Revue Lamy droit des affaires, Nº 199, 1er janvier 2024

Les prémices et perspectives du contentieux des cryptoactifs

Les contentieux relatifs aux cryptoactifs connaissent un essor considérable devant les juridictions françaises, soulignant la nécessité de préciser le cadre juridique qui leur est applicable. Tour d'horizon de ces contentieux, auxquels les différents acteurs du secteur doivent se préparer pour assurer la défense de leurs intérêts.

Clarisse LE CORRE

Avocat

Associée AdWise

Arthur TEBOUL

Juriste

La France a été pionnière dans l'implémentation de la blockchain et de ses corollaires (cryptoactifs, Web 3.0, métavers, etc.) au sein des entreprises traditionnelles ou « pure players ». En 2022, 89 % des entreprises françaises souhaitaient maintenir (33 %) ou augmenter (56 %) leur budget consacré à la blockchain pour l'année 2023, que ce soit pour diversifier leur trésorerie, optimiser leur croissance ou gagner en visibilité dans le métavers (1) . L'on observe ainsi une multiplication des acteurs de l'écosystème « crypto » et le développement d'une mouvance d'investisseurs, particuliers ou institutionnels, pour ce marché comprenant actuellement plus de 6 000 crypto-devises. Consécutivement, les contentieux en lien avec des cryptoactifs s'imposent désormais devant les juridictions françaises, soulignant la nécessité de préciser un cadre juridique, qui bien que pionnier, demeure lacunaire et fragmenté. Le juge français prendra notamment appui sur les fondamentaux du droit civil et du droit pénal pour trancher ces contentieux d'un nouveau genre, auxquels les entreprises doivent se préparer.

Les contentieux civils en matière de cryptoactifs

Les caractéristiques relatives aux parties au litige

Les contentieux civils en matière de cryptoactifs peuvent tout d'abord être catégorisés en fonction de la qualité des parties au litige. En effet, selon les parties en présence, des obligations spécifiques sont susceptibles de leur être imposées, de nature à orienter le contentieux subséquent.

C'est le cas des prestataires sur actifs numériques (ci-après « PSAN ») agréés auprès de l'AMF, lesquels sont soumis à des obligations spécifiques notamment en matière d'information claire et non trompeuse des clients et d'avertissement sur les risques associés aux actifs numériques (2) . La loi DDADUE (3) du 9 mars 2023 a étendu ces obligations d'information aux PSAN souhaitant fournir les quatre services sur actifs numériques soumis à enregistrement préalable obligatoire (conservation, achat-vente contre monnaie ayant cours légal, échange d'actifs numériques contre d'autres actifs numériques, exploitation d'une plateforme de négociation) (4) .

Une protection des investisseurs peut également être due au titre du droit de la consommation, à toute personne physique agissant à des fins étrangères à son activité professionnelle. Il appartient en effet au professionnel de communiquer au consommateur une information précontractuelle lisible et compréhensible, s'agissant notamment des caractéristiques essentielles du service, en ce compris ses risques (5) . Notons que par un arrêt du 21 octobre 2021, la cour d'appel de Montpellier a considéré qu'un utilisateur d'une plateforme de crypto-monnaies ayant subi une perte de 300 000 euros à la suite d'un piratage disposait de la qualité de consommateur et non de professionnel, bien que ce dernier ait lui-même participé au lancement du projet et réalisait des opérations de conversion de cryptoactifs à titre régulier (6) . Il revient ainsi aux entreprises présentes sur le marché des cryptoactifs de redoubler de vigilance lors de la rédaction de leurs conditions générales et autres documentations contractuelles.

Les caractéristiques relatives aux droits invoqués

Les contentieux afférents aux cryptoactifs mettent à l'épreuve les concepts classiques du droit civil que sont le droit de propriété et la responsabilité (7) .

→ **Droit de propriété**

La cession ou la conservation de cryptoactifs impliquent nécessairement des conséquences juridiques relatives au droit de propriété permettant à son titulaire d'user, d'exploiter et de disposer de son bien discrétionnairement.

