C. civ., art. 1343-3, al. 1.

(8) C. mon. fin., art. L315-1.

(9) J. Huet, Le bitcoin, dont la légalité paraît admise, est une sorte de monnaie contractuelle, RDC n°1, le 1er mars 2017, p. 5 ; G. Marain, Le bitcoin à l'épreuve de la monnaie, AJ Contrat, déc. 2017, p. 525.

(10) C. civ., art. 1343-3, al. 2.

(11) CJUE, 22 oct. 2015, aff. C-264/14 Skatteverket c/ David Hedqvist ; RDC 2017, 54, note J. Huet ; RISF 2016 n°1, p. 170, note R. Vabres ; *adde* : Th. Bonneau, Analyse critique de la contribution de la CJUE à l'ascension juridique du bitcoin, *in* Liber amicorum Blanche Sousi, L'Europe bancaire, financière et monétaire, Rev. Banque, 2016.

(12) Le projet de loi relatif à la croissance et la transformation des entreprises (ECOT1810669L).

(13) C. mon. fin., art. L. 552-3 (projet d'article).

(14) C. mon. fin., art. L. 552-2 (projet d'article).

(15) À ce sujet, le Programme d'étude de l'Autorité des Marchés Financiers (AMF) « *Universal Node to ICO's Research & Network* » (UNICORN) a considéré que le token peut être qualifié de token d'usage ou token droit politique ou financier. La doctrine est plus divisée (pour Th. Bonneau : les tokens ne sont jamais des titres financiers et appellent le législateur à adopter une réglementation *sui generis* nouvelle pour ces opérations (Th. Bonneau, Tokens, titres financiers ou biens divers, RD banc. Fin, 2018) ; pour A-S. Grimaldi : « *si le token offre un droit aux dividendes, un droit sur le boni de liquidation et des droits politiques, ou un droit à obtenir remboursement des sommes prêtées, la qualification qui s'impose est celle de titre de capital (action) ou de titre de créance (obligation) et le régime à appliquer est celui des titres financiers* » (A-S. Grimaldi, Les contraintes du droit des obligations sur les opérations d'ICO, D. n°21, le 7 juin 2018, p. 1171). En revanche, aux États-Unis, le jeton est considéré comme un titre financier (SEC, 25 july 2017, release n° 81207).

(16) Rapport J.-P. Landau, *op. cit.*, p. 88-90.

(17) *Ibid.*, p. 96-98.

I. – Les recours en droit pénal

À notre connaissance, aucune décision n'est venue sanctionner à ce jour en France un acte de cyber-délinquance en lien avec la souscription de cryptoactifs ou de jetons d'ICO. Seule la saisie d'actifs virtuels a déjà été ordonnée en cours de procédure pénale. Cependant, d'un point de vue prospectif, il est possible d'envisager la caractérisation d'infractions de droit commun et l'application de textes spéciaux.

A. – Les délits de droit commun : les qualifications vraisemblables d'escroquerie, d'abus de confiance ou de vol

L'escroquerie condamne le fait d'obtenir un bien ou de l'argent à la suite d'une manœuvre frauduleuse[18]. Cette infraction est punie de cinq ans d'emprisonnement et 375 000 euros d'amende[19].

Peut se rattacher à ce délit, l'**hameçonnage (ou « *fishing* »)** qui est une pratique visant les investisseurs de cryptoactifs. Dans sa version la plus classique, elle consiste à envoyer un courriel « *spam* » provenant d'un prétendu prestataire de services liés aux cryptoactifs. Il peut s'agir de fausses alertes de sécurité indiquant qu'un individu essaie de se connecter à son compte personnel. À la suite de ce « *spam* », la victime est incitée à se rediriger vers une fausse version du site du prestataire lui demandant d'entrer ses identifiants de portefeuille virtuel, de façon à permettre au cyber-délinquant le détournement des fonds. Dans une telle hypothèse, l'infraction d'**usurpation d'identité** peut être envisagée au côté de l'escroquerie[20].

