MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA SOUVERAINETÉ
INDUSTRIELLE ET NUMÉRIQUE

*Liberté*
*Égalité*
*Fraternité*

# Les jetons à vocation commerciale dans l'économie française : cas d'usage et enjeux juridiques

## RAPPORT ET ANNEXES

MAI 2023

Marc **AUBERGER**
Ivan **SALIN**
Valentin **MELOT**

**Inspection générale des finances**

MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA SOUVERAINETÉ
INDUSTRIELLE ET NUMÉRIQUE
*Liberté*
*Égalité*
*Fraternité*

Inspection générale
des finances

**MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE**
**MINISTÈRE DÉLÉGUÉ CHARGÉ DES COMPTES PUBLICS**
**MINISTÈRE DÉLÉGUÉ CHARGÉ DE LA TRANSITION NUMÉRIQUE ET DES TÉLÉCOMMUNICATIONS**

RAPPORT

N° 2022-M-062-05

# LES JETONS À VOCATION COMMERCIALE DANS L'ÉCONOMIE FRANÇAISE : CAS D'USAGE ET ENJEUX JURIDIQUES

## RAPPORT ET ANNEXES


Établi par

IVAN SALIN
Inspecteur des finances

VALENTIN MELOT
Inspecteur des finances adjoint

Sous la supervision de
MARC AUBERGER
Inspecteur général des finances



- MAI 2023 -

**Rapport**

# SYNTHÈSE

Le développement des technologies *blockchain* a permis l'apparition des jetons et des programmes autonomes, notamment sur la *blockchain Ethereum*, qui ouvre de nouveaux cas d'usage à cet outil. Les jetons peuvent être essentiellement à vocation financière ou à vocation commerciale. Dans ce dernier cas, ils se sont surtout développés dans trois secteurs : les jeux vidéo, le monde de l'art et de la culture et enfin, le secteur de la consommation, notamment de luxe. Quel que soit le secteur, les jetons ont pour propriété principale de dupliquer dans l'univers numérique la notion de rareté et de propriété : en effet, ils sont rivaux et exclusifs et permettent donc d'identifier le « propriétaire » d'un objet numérique (accessoire de jeu vidéo, image artistique ou sac de luxe dans un métavers) qui, lui, est duplicable à l'infini.

Les cas d'usage des jetons à vocation commerciale sont aujourd'hui peu nombreux et leurs effets sur l'économie française, limités. Le caractère très mouvant et innovant du secteur des *blockchains* peut faire émerger de nouvelles utilisations mais le dynamisme de l'écosystème *crypto* français, premier dans l'Union européenne, ne doit pas faire oublier qu'il est encore embryonnaire, loin derrière celui des États-Unis ou du Royaume-Uni. Il bénéficie d'atouts propres à la France (compétences en informatique fondamentale, présence de grandes entreprises utilisatrices de jetons, cadre réglementaire précoce grâce à la loi PACTE) mais pâtit de deux obstacles, qui doivent être surmontés : la difficulté pour les startups du secteur à ouvrir des comptes bancaires (du fait des risques de blanchiment de capitaux) et la difficulté pour les fonds d'investissement à investir en jetons, pour des raisons réglementaires.

Si les pouvoirs publics souhaitent encourager le développement des jetons à vocation commerciale dans l'économie française, plusieurs problématiques doivent être traitées afin d'apporter davantage de sécurité juridique aux acteurs et de maîtriser les risques afférents.

Tout d'abord, la nature des droits associés aux jetons (qui font souvent office de bons donnant droit à un sous-jacent, comme l'accès à un service) doit être clairement établie et rendue publique lors de leur émission, dans un souci de protection des consommateurs. À ce titre, le cas des jetons pointant vers des œuvres d'art doit faire l'objet d'une attention particulière : les jetons ne constituent pas des œuvres d'art ni des titres de propriété. Tout au plus peuvent-ils constituer, s'ils sont accompagnés de contrats de licence, des titres de concession des droits patrimoniaux associés aux œuvres vers lesquelles ils pointent.

Fiscalement, les jetons à vocation commerciale ne sont pas adaptés au régime conçu pour les actifs numériques par la loi PACTE. Dans la mesure où ces jetons ont un sous-jacent et constituent un bien accessoire par rapport à ce dernier, ils devraient être soumis au régime fiscal de leur sous-jacent, c'est-à-dire, la plupart du temps, le régime des biens meubles.

Enfin, des enjeux en matière de régulation se posent. Le règlement européen MiCA devrait entrer en vigueur courant 2023 et en application, fin 2024. Il remplacera alors le cadre réglementaire posé par la loi PACTE. Son périmètre d'application soulève plusieurs questions d'interprétation. Les jetons non fongibles et les plateformes d'échange de pair à pair (comme *OpenSea*) en sont exclus, en dépit de risques en matière d'abus de marché et de lutte anti-blanchiment à leur sujet. La mission recommande donc d'inclure les jetons non fongibles dans le champ du règlement, de prévoir un régime *ad hoc* pour les plateformes pair à pair et d'interdire le rachat des jetons par leurs émetteurs. En matière de lutte anti-blanchiment, l'adoption d'un nouveau « paquet » législatif fait des prestataires de services sur cryptoactifs des entités assujetties. Afin de limiter au maximum le point de fuite que constituent les portefeuilles autohébergés, la mission recommande de rendre obligatoire la vérification de l'identité du détenteur pour tout transfert supérieur à 1 000 € impliquant un prestataire de services sur cryptoactifs ou un professionnel.

# SOMMAIRE

# INTRODUCTION

**Le développement des « chaînes de blocs » (en anglais, « *blockchains* »), ces registres distribués en ligne sur lesquels l'écriture de données obéit à des règles déterminées à l'avance dont le respect est garanti par un protocole cryptographique de confiance, a suscité l'émergence d'une grappe d'innovations aux usages économiques multiples**. L'ensemble des technologies liées à cet écosystème *blockchain*, qui ont pour caractéristique première la décentralisation, est désigné par le terme de Web 3.0, en référence aux « versions » précédentes du Web, le Web 2.0 étant associé à l'interaction entre utilisateurs sur internet (réseaux sociaux, notamment).

La première des *blockchains*, *Bitcoin*, a été développée en 2008 pour permettre de gérer un système de paiements reposant sur une nouvelle unité de compte, le bitcoin, en se passant de tiers de confiance (État, banque centrale, banques).

**La *blockchain Ethereum* innove par rapport à *Bitcoin* par sa capacité à accueillir des inscriptions plus complexes qui constituent des programmes autonomes, appelés « *smart contracts* »**[1]. Ces programmes adoptent un comportement déterministe : leur exécution est programmée à l'avance et obéit à des conditions d'exécution. Ils détiennent une mémoire permanente, qui peut être utilisée pour stocker des jetons. Les jetons sont transférés d'un « portefeuille » (*wallet*) à un autre, chaque portefeuille étant associé à un identifiant sur la *blockchain* et ayant été ouvert par un utilisateur. Un jeton est un objet numérique, sans réalité autre que l'identification informatique d'un titulaire par un programme autonome sur *blockchain,* auquel peuvent éventuellement être associés des possibilités techniques ou des droits juridiques.

**Parmi les jetons, certains sont émis en un unique exemplaire, indivisible, distinct des autres, et pouvant être suivi individuellement. Un tel jeton est dit *non fongible* (en anglais, *non fungible token*, NFT).** Les NFT sont le plus souvent associés à des ressources extérieures à la *blockchain* qui les accueille : ils « pointent » vers cette ressource, généralement une image, *via* un hyperlien. La ressource est, elle, stockée sur des serveurs qui peuvent être centralisés ou, plus fréquemment, décentralisés, comme le « *interplanetary file system* » (IPFS). Pour faciliter l'interopérabilité des jetons, la conception des NFT sur la *blockchain Ethereum* a fait l'objet d'une standardisation (standard ERC 721).

Le transfert de jetons peut être réalisé sans contrepartie (don de jeton sur la blockchain) ou contre des unités de la cryptomonnaie[2] de la blockchain sur laquelle sont inscrits les jetons. Cette cessibilité donne une valeur marchande aux jetons et justifie leur intégration à des cas d'usage commerciaux.

**Les jetons peuvent présenter et combiner différentes finalités. Celles-ci permettent de les classer, en première approche, en plusieurs catégories** :

- l'objet des jetons peut être la perception de flux financiers futurs, ce qui les assimile à des actifs financiers (jetons-valeur, *security tokens*) ;
- ils peuvent permettre la participation à la gouvernance de l'entité ou du protocole ayant émis les jetons (jetons de gouvernance, *governance tokens*) ;

[1] Bien qu'ils ne constituent pas des contrats (*cf.* annexe II).