Action en revendication de cryptoactifs - L'action en revendication de propriété est l'action qu'exerce le propriétaire d'un bien contre le tiers qui le détient et refuse de le restituer. Cette action a pour but la restitution du bien et tend à la reconnaissance d'un droit de propriété. À la suite des récents dépôts de bilan des plateformes d'échange FTX ou Celsius, s'est posée la question de savoir s'il était possible de revendiquer des cryptoactifs notamment lorsqu'ils sont entre les mains d'un PSAN sous le joug d'une procédure collective. Puisque les cryptoactifs ne peuvent aucunement être appréhendés comme des biens immeubles par nature ou par destination, ils recevront la qualification de biens meubles incorporels de nature en principe fongible, à l'exception des *non-fungible tokens* (ou jetons non-fongible, ci-après « NFTS ») qui feront l'objet d'un traitement particulier. Le Conseil d'État, saisi de la question de la nature du « Bitcoin » afin de lui appliquer le traitement fiscal correspondant, a confirmé cette analyse (8) . Cette qualification a également été retenue par la juridiction consulaire de Nanterre (9) . Or, en droit français et en application de l'article 2369 du Code civil, il est possible d'obtenir restitution d'un bien meuble fongible dans les mains d'un tiers, par équivalence en termes de quantité et de valeur (10) . Il est, dès lors, envisageable que le propriétaire de cryptoactifs, qui apporterait la preuve de son droit de propriété, parvienne à obtenir leur restitution forcée entre les mains d'une plateforme tierce qui en a la possession.

NFTs et propriété intellectuelle - Du fait du flou juridique qui les entoure, les NFTS représentent de nouveaux enjeux en termes de titularité et d'exploitation des droits de propriété intellectuelle (droits d'auteur ou droits de marque) et soulèvent ainsi des questions de droit particulièrement épineuses. Cet objet juridique non identifié a déjà donné lieu à plusieurs contentieux outre-atlantique, dont l'affaire « Metabirkin » : se prononçant de manière inédite sur la contrefaçon d'une marque sous forme de NFT, une juridiction newyorkaise a condamné le 8 février 2023 l'artiste Mason rothschild à verser la somme de 133 000 dollars de dommages et intérêts à la maison Hermès. Dans l'attente d'une décision rendue par une juridiction française en la matière, cette affaire nous donne un aperçu de ce qui pourrait être jugé en France. En matière de contrats de cession de droits d'auteurs, les cessionnaires auront tout intérêt à viser expressément cette nouvelle forme d'exploitation. En matière de contrefaçon et selon la plateforme OpenSea, plus de 80 % des œuvres auxquelles se rattachent un NFT seraient susceptibles de faire l'objet d'une action en contrefaçon. Une telle statistique souligne combien il importe, pour les plateformes proposant des NFTS à la vente, de procéder à la vérification de l'existence d'un droit de propriété intellectuelle sur l'œuvre numérique attachée au NFT et la titularité dudit droit, et de s'appuyer sur des conditions générales sécurisant les ventes en raison des responsabilités civiles et pénales susceptibles d'être encourues par le vendeur.

→ **Responsabilité civile**

Plusieurs causes de responsabilité existent en matière de cryptoactifs sans que la liste ne puisse être exhaustive : piratage, mauvaise utilisation des cryptoactifs déposés, défaut d'information, perte de données, etc.

L'utilisateur final qui a subi un dommage du fait d'un dysfonctionnement de la blockchain peut envisager la mise en œuvre de la responsabilité des acteurs intervenant sur cette dernière. Pour cela, plusieurs fondements sont envisageables. Sans être exhaustif, en l'absence de lien contractuel (s'agissant par exemple des « mineurs », développeurs, etc.), le fondement privilégié sera celui de la responsabilité délictuelle. En revanche, lorsqu'un contrat aura été conclu (responsabilité d'une plateforme d'échanges de cryptoactifs par exemple), la responsabilité contractuelle sera recherchée et supposera la démonstration de l'existence d'un manquement contractuel.

En toute hypothèse, l'identification de la personne responsable du fait dommageable invoqué est souvent particulièrement complexe, du fait du caractère décentralisé des blockchains sur lesquelles circulent les cryptoactifs et de l'anonymat des transactions. L'identification du responsable pose néanmoins moins de difficulté lorsque l'action en responsabilité est engagée à l'encontre de l'émetteur d'une ICO ou d'une plateforme d'échanges et de conservation de cryptoactifs.

Les contentieux pénaux afférents aux cryptoactifs

Par définition, la blockchain permet de réaliser des transactions anonymes, instantanées, transfrontalières, s'affranchissant des institutions financières et de la régulation applicable au système bancaire traditionnel. En dépit du caractère transparent de la blockchain, la rapidité et l'extraterritorialité des opérations rendent particulièrement difficile de retracer la chaîne de transactions en cryptomonnaies, d'autant que diverses techniques permettent d'en complexifier le suivi (« blender », « mixer »). À la lumière de telles caractéristiques, les cryptoactifs étaient prédestinés à intéresser le droit répressif et alimenter des contentieux pénaux sur le fondement de diverses infractions.