L'infraction d'**abus de confiance** condamne, quant à elle, le fait de détourner, au préjudice d'autrui, des fonds, des valeurs, ou des biens quelconques qui lui ont été remis à charge de les rendre, les représenter ou d'en faire un usage déterminé[21]. Cette infraction est punie de trois ans d'emprisonnement et 375 000 euros d'amende.

Les arnaques sont relativement nombreuses dans l'économie des cryptoactifs. Plus de **5 000 arnaques liées à des investissements dans les cryptoactifs ou le minage, aux faux bitcoin, aux systèmes pyramidaux ou encore aux plateformes d'échange de cryptoactifs fantômes ou ne disposant pas des autorisations nécessaires ont déjà été recensées et cette liste évolue constamment** [22]. De même, une fraction significative des **ICO mettent en avant de faux projets** qui sont largement relayés et promus au moyen de **publicités mensongères.**

Le vol constitue un autre fondement envisageable à une action judiciaire. Le vol, soit la soustraction frauduleuse de la chose d'autrui, est puni par trois ans d'emprisonnement et 45 000 euros d'amende, selon l'article 311-1 du code pénal[23]. Au visa de cet article, la jurisprudence a admis l'application du délit de **vol de données informatiques**[24]. Cependant, cette infraction ne permettait qu'imparfaitement de couvrir la soustraction de données virtuelles très répandue en pratique. C'est pourquoi, la nouvelle rédaction de l'article 323-3 du code pénal a intégré à son champ de répression « l'extraction » de données (voir ci-après). Pour éviter tout conflit de qualification, seuls les faits postérieurs à l'entrée en vigueur de cette loi, soit le 15 novembre 2014, sont punissables sur ce fondement. En effet, cette nouvelle infraction étant punie par une peine plus lourde (cinq ans d'emprisonnement contre trois ans pour le vol), la loi dans le temps s'applique conformément au principe d'absence de rétroactivité de la loi pénale plus sévère[25].

Il est courant que des détenteurs de portefeuilles virtuels (ou « *wallet* ») mal protégés se voient subtilisés des cryptoactifs suite à un **vol de clé cryptographique (ou clé privée)**. L'auteur d'un vol de clé cryptographique en vue d'obtenir les fonds contenus dans un portefeuille virtuel pourrait, en principe, être sanctionné sur le fondement du vol. Il existe cependant une difficulté technique à identifier l'auteur de cette infraction (anonymat initial des parties sur le protocole bitcoin). En définitive, compte tenu de l'essor du bitcoin dès 2008, il n'est pas exclu que certaines infractions de soustraction de clés cryptographiques tombent sous le coup de la qualification générale de vol au sens de l'article 311-1 du code pénal.

B. – Les délits spéciaux

Bien que le droit pénal financier ne semble pas s'appliquer aux comportements frauduleux liés aux actifs virtuels et aux ICO, trois délits informatiques spéciaux pourraient s'appliquer.

➜ *L'exclusion des infractions de manipulation de cours et des abus de marché*

En droit français, l'infraction de manipulation de cours est prévue aux articles L. 465-3-1 et L. 465-3-3 du CMF. Est ainsi puni de cinq ans d'emprisonnement et 100 millions d'euros d'amende le fait de « *réaliser une opération, de passer un ordre ou d'adopter un comportement qui donne ou est susceptible de donner des indications trompeuses sur*

(18) C. pen., art. 313-1, al. 1.

(19) Notons que si les infractions étaient commises par une personne morale, les sanctions seraient quintuplées.

(20) C. pen., art. 226-4-1.

(21) C. pen., art. 314-1.

(22) Pour une liste complète mais non exhaustive, v. https://bitcoin.fr/bitcoin-scam-list/ (consulté le 20 août 2018).

(23) C. pen., art. 311-1.

(24) Cass. crim., 20 mai 2015, n° 14-81336 (confirmé par Cass. Crim., 28 juin 2017, n° 16-81113).