[2] Les cryptomonnaies de chaînes (bitcoin, éther, *etc.*) ne sont pas, d'un point de vue strictement technique, des jetons au sens de ce qui précède. En effet, leur gestion ne repose pas sur un programme autonome gérant leur stock, mais directement sur les règles de base de fonctionnement de la *blockchain.*

- ils peuvent avoir une contrepartie fixe, par exemple une monnaie officielle comme l'euro, garantie par l'émetteur : ils font office de monnaie stable (*stablecoins*) ;
- ils peuvent donner accès à un bien ou à un service fourni par l'entité émettrice, c'est-à-dire apporter une utilité (jeton utilitaires, *utility tokens*) ;
- enfin, certains jetons peuvent n'ouvrir aucun droit vis-à-vis d'une personne déterminée. Les NFT faisant office d'objets virtuels de collection rentrent dans cette catégorie.

La fongibilité ou la non fongibilité des jetons est une propriété qui est transversale aux différentes finalités (un *security token* peut être fongible ou non fongible).

**Le présent rapport traite des jetons à vocation commerciale (JVC), c'est-à-dire les jetons, fongibles ou non fongibles (NFT) qui sont vendus en tant que produits ou qui sont associés à un acte de vente de produits réels**. Ces jetons ne représentent pas des titres financiers ni des moyens d'échanges et ont une vocation première autre que de servir de support de placement. La catégorie des JVC regroupe des *utility tokens* et des jetons dépourvus de droits (objets d'art et de collection associés à des NFT). Les jetons à vocation financière et les cas d'usage financiers, comme la finance décentralisée (« DeFi ») sont en dehors du champ de la mission.

Conformément à la lettre de mission, le présent rapport vise à « dresser un panorama du développement des actifs numériques à vocation commerciale » et à « formuler des propositions pour soutenir le développement des actifs numériques ».

Pour ce faire, le rapport est construit en trois sections :

- la section 1 expose les cas d'usage actuellement constatés, en France, pour les JVC ;
- la section 2 développe toutes les problématiques juridiques et fiscales qui entourent le développement des JVC et fournit des recommandations d'amélioration ;
- la section 3 présente l'écosystème français du secteur du Web 3.0, son positionnement par rapport aux autres écosystèmes dans le monde et identifie deux leviers de développement.

Le rapport est accompagné de neuf annexes :

- l'annexe I présente les caractéristiques techniques des *blockchains,* les problèmes auxquels répond cette technologie et les limites consubstantielles à celle-ci ;
- l'annexe II prolonge la précédente en se centrant sur les propriétés et le fonctionnement des jetons ;
- l'annexe III développe les cas d'usage des JVC recensés par la mission ;
- l'annexe IV expose les problèmes liés à la qualification juridique des jetons et à l'imprécision des droits qui leur sont associés ;
- l'annexe V présente le cadre juridique, en l'espèce européen, qui vise à traiter les risques posés par les JVC (données personnelles, régulation financière, lutte anti-blanchiment) ;
- l'annexe VI analyse le régime fiscal appliqué aux JVC et les modifications à envisager ;
- l'annexe VII présente plus précisément l'écosystème Web 3.0 français ;
- l'annexe VIII est constituée de la lettre de mission à l'origine de ce rapport ;
- l'annexe IX énumère l'ensemble des personnes rencontrées par la mission.

# 1. Les jetons constituent une innovation des technologies *blockchain*, applicables à différents cas d'usage mais dépourvus de valeur juridique

## 1.1. Les jetons à vocation commerciale sont utilisés, aujourd'hui, dans trois secteurs principaux

Les *blockchains* peuvent être utilisées comme registres de propriété. Un jeton détient en effet un unique propriétaire et est transférable. Il est alors possible d'associer à chaque jeton une ressource numérique. Les jetons non fongibles sont alors particulièrement adaptés pour désigner la propriété de ces ressources numériques. Puisque les règles d'écriture dans la *blockchain* font des jetons des biens exclusifs et rivaux, si l'émetteur du jeton est capable d'assurer que seul son détenteur a accès à la ressource ou au service associé, alors cette dernière devient elle-même exclusive et rivale, et le jeton représente un titre de propriété sur celle-ci. Les jetons permettent donc d'introduire dans le monde numérique les notions de propriété et de rareté qui sinon seraient difficiles à appliquer à cet univers, dans la mesure où les objets virtuels sont duplicables à l'infini. Grâce à ces propriétés, ces jetons peuvent être vendus par leur émetteur puis échangés sur un marché secondaire, d'où leur vocation commerciale dans les jeux vidéo, l'art et le luxe.

### 1.1.1. Les JVC se développent dans le secteur des jeux vidéo en rendant cessibles les objets de jeu

**Les modèles économiques des jeux vidéo ont évolué dans les dernières décennies**, passant d'un modèle dominant où le jeu était acquis en une seule dépense qui couvrait tous les éléments de jeu, via un support physique (une console ou un CD-ROM, généralement), à une diversité de modèles, où changent tant les supports de jeu (jeux en ligne, jeux sur téléphones portables) que les sources de revenus. Les éditeurs de jeux ont ainsi développé des jeux évolutifs, où des accessoires supplémentaires sont ouverts à l'achat, en bonus (achats dits « *in game* »). Ces revenus complémentaires, associés aux éventuelles recettes publicitaires, peuvent permettre aux éditeurs de rendre l'accès au jeu initial gratuit (modèle dit « *freemium* »).

**Les technologies Web 3.0 s'inscrivent dans cette généralisation des achats *in game*.** L'association d'un JVC à un objet de jeu virtuel (épée, tenue vestimentaire, carte représentant un sportif, monnaie de jeu, etc.) permet de rendre ces objets cessibles entre joueurs et, éventuellement, interopérables entre jeux.

**L'intégration des technologies issues des *blockchains* dans le monde des jeux répond ainsi à la demande des joueurs de rentabiliser les montants – et le temps – investis dans le jeu, voire de faire du gain financier un objectif en soi** (modèle du « *play to earn* »), en leur donnant la possibilité de revendre ces objets sur un marché secondaire, de gré à gré ou géré par une plateforme d'échange. Le fonctionnement des jeux antérieurs au Web 3.0 était caractérisé par une « boucle fermée » : les objets échangés ne pouvaient pas être revendus, ils restaient dans le jeu. S'ils étaient vendus en dehors du jeu (par exemple, un compte joueur FIFA), le fraudeur encourait un risque de sanction : dans le cas de FIFA, cette possibilité est explicitement interdite par l'accord de licence du jeu donc les joueurs réalisant de telles ventes encourent la suspension de leur compte et la perte de leurs objets.

**Les jeux sont devenus le principal cas d'usage des technologies Web 3.0.** Selon le site DappRadar[3], les activités de jeu représentant 48,5 % des *wallets* uniques actifs (*« daily unique active wallets », dUAW)* sur la *blockchain* en janvier 2023.

Si le secteur français du jeu Web 3.0 n'est pas au premier rang mondial, puisqu'il ne compte aucun des jeux les plus utilisés (*Alien Worlds, Splinterlands, Farmers World*), il n'en reste pas moins dynamique, porté par des acteurs de niveau international (comme *Sorare*, dans le monde des « *play to earn* » sportifs), et par des projets nombreux (*Oval3* et *Metafight* dans la fantaisie sportive, *Immortal Games* dans les échecs, ou encore *Dogami*, un tamagotchi). Les atouts de la France dans le secteur des jeux vidéo, avec notamment la présence du leader Ubisoft, constituent également un levier de développement potentiel pour les jeux Web 3.0.

Néanmoins, dans la mesure où les jeux Web 3.0 remplissent le plus souvent les quatre critères qui définissent, en droit français, un jeu d'argent et de hasard (offre publique, sacrifice financier, intervention du hasard et espérance de gain), ceux-ci devraient être interdits en vertu du principe de prohibition de ces jeux qui prévaut en France (article L. 320-1 du code de sécurité intérieure). En effet, les jeux Web 3.0 ne rentrent dans aucune des exceptions à cette prohibition prévues à l'article L. 320-6 du CSI.

L'application stricte de cette analyse juridique conduirait donc à empêcher tout développement du jeu dans le secteur du Web 3.0 en France, par assimilation du « *gaming* » au « *gambling* ». **Le développement des jeux Web 3.0 suppose donc une évolution du cadre réglementaire.** Les enjeux d'une telle évolution sont présentés dans le rapport n° 2022-M-062-02 de l'Inspection générale des finances, « Donner un cadre juridique aux jeux à objets numériques échangeables » (janvier 2023).

### 1.1.2. Les NFT sont utilisés dans le domaine de la culture, sous la forme d'objets artistiques, de produits dérivés et d'outils de gestion de droits

**L'un des principaux cas d'usage des NFT consiste à présenter le titulaire du jeton comme étant le détenteur de l'œuvre d'art qu'est le fichier sous-jacent, le plus souvent une image.** Les jetons sont alors le plus souvent non fongibles et édités en série limitée et numérotée. Le fichier associé au jeton peut être une œuvre d'art « nativement » numérique ou le « jumeau numérique » d'une œuvre réelle. L'analyse de la qualification juridique des « NFT artistiques », développée en 1.2, montre néanmoins qu'ils ne peuvent aucunement être considérés comme une œuvre ni, plus généralement, comme une forme, même dégradée, de propriété sur une œuvre ou son support.