Les infractions dont la commission est liée, facilitée ou amplifiée par l'utilisation de la technologie de la blockchain

Les cryptoactifs ont rapidement été utilisés à des fins criminelles (trafic de stupéfiants, etc.), de blanchiment ou de financement du terrorisme. Il est ainsi apparu nécessaire de définir un cadre réglementaire et soumettre les professionnels du secteur des cryptoactifs aux obligations de LCB-FT : c'est chose faite avec la loi PACTE n° 2019-486 du 22 mai 2019, complétée par l'ordonnance n° 2020-1544 du 9 décembre 2020. Plus récemment, le règlement MICA, qui instaure un cadre juridique harmonisé au niveau européen en matière de cryptoactifs, prévoit des obligations renforcées en la matière, au titre de la directive 215/849/UE.

Surtout, cette utilisation des cryptoactifs à des fins criminelles a engendré les premières saisies d'actifs numériques dans le cadre de procédures pénales, saisies dont le nombre explose désormais. L'agence de gestion et recouvrement des avoirs saisis et confisqués (ci-après « AGRASC ») a en effet procédé à 39 saisies de cryptoactifs en 2020, 74 en 2021, 310 en 2022, soit une augmentation de 319 % (11) . La chambre criminelle a ainsi approuvé une saisie d'actifs en bitcoins ordonnée par la juridiction d'instruction sur le fondement de la présomption d'origine illicite des biens prévue par l'article 324-1-1 du Code pénal, aux motifs que « *les modalités de fonctionnement inhérentes à ces cryptoactifs (notamment l'anonymat) favorisent la dissimulation des profits générés tant par le trafic de stupéfiants que par les transactions portant sur la revente de téléphones dotés [d'une solution de*

cryptologie] dont il est démontré qu'elle est exclusivement utilisée par des organisations criminelles, et que, dès lors, les transactions de cryptoactifs qui alimentent ces comptes ne sauraient avoir d'autres justifications que de dissimuler l'origine frauduleuse de ces fonds qui constituent le produit direct voire indirect des infractions susvisées » (12) . Par communiqué du 5 septembre 2023, l'AGRASC a en outre annoncé avoir étendu son partenariat avec la BAnque des Territoires (Caisse des dépôts), qui sécurisait déjà depuis 2011 les fonds gérés par l'AGRASC, hors cryptoactifs, et a obtenu en septembre 2021 un enregistrement auprès de l'AMF en qualité de PSAN, pour lui confier la conservation des actifs numériques saisis dans le cadre de procédures pénales.

Les infractions spécifiques aux technologies de l'information et de la communication

Les cryptoactifs ont donné un nouvel essor à la cybercriminalité, entendue au sens des infractions spécifiques aux technologies de l'information et de la communication. L'on notera tout d'abord les attaques de portefeuilles électroniques, par l'obtention frauduleuse de la clé privée du portefeuille puis le transfert des actifs. Ce type de hacking suppose de compromettre le système informatique stockant la clef privée (ordinateur, smartphone), une des techniques les plus populaires étant l'exfiltration des données dites « copiées et collées » (fonctionnalité très souvent utilisée pour retranscrire la clef privée du portefeuille compte tenu des nombreux caractères utilisés) dans les presse-papiers des systèmes d'exploitation généralement insuffisamment sécurisés. Nombreux sont également les cas de *cryptojacking*, à savoir l'utilisation clandestine de la puissance de calcul des ordinateurs de particuliers ou d'entreprises et collectivités afin de miner des actifs numériques au bénéfice du cyberdélinquant, et dont les victimes n'ont pas toujours conscience (la majorité des logiciels de *cryptojacking* étant conçus pour ne pas trop ralentir l'ordinateur infecté, afin de rester furtifs et actifs le plus longtemps possible). Il sera enfin souligné le développement des « rançongiciels » (ou *ransomwares*), logiciels spécifiques prenant en otage des données notamment d'entreprises ou collectivités moyennant le paiement d'une rançon en cryptomonnaie.

Différentes qualifications pénales sont susceptibles de s'appliquer à de tels faits : outre des qualifications de droit commun (vol, extorsion, etc.), des qualifications spécifiques aux technologies de l'information et de la communication (atteintes aux systèmes de traitement automatisé de données, désignées usuellement sous le terme « piratage » (13) et atteintes aux droits de la personne résultant des fichiers ou traitements informatiques (14) .

Du point de vue des entreprises et collectivités susceptibles d'être victimes de tels faits, ce constat impose la mise en place de mesures adéquates de protection et de prévention des cyberattaques. Concrètement, il s'agit de prendre toutes les mesures nécessaires sur le plan technique (cloisonner le système d'information, limiter les droits des utilisateurs et les autorisations des applications, etc.), mais également de diffuser les bonnes pratiques en interne et s'assurer que l'entreprise a souscrit une police d'assurance couvrant le risque cyber. Il s'agit également de faire preuve de réactivité lorsque le risque se matérialise, par la notification de la violation de données personnelles à la CNIL dans un délai de 72 heures et un dépôt de plainte. À ce sujet, l'on soulignera que les entreprises sont trop souvent réticentes à déposer plainte, doutant de son utilité pour identifier les auteurs et craignant d'altérer leur image si elles sont perçues comme incapables de se prémunir contre les cyberattaques. Rappelons pourtant que le nouvel article L. 12-10-1 du Code des assurances, entré en vigueur en avril 2023, impose aux entreprises de déposer plainte dans un délai de 72 heures (à compter de la connaissance d'une atteinte à un STAD dont elles sont victimes) pour être indemnisées par leur assureur.