(25) C. pen., art. 112-1 et CEDH, art. 7.

l'offre, la demande ou le cours d'un instrument financier ou qui fixe ou est susceptible de fixer à un niveau anormal ou artificiel le cours d'un instrument financier »[26].

Cependant, les cryptoactifs ne peuvent être qualifiés d'instruments financiers[27]. En effet, les instruments financiers sont, soit des titres financiers, soit des contrats financiers. D'une part, les titres financiers peuvent être émis uniquement par l'État, une personne morale, un fonds commun de placement, un fonds de placement immobilier, un fonds professionnel de placement immobilier ou un fonds de titrisation[28]. Avec les cryptoactifs, il n'est donc pas envisageable, en principe, que les mineurs soient des émetteurs[29]. D'autre part, les cryptoactifs ne sont pas des contrats portant sur des actifs, des droits ou des obligations, des indices et des mesures. Ils ne se négocient pas non plus sur un marché réglementé, ne font pas l'objet d'appel de marge, ni de compensation par une chambre de compensation[30]. En ce sens, ils ne pourraient être qualifiés de titres financiers et échappent donc à l'infraction de manipulation de cours.

Si le marché secondaire des cryptoactifs peut se révéler opaque et propice à divers abus, seule la voie de la responsabilité délictuelle pourrait trouver à s'appliquer en France à condition qu'une faute, un préjudice et un lien de causalité soient prouvés[31].

Concernant, les jetons émis dans le cadre d'ICO, ils ne constituent pas, le plus généralement, des titres financiers. Dès lors, bien que la référence au risque de manipulation de cours ou de délits d'initié soit courante, ils échappent, tout comme les cryptoactifs, à ces infractions en droit français[32].

➜ *L'application envisagée des délits informatiques*

L'accès ou le maintien frauduleux dans un système de traitement automatisé de données (STAD) est une infraction qui vise à sanctionner tout individu qui cherche à s'introduire et à prendre connaissance d'informations contenues dans un STAD[33]. Ce délit est puni de deux ans d'emprisonnement et 60 000 euros d'amende. Au soutien de cette sanction - relativement clémente - des circonstances aggravantes peuvent être invoquées dans l'hypothèse de suppression ou modification de données contenues dans ce STAD. Celles-ci font encourir à son auteur une peine aggravée de trois ans d'emprisonnement et 100 000 euros d'amende.

Pourrait ainsi être poursuivi l'individu qui crée un logiciel malveillant (ou « *malware* ») dans le but d'avoir accès au système informatique d'une victime sans son consentement. Il en serait ainsi, par exemple, du logiciel « CryptoSchuffler »[34] permettant au cyber-délinquant de remplacer l'adresse publique utilisée par la partie à une transaction, par sa propre adresse, afin de recevoir les actifs virtuels à transférer. La modification de l'adresse initialement renseignée pourrait ici constituer une circonstance aggravante. Les rançongiciels (ou « *ransomwares* ») qui prennent en otage des données moyennant une rançon pourraient également entrer dans le champ d'application de ce délit. Il est apparu, notamment, que le rançongiciel « WannaCry » collectait sa rançon en bitcoins *via* l'adresse publique du cyber-délinquant[35].

Du reste, dans ces types d'affaires, les enquêteurs auront tout intérêt à utiliser les propriétés de la blockchain - notamment le caractère traçable du livre des comptes - pour remonter l'historique des transactions opérées à partir des adresses publiques des cyber-délinquants.

L'atteinte à l'intégrité des données sanctionne, en vertu de l'article 323-3 du code pénal, le fait « *d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données* » détenues dans un STAD[36]. Ce délit est puni de cinq ans et 150 000 euros d'amende. Depuis la loi n° 2014-1353 du 13 novembre 2014 dite « *Godfrain* », l'ajout du terme « extraire » a étendu cette infraction au vol numérique (voir développements *supra*)[37].