**La justification de ce cas d'usage repose sur la légitimité sociale, à défaut de reconnaissance juridique, que confère la détention du jeton.** En effet, seul le propriétaire du jeton est reconnu comme « propriétaire » légitime de la ressource vers lequel il pointe, quand bien même cette ressource est duplicable à l'infini et peut être légalement téléchargée par tout internaute en application du droit à la copie privée. Les NFT permettent donc d'introduire une logique de détention ostentatoire. Cette logique est fragile car la détention du NFT ne procure pas, en tant que telle, de droits à son propriétaire (*cf.* 2.1). Elle ne lui garantit pas que l'émetteur du jeton est le titulaire légitime des droits sur l'œuvre associée au jeton ni l'intégrité du ficher numérique vers lequel il pointe. Tout un écosystème s'est néanmoins constitué autour de l'art numérique natif et tend à légitimer ce cas d'usage : artistes, galeries, maisons de ventes aux enchères et même musées ; le musée Pompidou, à Paris, ayant acquis en février 2023 des œuvres d'art associées à des NFT.

[3] *Blockchain Games Report*, n° 12, mars 2023.

**La logique est la même pour l'utilisation des NFT en tant que « jumeaux numériques » d'œuvres existantes.** Les acquéreurs souhaitent pouvoir afficher une « propriété » de ces objets virtuels, par exemple dans des métavers, tandis que les musées peuvent y voir une source de recettes complémentaires. Ce cas d'usage est néanmoins encore plus contestable que l'art natif dans la mesure où il existe déjà un propriétaire légitime de l'œuvre — plus précisément, de son support corporel — et où les œuvres relèvent en règle générale du domaine public. À la connaissance de la mission, aucun musée français n'a pour l'instant publiquement expérimenté la « tokénisation » d'œuvres qu'il détient.

**Les NFT sont également utilisés par les institutions culturelles en tant que produits dérivés à destination des visiteurs.** Ils sont, dans ce cas, associés à des images qui font office de souvenirs, comme les cartes postales ou affiches vendues à la sortie des musées. La détention du NFT peut, dans certains cas, donner accès à des contenus interactifs complémentaires, ou ouvrir l'accès à une « communauté » : les détenteurs du NFT peuvent par exemple voir leur nom publié au sein d'une liste de soutiens, accéder à des espaces de discussion réservés, ou obtenir l'accès à des événements privatifs. Dans ce cas, la valeur du NFT, vendu à un prix variable selon l'expérience associée, ne réside pas dans sa dimension ostentatoire mais dans l'utilité des expériences. À la frontière de ce cas d'usage, les NFT peuvent constituer un certificat de mécénat dont le support peut avoir une dimension artistique : la logique de collecte de fonds est assumée par l'émetteur et les acquéreurs embrassent la logique ostentatoire, non pour afficher une « propriété légitime » mais pour afficher publiquement un soutien.

**Les NFT peuvent, enfin, constituer des outils à vocation plus technique que commerciale, utiles à certains usages rencontrés dans le secteur culturel.** Grâce aux programmes autonomes (*smart contracts*), des NFT peuvent être utilisés pour calculer les droits qui reviennent à différents acteurs impliqués dans une création artistique protégée par le code de la propriété intellectuelle (la production d'un film, par exemple). Si ces acteurs sont rémunérés en cryptomonnaies, les jetons peuvent même être utilisés pour opérer les flux financiers associés à ces droits. Les NFT peuvent aussi être utilisés comme supports de billets d'événements sportifs ou culturels afin de limiter la fraude, puisqu'ils ne peuvent être dupliqués, et de rendre ces billets cessibles entre clients, ce qui apporte de la liquidité sur le marché.

### 1.1.3. Les NFT peuvent servir à la fois à représenter des objets de consommation virtuels et à faire office de certificats numériques liés à des objets réels

De même qu'ils permettent de conférer un droit de « propriété » sur un objet de jeu virtuel (*cf.* 1.1.1) utilisé dans un jeu vidéo, **les NFT peuvent être associés à des objets de consommation dans les univers virtuels, appelés métavers**. Leurs caractéristiques techniques permettent d'identifier un propriétaire unique d'un jeton donné, et donc de l'objet virtuel sous-jacent associé. Si les éditeurs des métavers s'engagent à autoriser l'utilisation, dans les métavers, des objets concernés uniquement aux utilisateurs détenteurs des NFT correspondants, alors la propriété des objets réels est répliquée dans ces mondes virtuels et tous les objets réels peuvent avoir un jumeau numérique associé à un NFT. Dans la mesure où les métavers constituent des lieux de sociabilité avant tout, la logique ostentatoire prime de nouveau, si bien que les objets les plus susceptibles d'être numérisés sont, aujourd'hui, des accessoires de mode. Ce nouveau mode de consommation ouvre des débouchés pour les entreprises du secteur du luxe, dont la France abrite plusieurs leaders mondiaux, mais soulève également des interrogations en matière d'image de marque, de positionnement tarifaire et d'adoption réelle des métavers par le grand public.

C'est pourquoi le cas d'usage des NFT lié à la consommation sur lequel les entreprises rencontrées par la mission investissent le plus relève davantage de l'outil marketing que du produit à vendre. Plusieurs utilisations sont envisageables. **Les NFT peuvent tout d'abord représenter des objets numériques, souvent à dimension artistique, et être vendus comme un signe d'appartenance à une communauté de clients privilégiés** qui ouvre accès à des expériences réservées aux détenteurs des NFT (promotions, réseau social dédié, expériences particulières en boutique, invitations à des événements culturels, *etc.*). Dans ce cas, le NFT est bien un *utility token*, acheté pour les « privilèges » auxquels il donne droit. **Ce cas d'usage est parfois à la croisée du mécénat** puisque les marques peuvent s'engager à reverser les recettes des ventes à un projet associatif. Il présente en outre des porosités avec les deux cas d'usage précédents : les jeux vidéo constituent une forme de métavers, et certains objets numériques peuvent se situer à la frontière entre l'œuvre d'art et le produit dérivé.

**Les NFT peuvent aussi être émis à titre gratuit et associés à l'achat d'un produit réel. Le NFT devient ainsi un certificat d'achat ou un « passeport numérique » du produit**. Un tel certificat permet d'avoir accès à des informations sur le produit (traçabilité, conseils d'entretien, etc.) et peut être utilisé pour prouver sa propriété, auprès du fabricant en cas de réparation ou auprès d'un autre particulier en cas de revente. **Il peut aussi donner accès, gratuitement, à des expériences relatives à la marque ou au produit et ainsi, faire office d'outil marketing** visant à la fois à associer la modernité technologie à l'image de marque de l'émetteur, à recruter de nouveaux clients dans le segment ciblé (jeunes technophiles) et à fédérer la communauté de clients.

### 1.1.4. Les cas d'usages des JVC sont, pour le moment, peu nombreux

Les JVC relèvent de cas d'usages variés, qui reposent tous sur leur capacité à dupliquer dans le monde virtuel une « propriété ». En synthèse, la mission peut dresser deux constats.

**Premièrement, les cas d'usage recensés par la mission ne sont pas très nombreux[4] et les modèles économiques qui leur sont liés sont rarement matures.** Les entreprises réussissant à prospérer sur la base de ces cas d'usage sont rares (*cf.* 3.1, sur l'écosystème français), les effets d'entraînement sur l'économie française sont donc, pour l'instant, limités.

**L'écosystème des *blockchains* étant très mouvant, les cas d'usages observés aujourd'hui ne sauraient épuiser toutes les potentialités des JVC**, qui trouveront peut-être de nouvelles utilisations au fil du développement des technologies liées aux *blockchains* et, si elle advient, de leur adoption par le grand public. Par ailleurs, les JVC ne constituent qu'une composante de cet ensemble technologique, qui présente d'autres champs d'utilisation, notamment en matière financière (finance décentralisée, par exemple).

**Deuxièmement, la mission constate que le recours aux JVC apporte parfois peu de valeur ajoutée par rapport à des bases de données classiques**, notamment quand le jeton n'a pas vocation à être revendu par son détenteur (mécénat, programmes de fidélité, passeport numérique) et que le développement de certains cas d'usage est conditionné à des hypothèses fortes (intégration de l'interopérabilité dans le monde des jeux et des métavers, adoption des technologies *blockchain* et métavers au sein du grand public). De nombreux interlocuteurs de la mission ont rappelé que l'utilisation des JVC était une possibilité parmi d'autres pour leur cas d'usage, et que ce choix était au moins pour partie motivé par des raisons de marketing qui, si elles sont compréhensibles d'un point de vue commercial, constituent une justification fragile de la technologie. Le retournement du marché observé à l'automne 2022 rend le secteur plus concurrentiel et devrait permettre de distinguer les modèles économiques viables des propositions reposant essentiellement sur un effet de mode.