Les contentieux pénaux relatifs à la protection des investisseurs

Enfin, les cryptoactifs alimentent des contentieux pénaux relatifs à la protection des investisseurs lésés, victimes de fraudes de diverses natures (rendements promis non atteints, défaut de mise en œuvre des projets après l'ICO, disparition des émetteurs ou dirigeants du projet, mauvaise gestion budgétaire du projet, pyramide de Ponzi, etc.), sous des qualifications de droit commun telles que le vol, l'escroquerie ou encore l'abus de confiance. L'essor de ces contentieux est proportionnel à l'augmentation des ICO à l'échelle mondiale - culminant en 2018 avec un montant total collecté de plus de 10 milliards de dollars. Compte tenu du nombre élevé de projets frauduleux d'ICO, l'AMF a d'ailleurs établi une liste noire des plateformes proposant en France des produits dérivés sur cryptoactifs sans y être autorisés. Si ces contentieux empruntent les qualifications pénales de droit commun, ils revêtent une complexité particulière en terme probatoire et de poursuite. Ici encore, la saisie d'actifs numériques à titre conservatoire auprès des plateformes d'échange constitue un enjeu considérable pour la sauvegarde des intérêts des plaignants.

Du point de vue normatif, la loi PACTE susmentionnée est intervenue pour sécuriser les ICO en instaurant un cadre réglementaire et mettant en place un visa optionnel de l'AMF délivré aux porteurs de projets respectant certaines conditions. Le règlement MICA encadre également l'offre au public et met l'accent sur la répression des abus de marché sur cryptoactifs en créant des délits en lien avec les ICO : à compter du 30 décembre 2024, seront interdits les opérations d'initiés (15) , la divulgation illicite d'informations privilégiées (16) et les manipulations de marché (17) impliquant des cryptoactifs.

Ainsi les cryptoactifs alimentent des contentieux variés, auxquels les différents acteurs du secteur doivent nécessairement se préparer pour assurer la défense de leurs intérêts. Et ce d'autant que l'essor de ces contentieux pose un certain nombre de défis : sur le plan probatoire, tout d'abord, dès lors que la multiplicité des transactions sur la blockchain et leur caractère anonyme, instantané et transfrontalier complexifie le traçage et la corrélation des informations. Sur le plan indemnitaire, également, car le caractère volatile des cryptoactifs et les variations de grande ampleur du marché posent des difficultés quant à la valorisation du préjudice, *a fortiori* lorsque les investissements ont été réalisés avec d'autres cryptoactifs, eux-mêmes soumis à des fluctuations.

---

(1) PWC, Étude Blockchain & crypto : comment les entreprises en tirent enfin bénéfice ?, 2022

(2) C. mon. fin., art. L. 54-10-5.

(3) L. n° 2023-171, 9 mars 2023 portant diverses dispositions d'adaptation au droit de l'Union européenne dans les domaines de l'économie, de la santé, du

travail, des transports et de l'agriculture.

(4) C. mon. fin., art. L. 54-10-3.

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

(6) CA Montpellier, 2e ch. civ., 21 oct. 2021, no 21/00224.

(7) H. De Vauplane, Le droit civil à l'épreuve de la blockchain, revue des juristes de Sciences Po, no 16, 2019.

(8) CE, 8eet 3e ch. réunies, 26 avr. 2018, no 417809, publié au recueil Lebon.

(9) T. com. Nanterre, 26 févr. 2020, no 2018F00466.

(10) « *La propriété réservée d'un bien fongible peut s'exercer, à concurrence de la créance restant due, sur des biens de même nature et de même qualité détenus par le débiteur ou pour son compte.* »

(11) Rapport d'activité 2022 de l'AGRASC.

(12) Cass. crim., 15 févr. 2023, no 22-81.326.

(13) C. pén., art. 323-1 à 323-4-1.

(14) C. pén., art. 226-16 à 226-22-1.

(15) Règl. (UE) no 2023/1114, 31 mai, art. 89.

(16) Règl. (UE) no 2023/1114, 31 mai, art. 90.

(17) Règl. (UE) no 2023/1114, 31 mai, art. 91.