C. – La saisie de cryptoactifs en cours de procédure pénale

En matière pénale, des mesures de saisie peuvent intervenir à tout moment de la procédure, en phase d'enquête

(26) *A contratrio*, une enquête de la justice américaine est ouverte au sujet d'une supposée manipulation de cours du bitcoin. Il est question plus précisément de « *Spoofing* », soit le fait d'offrir des bitcoins à la vente ou à l'achat dans l'intention d'annuler un ordre avant qu'il ne soit exécuté. O. Delaunay, Le bitcoin, objet de manipulation de cours ?, Dr. et patr. n° 281, le 1er juin 2018.

(27) C. mon. fin., art. L. 211-1 et D. 211-1 A, 8°.

(28) C. mon. fin., art. L. 211-2.

(29) Le mineur est l'individu qui met à disposition sa puissance de calcul pour valider les transactions sur le protocole Bitcoin notamment. V. à ce sujet : N. Mathey, La nature juridique des monnaies alternatives à l'épreuve du paiement, RD banc. fin. n°6 dossier 41, Nov. 2016.

(30) C. mon. fin., art. L211-36 et s.

(31) C. civ., art. 1240.

(32) Sur le plan des sanctions administratives pouvant être prononcées par l'Autorité des marchés financiers (AMF), on notera également que la réglementation réprimant les abus de marché issue du règlement européen 576/2014 du 16 avril 2014 ne vise que les instruments financiers.

(33) C. pen., art. 323-1.

(34) B. Eschapasse, Attention aux voleurs de cryptomonnaies, Le Point, 16 déc. 2017, http://www.lepoint.fr/economie/attention-aux-voleurs-de-cryptomonnaies-16-12-2017-2180508_28.php# (consulté le 1er août 2018).

(35) Cyberattaque, ransomware et Bitcoin, bitcoin.fr, https://bitcoin.fr/cyberattaque-ransomware-et-bitcoin/ (consulté le 1er août 2018).

(36) C. pen., art. 323-3.

(37) L. n° 2014-1353, 13 nov. 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

préliminaire, de flagrance ou lors de l'instruction. Elles permettent soit de placer sous-main de justice tout objet utile à la manifestation de la vérité, soit de faciliter l'usage ultérieur de la peine complémentaire de confiscation, soit enfin à titre conservatoire, de garantir l'exécution d'une éventuelle condamnation pécuniaire.

En France, une mesure de perquisition a permis la saisie, dans le cadre d'une instruction judiciaire, de près de 388 bitcoins sur une plateforme d'échange par la section de recherche de la gendarmerie de Toulouse, le 7 juillet 2014. Cette plateforme fonctionnait, par ailleurs, sans autorisation de l'Autorité de contrôle prudentiel (ACPR)[38]. Des mesures similaires ont également été menées aux États-Unis[39].

II. – Les recours en droit civil

Les recours en droit civil se concentrent essentiellement contre les plateformes d'échange puisque très empruntées par les investisseurs. Ils peuvent également être dirigés à l'encontre des émetteurs d'ICO.

A. – Les recours à l'encontre des plateformes d'échange de cryptoactifs

Le code civil permet d'utiliser la voie électronique pour conclure un contrat[40]. Les conditions générales d'utilisation (CGU) des plateformes d'échange sont donc des engagements contractuels qui tiennent lieu de loi entre les parties dès lors qu'elles ont été portées à la connaissance de celles-ci et qu'elles ont été acceptées[41].

Les CGU sont le plus souvent des contrats d'adhésion, à savoir des contrats standards dont les conditions générales ne permettent pas à l'utilisateur, en pratique, d'en négocier les termes. En effet, seule une partie en détermine les termes à l'avance[42]. Ainsi, il serait possible de demander qu'une clause au contrat d'adhésion d'une plateforme d'échange soit réputée non écrite si un déséquilibre significatif, entre les droits et obligations des parties, est constaté[43]. Par exemple, pourrait créer un déséquilibre significatif la clause qui mentionne que le risque technique de tous types de dysfonctionnements doit être assumé par l'usager de la plateforme. Si cette clause est ambiguë, le doute profitera au débiteur de l'obligation. En effet, dans le doute sur le sens du contrat, ce dernier devra être interprété en défaveur de celui qui l'a proposé[44].