[4] La mission a également identifié le cas d'usage de l'identité numérique, pour lequel les jetons n'ont cependant pas une vocation commerciale mais technique. Encore peu développé, ce cas d'usage est traité en annexe III.

**Le potentiel des JVC est à mettre en regard de leurs coûts et des risques qu'ils posent**. Comme toutes les inscriptions sur les *blockchains*, les transactions faisant intervenir des JVC se font sous pseudonymes et posent des difficultés en matière de lutte anti-blanchiment, puisque l'identité des parties n'est pas publique. Par surcroît, certaines technologies se développent pour permettre de rendre les transactions sur *blockchains* intraçables (*cf.* section 2.4).

**Les données inscrites sur une *blockchain* étant publiques, et le fonctionnement des *blockchains* étant par nature décentralisé, leur utilisation pose également un problème en matière de protection des données personnelles,** puisque certaines données inscrites constituent des données personnelles (les données de transaction, par exemple). La Commission nationale de l'informatique et des libertés (CNIL) a publié en septembre 2018 une position analysant la conformité des *blockchains* au règlement général sur la protection des données (RGPD). Cette position indique que de nombreux droits des personnes concernées sont compatibles avec les *blockchains* (droit à l'information, droit d'accès, droit à la portabilité) mais constate que d'autres droits ne peuvent être respectés (droit de rectification, droit à l'effacement). La CNIL recommande donc de ne pas faire figurer de données personnelles sur les *blockchains*, dans une logique principalement préventive. Des procédés cryptographiques permettent parfois d'utiliser l'infalsifiabilité des *blockchains* sans inscrire directement de données personnelles, par exemple lorsque le but est de prouver la détention d'une information sans la révéler. En revanche, lorsque les données sont relatives à des transactions, le respect des droits garantis par le RGPD suppose l'utilisation de techniques d'anonymisation qui constituent un important facteur de risque de blanchiment, et supposent donc que des tiers de confiance centralisés conservent une copie des données. Un travail d'harmonisation des positions des régulateurs européens est en cours, notamment sur la qualification des « mineurs » (ordinateurs chargés de la validation des transactions sur la *blockchain*) et des concepteurs de *smart contracts* de sous-traitants au sens du RGPD, mais n'a pas, pour l'instant, abouti. Il devrait conduire à clarifier l'effectivité des droits reconnus par le RGPD, soit en tirant les conséquences de l'incompatibilité des traitements de données sur *blockchain* avec le droit, soit en modifiant ce dernier.

**Enfin, l'utilisation des *blockchains* présente un coût environnemental majeur, au vu de la consommation électrique nécessaire à leur fonctionnement** (émissions de l'ordre de 400 kg équivalents $CO_2$ en 2020 pour chaque transaction sur *Bitcoin*, soit l'équivalent d'un aller simple Paris-New York en avion pour un passager). L'émergence de technologies annexes (*layers 2*, *Lightning Network*, preuve d'enjeu) peut permettre de considérablement réduire la consommation énergétique, au prix néanmoins d'une recentralisation des systèmes ou de moindres garanties de sécurité. Un développement plus soucieux de l'environnement est donc envisageable mais la « promesse » des *blockchains* en serait altérée : quels que soient les progrès récents, leur avenir reste soumis à un triangle d'incompatibilité entre décentralisation, sécurité et passage à grande échelle. Ces enjeux techniques sont abordés en annexe I.

## 1.2. Le jeton est distinct de son sous-jacent et ne confère, à lui seul, aucun droit

Tant le vocabulaire utilisé par les utilisateurs des *blockchains* (*wallet*, *smart contract*, *owner*, *etc.*) que l'utilisation qui est faite des jetons laissent penser que le titulaire du jeton jouit de droits du seul fait de sa détention. Cette vision donne lieu à des confusions entre le jeton, c'est-à-dire l'inscription dans la *blockchain* d'une association entre une URL et l'adresse d'un détenteur, et les données auxquelles il renvoie, voire les objets réels auxquels il peut être fait référence. Une telle confusion est présente, par exemple, dans l'expression « *œuvres d'art sous forme de NFT* » : l'œuvre (en l'espèce, une image, qui a pour support immatériel un fichier stocké sur un serveur) est bien distincte du jeton (inscription sur une *blockchain* du nom d'un titulaire) qui lui est associé. Juridiquement, il faut bien distinguer le sous-jacent, qui constitue un premier bien, et le jeton, qui constitue un bien incorporel différent. Le plus souvent, le second n'est que l'accessoire du premier, considéré comme principal.

**Les qualités de sécurité et d'infalsifiabilité des *blockchains* ne doivent pas tromper leurs utilisateurs en laissant penser qu'une *blockchain* constitue, par elle-même, une source de droits.** Les *blockchains*, au même titre que les jetons qui leur sont associés, sont des outils informatiques utilisant des techniques cryptographiques. La possession d'un jeton à elle seule ne confère aucun droit : elle ne peut qu'être associée à des droits par ailleurs définis grâce à des actes juridiques classiques, comme les contrats. Ainsi, un jeton ne constitue ni un contrat ni un titre de propriété.

Un JVC peut être dépourvu de tout contrat associé. Dans ce cas, il ne conférera aucun droit ou créance sur un tiers, et sera purement spéculatif et ostentatoire. La simple propriété du jeton n'emporte aucun droit sur l'objet virtuel vers lequel il pointe, ce qui est normal puisque n'importe quel utilisateur peut créer n'importe quel jeton pointant vers n'importe quel objet virtuel.

La majorité des JVC visent néanmoins à conférer des droits : créance sur un projet financé grâce au JVC, accès à des expériences privilégiées, droit à réception d'un objet réel, accès à un service informatique, transfert de droits de propriété intellectuelle. Dans ce cas, l'émetteur du JVC doit être détenteur des droits qu'il souhaite associer au NFT (par exemple, détenir les droits de propriété qu'il transfère) et prévoir un contrat en parallèle. La clarification de ces droits est un des enjeux clés de l'accompagnement du développement de ces technologies.

## 2. Le développement des jetons à vocation commerciale soulève plusieurs problèmes juridiques, dont certains relèvent du droit de l'Union européenne

Le développement des jetons à vocation commerciale à plus grande échelle, que ce soit au sein des cas d'usage identifiés par la mission ou par l'émergence de nouveaux cas d'usage, suppose de traiter un certain nombre de difficultés juridiques qui, actuellement, font peser des risques ou apportent de l'insécurité juridique qui agissent comme un frein. Un cadre clair favorise le développement de ces technologies, comme le montre le succès de la Suisse qui s'est affirmée comme l'un des acteurs les plus dynamiques en Europe grâce à son cadre réglementaire.

### 2.1. La protection des consommateurs requiert de préciser la qualification juridique des jetons en clarifiant les droits associés à chaque jeton

En application du règlement européen MiCA[5], un jeton devra être accompagné lors de son émission de certaines informations, en fonction de sa nature : prospectus[6] pour un *security token* et livre blanc pour un cryptoactif soumis au titre II du règlement (*cf.* 2.3). Néanmoins, certains jetons sont exclus de ces dispositions de MiCA : les *utility tokens* présentant certaines caractéristiques[7], les NFT (*cf.* 2.3.2), ainsi que les jetons qui ne sont pas admis à la négociation sur une place de marché centralisée et dont le volume d'émission est inférieur à 1 M€ par an. La mission considère qu'un document contractuel explicitant les droits associés doit accompagner l'émission de ces jetons.

[5] Règlement sur les marchés de crypto-actifs, et modifiant les règlements (UE) n° 1093/2010 et (UE) n° 1095/2010 et les directives 2013/36/UE et (UE) 2019/1937 présenté *infra* en section 2.3.

[6] En vertu du règlement (UE) 2017/1129 du Parlement européen et du Conseil du 14 juin 2017 concernant le prospectus à publier en cas d'offre au public de valeurs mobilières ou en vue de l'admission de valeurs mobilières à la négociation sur un marché réglementé.

[7] Les *« utility tokens »* émis en vue de l'accès à un service qui sera développé ultérieurement à leur émission ou admis à la négociation sur une plateforme réglementée doivent néanmoins être accompagnés d'un livre blanc.

### 2.1.1. La protection des consommateurs requiert de préciser les droits associés à chaque jeton dans un document contractuel que la mission recommande d'annexer au jeton

Les jetons à usage commercial sont souvent associés à un sous-jacent et ouvrent des droits (accès à un jeu, réception d'un bien matériel, *etc.*). Ces droits peuvent être « consommables » (si le jeton donne droit à une place de concert, une fois la place utilisée, le droit est éteint) ou permanents. Ces droits sont attachés au jeton : le détenteur du jeton est donc censé en bénéficier, quel qu'il soit. Ils passent donc par plusieurs relations contractuelles : une relation originelle entre l'émetteur du jeton (auquel le droit est généralement opposable) et son premier acquéreur puis à chaque revente du jeton, sur le marché secondaire. Ces droits trouvent en principe leur siège dans les documents contractuels associés au jeton – contrat, conditions générales d'utilisation ou de vente – mais ceux-ci n'existent pas toujours.

Le code de la consommation encadre les ventes entre professionnels et consommateurs particuliers. Son article L. 221-5 prévoit notamment que le professionnel a l'obligation de fournir au consommateur l'information des « *caractéristiques essentielles du bien, du service, du service numérique ou du contenu numérique* », ce « *de manière lisible et compréhensible* ». Les droits associés au jeton font partie de ces caractéristiques essentielles. Elles devraient donc être transmises au consommateur à chaque fois que le jeton est (re)vendu par un professionnel **Or, la mission constate que ce n'est pas toujours le cas, ce qui est source d'insécurité juridique pour les consommateurs, qui ne connaissent pas toujours les droits qui leurs sont garantis et qu'ils peuvent réellement opposer à l'émetteur**.

Par ailleurs, cette protection ne vaut que pour les ventes entre professionnels et particuliers. Or, les jetons ont pour qualité principale d'être cessibles, donc de donner lieu à des reventes entre particuliers, notamment sur les plateformes de pair à pair. Dans ces cas, la revente du jeton s'apparente à un transfert de créance, le plus souvent implicite et déduit du transfert du jeton sur la *blockchain*. Le contrat, même s'il était présent lors de la vente primaire avec un professionnel, peut ne pas « suivre » le jeton si les parties ne se sont pas explicitement entendues pour cela : dans ce cas, les acheteurs secondaires n'ont aucune visibilité sur les droits associés au jeton.

C'est pourquoi la mission recommande d'amender le code de la consommation afin d'obliger les émetteurs de jetons à annexer à tout jeton destiné à être vendu un document contractuel présentant les droits associés. Étant annexé au jeton (si possible, avec un *hash* prouvant son immuabilité), le contrat le « suivrait » ainsi et bénéficierait également aux acquéreurs secondaires. Cette protection vaudrait pour tous les jetons à usage commercial. Afin d'en maximiser l'effectivité et l'adéquation avec les principes du marché unique, la mise en œuvre de cette protection devrait être envisagée dans le cadre des discussions à venir sur un texte ayant vocation à compléter le règlement MiCA.

**<u>Proposition n° 1</u> : Rendre obligatoire l'association à tout jeton à vocation commerciale émis ou/et échangé dans l'Union européenne d'un document contractuel définissant les droits et obligations incorporés comme sous-jacent dont bénéficie le porteur du jeton (*cf.* annexe IV).**

### 2.1.2. La valeur juridique des inscriptions sur *blockchain*, notamment en matière probatoire, peut être reconnue à droit constant

L'enjeu de la reconnaissance de la valeur juridique des inscriptions sur *blockchain* est une condition au développement à grande échelle de ces technologies. Considérant que cette valeur juridique n'est pas garantie en l'état actuel du droit, la Fédération française des professionnels de la blockchain (FFPB) a proposé une modification du code des postes et des communications électroniques[8].

La question de la valeur juridique des inscriptions sur les *blockchains* se pose dans plusieurs situations qui doivent être distinguées, selon que ces inscriptions :

- sont utilisées pour prouver des *faits juridiques*, par exemple le fait qu'une personne ait eu connaissance d'une information à une certaine date. Dans ce cas, **la preuve est libre hors des cas où la loi en dispose autrement** (art. 1358 du Code civil) ;
- sont utilisées pour prouver l'existence *d'actes juridiques*, par exemple l'existence d'un engagement de l'émetteur de jetons vis-à-vis de la personne qui les achète. Dans ce cas, **l'écrit[9] est obligatoire, conformément à l'article 1359 du Code civil**, sauf pour les cas dans lesquels l'obligation dont on cherche à prouver l'existence a une valeur inférieure à 1 500 € ou est celle d'un commerçant (la preuve est alors libre) ;
- respectent les conditions de formes requises pour la validité de certains *actes juridiques*, et notamment pour les contrats qui pourraient être passés *via* une *blockchain*. **Sur la validité des contrats, le principe est celui du consensualisme** (art. 1172 du Code civil) : la validité des contrats n'est soumise à aucune condition de forme, sauf quand la loi en dispose autrement. Par exemple, l'article 1322 du Code civil requiert que les cessions de créance soient constatées par écrit. Dès lors que l'une des finalités principales de JVC est de constituer un titre de créances sur l'émetteur, **il est nécessaire pour que ce cas d'usage puisse prospérer que les transferts de jetons sur une *blockchain* aient la valeur d'un écrit.**

Dans les situations dans lesquelles la preuve est libre et la passation des contrats dispensée de toute forme, la valeur juridique des inscriptions sur une *blockchain* n'est source d'aucune difficulté (il appartient au juge d'apprécier la force probante des inscriptions). Dès lors que le code source des programmes utilisés sur la *blockchain* est public, **l'intelligibilité** des données inscrites, entendue comme la possibilité de retrouver une signification, peut être reconnue par le juge. De même, **l'intégrité** des données inscrites sur la *blockchain* peut être établie par le juge en se fondant sur le fonctionnement technique des *blockchains*, bien que celles-ci ne bénéficient pas de présomption d'intégrité. Le développement du commerce électronique dans les années 2000 constitue un précédent : dans les contentieux relatifs aux contrats conclus à distance, les problématiques d'intégrité et d'intelligibilité des paquets de données échangés lors des achats n'ont pas suscité de difficulté.

En conséquence, une fois déterminés le sens, l'auteur et l'intégrité des inscriptions, **ce n'est que lorsque la loi rend l'écrit obligatoire que leur valeur juridique peut être problématique**.

Pour que l'écrit électronique ait la même force probante que l'écrit parfait sur support papier, trois conditions, définies aux articles 1366 et 1367 du Code civil, doivent être remplies :

- la personne dont il émane doit pouvoir être « *dûment identifiée* » ;
- il doit être « *établi et conservé dans des conditions de nature à en garantir l'intégrité* » ;
- il doit être signé électroniquement.

---

[8] FFPB, *Blockchain et preuve : pour une reconnaissance de la valeur probatoire de la blockchain en droit français*, mars 2023.

[9] La preuve écrite s'entend comme la preuve par un écrit *parfait*, et donc signé.

**Or, le terme « *signature électronique* » désigne, dans le domaine juridique, la réunion de l'empreinte obtenue par la clef privée avec un certificat de signature électronique assurant que la clef privée appartient à l'auteur.** Les signatures utilisées pour réaliser des inscriptions sur les *blockchains* publiques sont généralement dépourvues de certificat. De ce fait, une inscription sur une *blockchain* ne constitue pas toujours un écrit fiable au sens des articles 1366 et 1367 du Code civil.

**Cependant, les inscriptions sur une *blockchain* peuvent, à droit constant, constituer des écrits parfaits** : il suffit pour cela que la signature électronique utilisée soit associée à l'auteur par un certificat électronique émis par un tiers qualifié de prestataire de services de confiance au sens du règlement européen eIDAS. Les prestataires de services sur cryptoactifs qui hébergent les portefeuilles des utilisateurs peuvent assurer ce rôle.

Si les pouvoirs publics souhaitaient favoriser la reconnaissance juridique des écrits électroniques réalisés sans passer par un tiers de confiance — qu'ils soient inscrits sur une *blockchain* ou sur un autre type de support —, il serait préférable, plutôt que de modifier le droit pour accorder aux signatures électroniques sur *blockchain* une présomption de fiabilité[10], de modifier le régime des écrits électroniques. Une telle évolution pourrait en particulier passer par un assouplissement de l'obligation de certification par un tiers du lien entre la clef de signature et l'auteur de l'acte et par un alignement des régimes applicables aux signatures manuscrites et électroniques. Cet enjeu dépasse toutefois le cadre de la mission (*cf.* annexe IV).

### 2.1.3. Les droits portés par des « NFT artistiques » sont limités et doivent inciter à la prudence

**Contrairement à certaines présentations rencontrées au sein de la communauté des utilisateurs de NFT, ces derniers ne peuvent pas, en droit français, constituer des œuvres d'art.** Comme l'a rappelé le rapport de M. Jean Martin, avocat à la Cour et M^me^ Pauline Hot, auditrice au Conseil d'État, remis en juillet 2022 au conseil supérieur de la propriété littéraire et artistique (CSPLA), le code de la propriété intellectuelle, suppose, pour qu'un travail soit qualifié d'œuvre de l'esprit, que soient remplies des conditions d'originalité et de mise en forme. Or, le NFT ne constitue que la réunion, dans la mémoire d'un programme, de l'identifiant d'un détenteur, d'un lien vers l'emplacement du fichier numérique constituant l'œuvre, et d'éventuelles métadonnées.