Lorsque la condition fera dépendre sa réalisation à la seule volonté de son débiteur, il sera aussi possible d'invoquer la nullité des conditions potestatives[45]. En effet, les CGU d'une plateforme ne pourraient pas créer une obligation qui, dans les faits, serait uniquement subordonnée à la discrétion des dirigeants de la plateforme.

Enfin, la responsabilité contractuelle de la plateforme pourrait être soulevée en cas de manquement contractuel aux CGU après avoir mis en demeure la plateforme de s'exécuter dans un délai raisonnable[46]. À cet égard, celle-ci pourrait justifier que l'exécution a été empêchée par la force majeure[47].

B. – Les recours à l'encontre des émetteurs d'ICO

Les recours à l'encontre des émetteurs d'ICO pourraient être initiés, tant au cours de la période de formation du contrat, qu'au cours de son exécution.

➜ *Concernant la période de formation du contrat*

L'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats a étendu la bonne foi à la période précontractuelle[48]. Résultant de ce principe, l'obligation précontractuelle d'information contraint les parties à fournir toutes les informations susceptibles d'être déterminantes pour le consentement[49].

Lors d'une opération d'ICO, ce devoir est matérialisé par la pratique consistant à ce que l'émetteur mette à disposition des investisseurs un livre blanc. Cette documentation d'information, déterminante du consentement, est supposée renseigner les investisseurs sur le contenu et les parties au projet. En pratique, dans une très grande part, les livres blancs ne constituent que des supports marketing sans réelle consistance et ne permettent pas d'avoir une information complète sur l'investissement et ses modalités.

C'est pourquoi, il est possible d'envisager qu'un investisseur puisse intenter une action à l'encontre de l'émetteur de l'ICO sur le fondement du manquement à son de-

(38) https://www.latribune.fr/technos-medias/internet/20140707trib000838782/bitcoin-le-premier-trafic-demante-le-en-europe-est-francais.html (consulté le 1er août 2018).

(39) Aux États-Unis, l'affaire « *Silk Road* » du 2 octobre 2013 illustre le recours à la saisie et confiscation. Le site de e-commerce Silk Road offrait des services illégaux sur une plateforme du web cachée ou « *deep web* » pour lesquels des paiements étaient systématiquement effectués en bitcoins. Ce site a donc été fermé par le « *Federal Bureau of Investigation* » (FBI) et une saisie et confiscation de bitcoins a eu lieu avec une vente aux enchères par les autorités judiciaires américaines de 27 millions de dollars.

(40) C. civ., art. 1125.

(41) C. civ., art. 1103 et art. 1119, al. 1er.

(42) C. civ., art. 1110, al. 2.

(43) C. civ., art. 1171.

(44) C. civ., art. 1190.

(45) C. civ., art. 1304-2.

(46) C. civ., art. 1231 et s.

(47) C. civ., art. 1231-1.

(48) Ord. n° 2016-131, 10 févr. 2016, portant réforme du droit des contrats, du régime général et de la preuve des obligations.

(49) C. civ., art. 1112-1.

voir d'information. Cependant, ce manquement, s'il est constaté, ne pourrait donner lieu qu'à des dommages et intérêts. Il apparaît donc plus opportun pour l'investisseur de se fonder sur le vice de consentement et dans l'hypothèse d'une dissimulation intentionnelle d'information, sur le dol ou la réticence dolosive[50]. En effet, un tel recours permettrait d'atteindre la nullité du contrat et excuserait, de surcroît, l'erreur du contractant puisqu'une erreur sur la valeur pourrait être caractérisée[51]. Néanmoins, avec le dol, il incomberait à l'investisseur de fournir également la preuve de l'intention délibérée de l'émetteur de tromper l'investisseur. Cette charge de la preuve apparait particulièrement lourde pour l'investisseur et pourrait être de nature à compromettre le succès de son action[52].