**Le jeton doit donc être distingué de l'œuvre vers laquelle il pointe. Il ne peut pas davantage être qualifié de support de l'œuvre.** En effet, le support constitue un bien matériel soumis aux règles de propriété du code civil et dissocié de l'œuvre de l'esprit incorporelle soumise aux règles de la propriété intellectuelle. Le NFT n'est qu'un outil technique « pointant » vers le fichier numérique constituant le support immatériel de l'œuvre, lui-même stocké sur un support physique (disque dur, cartes mémoires, *etc.*).

**Enfin, le NFT ne saurait être regardé comme un certificat d'authenticité ou d'unicité de l'œuvre sur laquelle il porte.** En effet, aucun élément n'assure, en cas d'émission d'un NFT « sur » une œuvre d'art, que seul un NFT a été émis, que l'œuvre vers laquelle il pointe est authentique et que le fichier ne sera pas altéré ultérieurement. Les propriétés d'infalsifiabilité et d'unicité du jeton sur la *blockchain* ne doivent pas laisser penser que le sous-jacent en bénéficie aussi.

[10] En effet, les caractéristiques techniques des *blockchains* apportent des garanties en matière d'intégrité des données mais pas de fiabilité de la signature puisqu'aucune vérification de l'identité des utilisateurs n'est opérée.

**Dès lors, les NFT ne peuvent qu'être « nus » ou constituer des titres de droits portant sur certains droits d'auteur afférents aux œuvres vers lesquelles ils pointent.** Les droits d'auteur sont composés de droits moraux inaliénables et éternels et de droits patrimoniaux (droits d'exploitation, comme la reproduction ou la représentation), qui sont cessibles et ont une durée limitée (ils expirent 70 ans après le décès de l'auteur, l'œuvre entre ensuite dans le domaine public). Ces droits peuvent être cédés par contrat écrit (article L. 131-2 du code de la propriété intellectuelle, CPI). Si les inscriptions sur *blockchain* peuvent être considérées comme des écrits parfaits (*cf.* 2.1.2), alors les NFT pourraient valoir contrat de cession de droits patrimoniaux sur des œuvres d'art.

**Cependant, selon la majorité de la doctrine, la loi doit être interprétée comme interdisant la sous-cession de droits (par exemple, via une revente sur le marché secondaire du jeton) sans le consentement de l'auteur**, par application extensive d'une prescription relative aux contrats d'édition (articles L. 132-7 et L. 132-16 du CPI). Pour permettre au NFT d'être le siège de droits portant sur une œuvre d'art, l'auteur de cette dernière devrait donc, dès l'émission du jeton, prévoir un contrat de licence stipulant qu'il concède un ensemble de droits d'exploitation à toute personne, sous réserve que le concessionnaire détienne le NFT au moment où a lieu cette exploitation. Cette possibilité doit toutefois être expertisée par le ministère de la culture et validée par le juge.

L'étendue des droits qui pourraient être ainsi associés à un NFT reste toutefois limitée. En effet, de nombreuses œuvres relèvent du domaine public ou ne sont pas protégées par le CPI. Même pour celles qui sont protégées, une telle licence ne procurerait que peu d'avantages supplémentaires (si ce n'est, le cas échéant, un droit d'exploitation publique ou commerciale) par rapport au droit à la copie privée.

**<u>Proposition n° 2</u> : Confirmer la compatibilité des dispositions du CPI relatives aux cessions de droit d'auteur (article L. 132-7) avec une licence de cession de droits à une personne identifiée par la détention d'un jeton, et envisager une modification de ces articles dans le seul cas où une incompatibilité serait identifiée. Fournir un modèle de contrat de licence qui pourrait être utilisé par les acteurs économiques (*cf.* annexe IV).**

## 2.2. La qualification juridique des jetons emporte des conséquences fiscales que la mission recommande de clarifier

L'analyse des jetons porteurs de droits comme des objets accessoires par rapport à leur sous-jacent, considéré comme objet principal, devrait entraîner un traitement fiscal des NFT qui reste à clarifier, notamment en matière de fiscalité des particuliers.

**Une incertitude demeure sur le régime fiscal appliqué aux plus-values réalisées par des particuliers sur la revente de jetons, notamment de NFT**. En effet, les jetons[11] rentrent dans la catégorie des actifs numériques, définis à l'article L. 54-10-1 du code monétaire et financier (CMF). **L'article 150 VH bis du code général des impôts (CGI) prévoit un régime dédié aux plus-values réalisées sur les actifs numériques cédés contre un autre bien ou contre de la monnaie**, qui sont imposées au prélèvement forfaitaire unique de 30 % (12,8 % d'impôt sur le revenu – IR – et 17,2 % de prélèvements sociaux). Les ventes d'actifs numériques contre actifs numériques sont en revanche exonérées.

[11] Définis à l'article L. 552-2 du CMF.

**Ainsi, l'application de l'article 150 VH bis porte sur tous les actifs numériques de manière uniforme et est indifférente à leur sous-jacent** (sauf si le jeton est assimilé à un instrument financier, auquel cas il est fiscalisé comme tel). Dans les faits, il est très rare que les plus-values sur NFT (comme sur l'ensemble des actifs numériques) soient imposées, puisque les NFT sont quasiment toujours échangés contre des cryptomonnaies, donc contre d'autres actifs numériques. L'imposition n'a lieu que lorsque les sommes détenues sous forme d'actifs numériques sont converties en monnaie *fiat*.

**La mission recommande de considérer les jetons utilitaires comme des objets accessoires en matière fiscale, donc d'appliquer aux cessions de tels jetons le régime fiscal de l'objet principal**. Les ventes de ces jetons contre un autre actif numérique ne rentreraient donc pas dans le champ de l'article 150 VH bis du CGI. Leur acquisition à l'aide d'un actif numérique emporterait imposition des plus-values réalisées sur ce dernier.

**Les plus-values de cession sur ces jetons seraient alors assujetties au régime des biens meubles**, corporels ou incorporels : imposition des plus-values à hauteur du 36,2 % (19 % d'IR et 17,2 % de prélèvements sociaux), avec un abattement de 5 % sur la plus-value brute pour chaque année de détention du bien, au-delà de la deuxième année.

Il convient de préciser que les NFT ne peuvent pas être considérés comme des œuvres d'art en matière fiscale. En effet, la doctrine fiscale précise que les objets d'art visés par le CGI doivent être produits à douze exemplaires maximum, ce qui n'est pas possible pour un fichier numérique. Dès lors, le régime des objets précieux et œuvres d'art ne peut pas être applicable et seul le régime des biens meubles semble envisageable pour les cessions de NFT avec sous-jacent[12].

Le périmètre d'application de l'article 150 VH bis du CGI ainsi redéfini pourrait être précisé par l'administration fiscale dans la doctrine afin d'en informer les acteurs économiques concernés. L'opportunité de modifier le droit doit être expertisée, selon la mission, dans la mesure où les NFT demeurent techniquement des actifs numériques pour lesquels un régime spécial a été conçu et dont il pourrait être difficile de s'extraire sans clarification du droit. Les définitions sur lesquelles repose ce régime fiscal ayant vocation à être amendées lors de l'entrée en vigueur du règlement européen MiCA, celle-ci pourrait constituer une bonne occasion pour procéder à la clarification du régime fiscal.

**<u>Proposition n° 3</u> : Appliquer aux plus-values réalisées sur jetons utilitaires le régime fiscal de leur sous-jacent, c'est-à-dire celui des biens meubles, et non le régime prévu pour les actifs numériques par l'article 150 VH bis du CGI (*cf.* annexe VI).**

**La mission souligne que le traitement fiscal du sous-jacent qu'elle recommande en matière de fiscalité des plus-values est aligné avec l'analyse de la Commission européenne en matière de TVA.** Dans un document de travail du 21 février 2023, le Comité TVA indique en effet qu'un NFT peut être qualifié, selon les cas, de titre de propriété ou de bon (à usage unique ou multiple). Dans tous les cas, c'est le sous-jacent qui détermine l'application du régime de TVA.

[12] Un jeton dépourvu de sous-jacent (par exemple, un NFT artistique nu) resterait qualifié d'actif numérique et relèverait du régime fiscal afférent.

**L'application de la TVA aux ventes de NFT soulève, en revanche, un problème de territorialité.** En effet, lorsque les NFT ont pour sous-jacent une livraison de service électronique, le principe de destination s'applique : le taux de TVA à appliquer est celui du pays de résidence du consommateur (*cf.* article 259 D du CGI et article 58 de la directive TVA). Or, les entreprises commercialisant des NFT ne connaissent pas nécessairement le pays de résidence de leurs clients, la livraison se faisant sur une *blockchain*. L'adresse IP pourrait constituer un élément de preuve, si le client doit passer par un site internet qui fournit cette information au prestataire, mais il ne serait pas suffisant à lui seul. Dès lors, toute vente de NFT devrait être, *a priori*, accompagnée d'une procédure d'identification du pays de résidence du client. Il reste à savoir quelles modalités de collecte de cette information sont jugées suffisantes par l'administration fiscale, enjeu propre à toute prestation de service électronique.

**La fiscalité des entreprises relative aux jetons ne pose pas, quant à elle, de difficulté particulière.** La vente de NFT émis par des sociétés donne lieu à des produits, qui viennent abonder le résultat imposable. Le plan comptable général a été révisé en 2018 pour expliciter les modalités de comptabilisation des jetons. Lorsque les NFT sont acquis puis revendus, ceux-ci sont comptabilisés comme des immobilisations incorporelles. Les plus-values sur cryptoactifs obéissent aux règles de la fiscalité des plus-values professionnelles pour les sociétés soumises à l'impôt sur les sociétés (IS). Les plus-values professionnelles nettes à long terme[13] sont taxées au taux d'IS de 15 % (article 219 du CGI). Les plus-values de court terme sont intégrées au résultat imposable, soumis au taux normal de l'IS, fixé par l'article 219 du CGI à 25 %.

## 2.3. Le règlement MiCA pose un cadre de régulation, dont l'application aux NFT n'ira pas sans poser de difficultés

### 2.3.1. Le règlement MiCA va, à compter de la fin de l'année 2024, se substituer au cadre réglementaire instauré par la loi PACTE

**Le cadre réglementaire relatif aux cryptoactifs a été défini, en France, par la loi n° 2019-486 du 22 mai 2019 relative à la croissance et à la transformation de l'économie (« loi PACTE »).** Cette loi définit, à l'article L. 54-10-1 du CMF, les « actifs numériques » (terme équivalent aux cryptoactifs du langage courant), dont font partie les jetons, eux-mêmes définis à l'article L. 552-2 du CMF.

La loi PACTE instaure un cadre réglementaire relatif à deux types d'activités :

- en matière de levées de fonds par émission de jetons offerts au public (en anglais, « *initial coin offerings* », ICO), la loi prévoit la possibilité, pour l'émetteur, de produire un livre blanc sur l'offre et de solliciter un visa de l'Autorité des marchés financiers (AMF). Ce régime est optionnel et a connu un succès limité : au 1er avril 2023, seuls quatre documents d'informations relatifs à des ICO avaient reçu un visa de l'AMF ;

[13] En vertu de l'article 39 duodecies du CGI, une plus-value est considérée comme à court terme si l'actif est cédé moins de deux ans après son acquisition, et à long terme si l'actif est cédé plus de deux ans après son acquisition.

- en matière de prestataires de services sur actifs numériques (PSAN), la loi prévoit l'obligation, pour les prestataires qui proposent certaines activités (l'achat et la vente d'actifs numériques, l'échange d'actifs numériques contre d'autres actifs numériques, la conservation pour compte de tiers et l'exploitation d'une plateforme de négociation d'actifs numériques), d'effectuer un enregistrement auprès de l'AMF. La procédure d'enregistrement est légère : l'AMF vérifie l'honorabilité et la compétence des dirigeants et le respect de certaines exigences en matière de lutte contre le blanchiment. La loi offre aussi aux PSAN la possibilité, optionnelle, de demander un agrément, dont le niveau d'exigences est plus élevé (niveau de fonds propres suffisant, ségrégation des actifs propres et des actifs des tiers, publication des ordres de transactions, *etc.*). Si l'enregistrement obligatoire a bien été sollicité et obtenu, au 5 avril 2023, par 71 PSAN, aucun n'a sollicité l'agrément facultatif**.**

**Le cadre réglementaire français sera remplacé, lors de son entrée en application, par le règlement européen sur les marchés de cryptoactifs (MiCA).** Le texte, déposé par la Commission européenne en septembre 2020, a été adopté dans sa version définitive par le Parlement européen le 20 avril 2023 et devrait être publié au *Journal officiel* de l'UE durant l'été 2023. Il sera rendu applicable 18 mois après son entrée en vigueur, soit à la fin de l'année 2024, avec une période de transition de 18 à 36 mois pour les émetteurs de jetons et prestataires de services qui exerçaient leur activité avant l'entrée en application du règlement.

À l'instar de la loi PACTE, dont il s'inspire sur plusieurs points, le règlement MiCA instaure un cadre de réglementation :

- il impose aux émetteurs de cryptoactifs la **publication d'un livre blanc** (pour certains cryptoactifs et au-delà de certains seuils) permettant aux investisseurs de disposer des informations nécessaires à une décision éclairée, dans la logique du prospectus pour les titres financiers (**titres II à IV** du règlement) ;
- il impose aux prestataires de services sur cryptoactifs (en anglais « *crypto-assets service providers* », CASP) un **agrément**, dont les exigences sont très proches de l'agrément PSAN prévu par la loi PACTE (**titre V** du règlement) ;
- il **interdit les opérations d'initiés et les manipulations de marché relatives à des cryptoactifs** (**titre VI** du règlement).

Bien que de nombreuses dispositions de MiCA soient proches de celles de la loi PACTE, le droit français devra être adapté pour mettre en cohérence les dispositions de droit interne avec le règlement européen, d'application directe. En particulier, les définitions des « actifs numériques » de la loi PACTE et des « cryptoactifs » du règlement MiCA diffèrent : MiCA distingue trois catégories de cryptoactifs, selon « *le fait que les crypto-actifs cherchent ou non à stabiliser leur valeur par référence à d'autres actifs* » (considérant 18 du règlement) :

- les cryptoactifs qui visent à stabiliser leur valeur en se référant à une seule monnaie officielle, communément appelés « *stablecoins* », assimilés à de la monnaie électronique (le règlement utilise le terme de « *electronic money tokens* », EMT) ;
- les jetons se référant à un ou à des actifs, « *qui visent à stabiliser leur valeur en se référant à une autre valeur ou à un autre droit, ou à une combinaison de ceux-ci, y compris une ou plusieurs monnaies officielles* » (le règlement utilise le terme de « *asset referenced tokens* », ART) ;
- les « autres cryptoactifs », incluant les cryptoactifs à usage commercial, objets de la présente mission.

L'article 9 de la loi n° 2023-171 du 9 mars 2023 portant diverses dispositions d'adaptation au droit de l'Union européenne habilite le Gouvernement à prendre, par voie d'ordonnance, avant le 8 mars 2024, toute mesure pour adapter les dispositions du CMF et, le cas échéant, d'autres codes ou lois pour assurer leur cohérence avec le règlement MiCA.

### 2.3.2. Le champ d'application du règlement MiCA soulève plusieurs difficultés, notamment en matière d'abus de marché

**L'entrée en application de MiCA posera des difficultés particulières en ce qui concerne les NFT. En effet, les NFT sont exclus du champ du règlement par son considérant 10[14] et son article 2, mais le critère de la non fongibilité n'est pas suffisant.**

Afin d'éviter un contournement de la réglementation, le texte a prévu la requalification possible de jetons techniquement non fongibles en jetons soumis au règlement MiCA : « *L'émission de crypto-actifs en tant que jetons non fongibles en grande série ou collection devrait être considérée comme un indicateur de leur fongibilité. La seule attribution d'un identifiant unique à un crypto-actif ne suffit pas en soi pour le classer comme unique et non fongible. Pour que le crypto-actif soit considéré comme unique et non fongible, il convient que les actifs ou les droits représentés soient également uniques et non fongibles. […] Le présent règlement devrait également s'appliquer aux crypto-actifs qui semblent être uniques et non fongibles, mais dont les caractéristiques de fait ou les caractéristiques qui sont liées à leurs utilisations de facto les rendraient soit fongibles, soit non uniques. À cet égard, lorsqu'elles évaluent et classent les crypto-actifs, les autorités compétentes devraient adopter une approche qui privilégie le fond par rapport à la forme, de sorte que les caractéristiques du crypto-actif en question déterminent le classement et non sa désignation par l'émetteur* ».

La définition exacte du périmètre d'application de MiCA aux NFT devra donc faire l'objet d'analyses au cas par cas et pourrait donner lieu à une certaine insécurité juridique dans les premiers temps. L'article 142 du règlement MiCA prévoit que la Commission présente un rapport « *sur les dernières évolutions intervenues en matière de crypto-actifs* », dont une « *évaluation de l'évolution des marchés de crypto-actifs uniques et non fongibles et du traitement réglementaire approprié de ces crypto-actifs, y compris une évaluation de la nécessité et de la faisabilité d'une réglementation applicable aux offreurs de crypto-actifs uniques et non fongibles ainsi qu'aux prestataires de services liés à ces crypto-actifs* ».

La volonté du législateur européen a été, par ce considérant, d'exclure les NFT de l'intégralité du règlement MiCA, qu'il s'agisse des dispositions relatives à l'émission des jetons ou aux prestataires de services sur crypoactifs. **Cependant, une ambiguïté demeure en raison de la qualité de cryptoactifs des NFT[15] et gagnerait à être levée dans une éventuelle révision ultérieure du texte.**

Les jetons utilitaires sont inclus dans le champ d'application du règlement MiCA mais sont exemptés de certaines obligations. Ainsi, le titre II (obligation de notification d'un livre blanc) ne leur est pas applicable et les dispositions sur les abus de marché ne leur sont que lorsqu'ils sont admis à la négociation.