Sur ce point, le projet de loi Pacte vise à permettre la mise en place d'un cadre plus sécurisant pour les investisseurs. Il est en effet prévu, si ce projet est adopté, que le livre blanc et les communications à caractère promotionnel devront avoir un contenu exact, clair et non trompeur. D'autre part, ce livre pourra être soumis au visa de l'AMF sur demande optionnelle de l'émetteur[53]. Les précisions apportées par le règlement général de l'Autorité des marchés financiers (RGAMF) sur le contenu des livres blancs visés par l'AMF seront assurément utiles quant à la preuve à apporter du contenu déterminant du consentement des investisseurs lors des actions susmentionnées.

Plusieurs autres fondements pourraient être utilisés dans la perspective d'un recours civil sur la base de faits survenus pendant la période précontractuelle. C'est le cas, notamment, d'une demande en nullité pour contrepartie illusoire ou dérisoire du « contrat de vente » de jetons[54]. Il pourrait ainsi être argué que serait dénué de contrepartie le jeton qui, dès la formation de ce contrat, n'aurait jamais aucune valeur[55]. À ce titre, dans le cadre des arnaques ou « *scams* » telles que Pincoin, Centratech, HoweyCoins, ou OneCoin, les tokens étaient dès l'origine sans valeur[56].

L'investisseur pourrait aussi prétendre à la nullité du contrat sur la base de la prestation non-déterminable qui porte sur une prestation future[57]. C'est par exemple le cas, lorsque des jetons donnent un droit d'usage sans qu'il ne soit finement délimité[58].

➜ *Concernant la période d'exécution du contrat*

La bonne foi - et les obligations qui en découlent - se trouve être un fondement central pour invoquer des recours relatifs à la formation du contrat, mais il peut aussi s'avérer utile au moment de l'exécution du contrat.

En effet, l'émetteur doit en principe tout mettre en œuvre pour mener à bien le développement du projet[59]. Il lui incombe donc une obligation de moyens qui doit être exécutée de bonne foi[60]. Cette obligation induit qu'un recours sur le fondement de la responsabilité contractuelle est envisageable en cas de mauvaise foi de l'émetteur pendant cette période d'exécution de l'opération d'ICO[61].

III. – Les recours en droit de la consommation

En France, l'action de groupe - en vigueur depuis le 1er octobre 2014 - a pour but d'instaurer une procédure de poursuite collective des consommateurs, victimes d'un même préjudice, de la part d'un professionnel[62]. Ces consommateurs se regroupent et agissent par l'intermédiaire de l'une des quinze associations agréées qui peuvent porter l'affaire. En pratique, la première action de groupe en France contre Foncia a été jugée irrecevable par le Tribunal de grande instance de Nanterre le 14 mai 2018[63].

Pour le moment, aucune action de groupe n'a, à notre connaissance, été formée à l'initiative d'investisseurs en cryptoactifs et jetons d'ICO. Cela étant, aux États-Unis, cette voie a déjà été empruntée. Pour financer une nouvelle monnaie virtuelle, le projet Tezos a lancé en 2017 une importante ICO qui leva 232 millions de dollars. À l'issue d'une division entre les dirigeants concernant la gestion des fonds levés, une action de groupe a été lancée par les investisseurs devant la Cour supérieure de Californie du comté de San Francisco sur la base du « *Securities Act* » de 1933[64]. Aux États-Unis encore, à la suite de la découverte de la pyramide de Ponzi liée à la plateforme

(50) C. civ., art. 1137.

(51) C. civ., art. 1139.

(52) De plus, depuis l'ordonnance n° 2016-131 du 10 févr. 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, il n'est pas fait de mention sur la preuve à apporter en cas de dol. Pour l'instant, nul ne sait quelle sera l'interprétation des tribunaux à ce sujet (N. Dissaux, C. Jamin, Réforme des contrats, du régime général de la preuve des obligations, Dalloz, 2017, p. 44).

(53) C. mon. fin., art. L.552-4 (projet d'article).

(54) C. civ., art. 1169.

(55) A-S. Grimaldi, *op. cit.*, p.1173.

(56) https://bitcoinexchangeguide.com/top-5-biggest-2018-ico-scams-ponzi-schemes-crypto-thefts-hacks-so-far/ (consulté le 22 août 2018).

(57) C. civ., art. 1163.

(58) V. une illustration avec l'ICO réalisée par TomRaider en France.

(59) A-S. Grimaldi, *op. cit.*, p. 1174.

(60) C. civ., art. 1104.

(61) C. civ., art. 1231-1.

(62) L'action de groupe est introduite par l'article 1er de la loi n° 2014-344 du 17 mars 2014.

(63) TGI Nanterre, 14 mai 2018, n° 14/11846.

(64) United States District Court, Norhern District of California, Case No.: 3:17-cv-06779-RS.

« BitConnect », une action de groupe a été déposée en janvier 2018[65].

Au titre de l'obligation précontractuelle d'information pour les contrats conclus par un professionnel avec un consommateur, ce dernier doit se voir communiquer par le professionnel, de manière lisible et compréhensible, les caractéristiques essentielles du service, son prix, la date ou le délai auquel le professionnel s'engage à exécuter ce service, les informations relatives à son identité, ses coordonnées, les garanties légales, et les fonctionnalités du contenu numérique[66]. À défaut, le professionnel pourra être sanctionné d'une amende administrative - cumulable avec les règles de responsabilité civile - dont le montant ne pourra pas excéder 3 000 euros pour une personne physique et 15 000 euros pour une personne morale[67]. La difficulté d'utiliser ce fondement pour des investisseurs sur de telles opérations, sera de prouver que ces derniers avaient bien la qualité de consommateur. Si l'investisseur est une personne physique, il pourra être considéré comme consommateur dès lors qu'il agit à des fins qui n'entrent pas dans le cadre de son activité[68].

Les clauses abusives contenues dans les CGU pourraient être réputées non-écrites dans un rapport consommateur-professionnel (voir les développements *supra*). Par exemple, une clause qui exonère la responsabilité de la plateforme d'échange pourrait être réputée non-écrite en ce qu'elle est abusive[69]. En définitive, le consommateur qui utilise une plateforme d'échange a tout intérêt à se fonder sur le droit de la consommation à l'appui de son recours lequel est plus protecteur pour l'usager que ceux du droit commun.

IV. – Les autres recours

A. – Les recours relatifs à l'agrément des plateformes d'échange

Selon un arrêt de la cour d'appel de Paris du 26 septembre 2013[70] et une décision de l'ACPR du 29 janvier 2014, les plateformes d'échange de cryptoactifs doivent être agréées par l'ACPR afin d'exercer l'activité de prestataire de services de paiement[71]. Sans cet agrément, l'exercice de ces prestataires est illégal et pourrait être réprimé à hauteur de trois ans d'emprisonnement et de 375 000 euros d'amende[72].

Le rapport Landau suggère à ce sujet la mise en place d'une licence nationale pendant deux à trois ans pour ensuite la convertir en une « *Euro Bitlicense* ». Ce régime de licence viserait à instaurer un agrément unique des plateformes d'échange en Europe sur le modèle de la Bitlicense New-Yorkaise[73]. Il reste à savoir quelles conditions seront établies pour, non seulement rassurer les investisseurs, mais surtout faire preuve de flexibilité pour les entrepreneurs (condition minimale de capital social, inscription au Registre du commerce et des sociétés, garanties en matière de lutte contre le blanchiment et le financement du terrorisme …).

B. – Les recours relatifs au futur visa des ICO

Afin d'assurer la fiabilité des projets d'ICO, tout en conservant la souplesse propre à ces opérations, le projet de loi Pacteprévoit la possibilité pour l'émetteur de passer par l'obtention d'un visa optionnel de l'AMF[74].

Cette disposition présente un intérêt double. D'une part, l'obligation de l'émetteur de fournir des informations exactes, claires et non trompeuses constituera une meilleure base probatoire pour invoquer des recours en vice de consentement et manquement au devoir d'information (voir développements *supra*). D'autre part, un tel mécanisme rendrait possible les recours à l'encontre des visas de l'AMF afin d'annuler son autorisation, même s'il s'avère rare que de telles demandes aboutissent en pratique avec les IPO[75].

De surcroît, le projet de loi Pacte envisage aussi de conférer des pouvoirs de sanction administrative à l'AMF. Notamment, elle pourrait retirer son visa dans la situation où l'ICO validée ne serait plus en conformité avec le document d'information ou ne présenterait plus ses garanties initiales[76]. Sur ce point, l'AMF se devra de préciser quelles seront les conditions et modalités exactes de mise en œuvre de ce droit de retrait dans le RGAMF.

Enfin, à l'aune de ce même projet de loi, l'AMF pourrait se voir octroyer un pouvoir réglementaire quant aux pratiques professionnelles[77], un pouvoir de contrôle et

(65) United States District Court, Southern District of Florida, Lead Case No.: 9:18-cv-80086-DMM.

(66) C. conso., art. L.111-1.

(67) C. conso., art. L.111-6.

(68) C. conso., art. liminaire.

(69) C. conso., art. R212-1-6°.

(70) CA Paris, 26 sept. 2013, n° 12/00161 : JurisData n° 2013-024887 ; RD bancaire et fin. 2014, comm. 3, obs. F.-J. Crédot et T. Samin ; JCP E 2014, 1091, note Th. Bonneau.

(71) ACPR, 29 janv. 2014-P-01.

(72) C. mon. fin., art. L. 521-2 et L. 572-5. Cette position est soutenue par S. Almaseanu, magistrat en chef du pôle juridique de l'Agence de gestion et de recouvrement des avoirs saisis et confisqués (AGRASC) (S. Almaseanu, Le traitement pénal du Bitcoin et des autres monnaies virtuelles, Gaz. Pal. n° 242, 30 août /2014, p. 11).

(73) Rapport J.-P. Landau, *op. cit.*, p. 60.

(74) C. mon. fin., art. L.552-4 (projet d'article).

(75) CA Paris, 29 avr. 2014, n° 2013/15177 ; CA Paris, 27 sept. 2017 n° 2017/17361 ; CA Paris, 18 mai 2017, n° 2016/26029.

(76) C. mon. fin., art. L.552-6 (projet d'article).

(77) C. mon fin., art. L.621-7 (projet d'article).

d'enquête afin de veiller à la régularité des ICO[78], et un pouvoir de sanction en cas de diffusion de fausses informations ou de manquements à différentes obligations[79].

En définitive, même si certains recours de droit commun ou spécial se révèlent adaptés aux cryptoactifs et ICO, il n'est pas recensé de jurisprudence permettant à l'investisseur d'anticiper l'analyse des juges dans ce type de litiges. Au regard de la rapide évolution technique des cryptoactifs et des ICO, le législateur aura la tâche, à terme, d'initier des réflexions de grande ampleur pour couvrir les zones dénuées d'un droit spécial, tout en s'attachant à assurer une certaine attractivité aux acteurs économiques. Le projet de loi Pacte et les différentes missions d'information au sein de l'Assemblée nationale constituent une première pierre à cet édifice en vue de protéger les investisseurs d'arnaques de plus en plus sophistiquées et internationales. ■

(78) C. mon. fin., art. L.621-9 (projet d'article)

(79) C. mon. fin., art. L.621-15 (projet d'article).