*In fine*, de nombreuses formes de JVC ne relèvent pas, ou que partiellement, du règlement MiCA (*cf.* tableau 1).

---

[14] « *Le présent règlement ne devrait pas s'appliquer aux crypto-actifs qui sont uniques et non fongibles avec d'autres crypto-actifs, y compris l'art numérique et les objets de collection numériques.* »

[15] Les NFT n'étant pas exclus de la définition des cryptoactifs dans le texte du règlement MiCA, la question de l'applicabilité des dispositions relatives aux services liés aux NFT se pose. En effet, aucune disposition du titre V du règlement, traitant des prestations nécessitant un agrément (CASP), ne limite son champ d'application aux seuls cryptoactifs régis par MiCA. Ainsi l'échange de NFT – un cryptoactif au sens de MiCA, bien que hors champ du règlement – contre des cryptomonnaies devrait entrer dans le champ du titre V (cf. article 3 (16) du règlement).

**Tableau 1 : Applicabilité des différents titres du règlement MiCA aux jetons à vocation commerciale et aux services et opérations afférents (JVC)**

| Type de JVC | Titre II applicable à l'émission de ces jetons (livre blanc) | Titre V applicable aux prestataires de services sur ces jetons (agrément CASP) | Titre VI applicable aux transactions sur ces jetons (abus de marché) |
|---|---|---|---|
| JVC non fongibles (définis dans un sens économique) | Non | Non. Les services impliquant à la fois des JVC non fongibles et des JVC fongibles sont cependant soumis au titre V. | Non |
| Autres JVC utilitaires donnant accès à un bien existant ou à un service opérationnel (*utility tokens*) | Si et seulement s'ils sont admis à la négociation | Oui, exception faite des services de conservation et d'administration de ces jetons pour le compte de clients, et de transfert de cryptoactifs en lien avec ces jetons L'exception ne s'applique pas si les jetons sont admis à la négociation | Si et seulement s'ils sont admis à la négociation |
| Autres JVC relevant des exceptions *de minimis*[16] | Si et seulement s'ils sont admis à la négociation | Oui | Si et seulement s'ils sont admis à la négociation |
| Autres JVC fongibles[17] | Oui | Oui | Si et seulement s'ils sont admis à la négociation |

*Source : Mission, d'après le règlement MiCA adopté le 20 avril 2023.*

Cette situation est problématique, selon la mission, car les JVC présentent les mêmes risques, en matière d'abus de marché, que les jetons à vocation financière. En effet, les *blockchains* constituent des places de marché où les jetons sont cotés publiquement, en continu.

La mission recommande donc d'intégrer les jetons non fongibles dans le champ d'application du règlement MiCA et de leur appliquer le même régime que les jetons utilitaires (exclusion du titre II, application des règles sur les abus de marché).

**Proposition n° 4 : Lors de la révision prévue du règlement MiCA, étendre son champ d'application aux jetons non fongibles. Appliquer aux jetons non fongibles un régime identique à celui des *utility tokens*[18]. Préciser que la catégorie des *utility tokens* inclut les jetons qui constituent en eux-mêmes un bien ou un service déjà existant ou opérationnel (*cf.* annexe V).**

[16] Représentant moins de 1 M€ par an, acquis par moins de 150 personnes, réservés aux investisseurs qualifiés.

[17] Par exemple, grandes séries de *collectibles* ne donnant accès à aucun droit ou service.

[18] Pour rappel, les *utility tokens* sont soumis aux dispositions sur le livre blanc (titre II) et les abus de marchés (titre VI) à condition d'être admis à la négociation. Les prestataires de services sur ces jetons doivent par ailleurs obtenir l'agrément CASP (titre V).

**Une seconde question d'interprétation doit être résolue pour déterminer l'applicabilité du règlement MiCA aux plateformes d'échange de pair à pair**. En effet, la définition des plateformes de négociation (article 3 du règlement), similaire à celle retenue pour les marchés d'instruments financiers, semble incompatible avec le fonctionnement d'une plateforme de pair à pair, qui est pourtant l'architecture la plus répandue pour les plateformes de JVC, comme *OpenSea*. À moins que cette définition ne soit entendue de manière très extensive, de manière à y inclure les plateformes de pair à pair, les plateformes d'échange de JVC seraient exclues du périmètre de MiCA, si bien que les dispositions sur la lutte contre le blanchiment d'argent et le financement du terrorisme (LCB-FT) qui découlent de la qualification de CASP et sur les abus de marché ne trouveraient pas à s'appliquer[19].

**Pourtant, les risques que vise à prévenir le cadre réglementaire de MiCA sont aussi valables pour l'échange de JVC sur des plateformes de pair à pair** : ils peuvent avoir une forte dimension spéculative, susceptible de donner lieu à des manipulations de marché et à des opérations d'initiés. Contrairement aux instruments financiers, il n'est en effet pas nécessaire que les cryptoactifs soient échangés sur des marchés centralisés pour être liquides et avoir un cours. Par conséquent, la mission recommande d'appliquer les règles sur les abus de marché du titre VI de MiCA à tous les cryptoactifs, y compris ceux qui ne sont pas admis à négociation sur une plateforme centralisée, de sorte à inclure dans son champ les échanges sur plateformes de pair à pair.

**<u>Proposition n° 5</u> : Rendre applicables les interdictions du titre VI du règlement MiCA à l'ensemble des cryptoactifs, indépendamment du fait qu'ils soient ou non admis à la négociation sur une plateforme centralisée (*cf.* annexe V).**

Par ailleurs, des obligations pourraient être imposées aux plateformes d'échange de pair à pair, actuellement en dehors de MiCA, en matière de transparence, de loyauté, de vigilance en matière de LCB-FT et de prévention des abus de marché, pour compenser le fait qu'elles ne soient pas soumises à ces exigences via l'agrément de CASP. L'assujettissement des opérateurs de *layer 2*, en particulier de *rollups*, au régime CASP ou au régime que la mission propose de créer pour les autres plateformes dépendra de leurs caractéristiques techniques. Afin de renforcer la sécurité juridique des prestataires, la mission recommande que l'Autorité européenne des marchés financiers précise la délimitation exacte entre ces deux régimes.

**<u>Proposition n° 6</u> : Astreindre les plateformes de mise en relation des offreurs et acheteurs autres que les CASP à un régime allégé prévoyant des obligations de loyauté, de transparence, de diligence et de vigilance quant aux opérations à risque en matière de LCB-FT et de manipulations de marché (*cf.* annexe V).**

Afin de renforcer la lutte contre les abus de marché, la mission recommande par ailleurs d'interdire aux émetteurs de JVC de racheter sur leurs jetons sur le marché. En effet, le rachat par les émetteurs ne peut être justifié, dans le cas des JVC, par un souci de liquidité et fait peser un risque de manipulation du cours à la hausse en vue d'une prochaine émission.

**<u>Proposition n° 7</u> : Interdire aux émetteurs de jetons à vocation commerciale et à toute personne agissant de concert de procéder au rachat des jetons émis en monnaie *fiat* ou en cryptomonnaie grand public (bitcoin, éther, *etc.* – *cf.* annexe V).**

[19] Si ces plateformes exercent par ailleurs une activité de conservation de cryptoactifs soumis à MiCA, comme les cryptomonnaies, elles devront obtenir l'agrément CASP et seront donc soumises aux obligations en matière d'abus de marché et de lutte anti-blanchiment.

Par ailleurs, la mission relève que le titre VI du règlement MiCA ne prévoit pas d'obligation pour les personnes affiliées à un émetteur de jetons (actionnaires et personnes chargées de la direction de l'entreprise émettrice) de déclarer à l'émetteur et à l'AMF les transactions qu'elles réalisent sur ces jetons pour leur compte propre, contrairement à ce que prévoit le règlement sur les abus de marché pour les titres financiers.

**Proposition n° 8 : Étudier l'opportunité d'une obligation pour les dirigeants d'entités émettant des jetons de déclarer les opérations qu'ils effectuent pour leur compte propre sur ces jetons (*cf.* annexe V).**

## 2.4. Les risques en matière de blanchiment d'argent sont à l'origine d'un encadrement renforcé des cryptoactifs mais des failles demeurent

**Le développement des technologies de *blockchain* pose de nouveaux enjeux en matière de lutte contre le blanchiment d'argent et le financement du terrorisme (LCB-FT).** En effet, les *blockchains* permettent de réaliser des transferts de valeurs et des transactions de manière rapide et transfrontalière, sans passer par les établissements bancaires traditionnels, soumis à de fortes exigences de LCB-FT. Par ailleurs, les transactions sur *blockchain* sont, dans le cas de *blockchains* publiques, traçables et publiques, mais l'identité des parties ne l'est pas : les identifiants des détenteurs de *wallets* sont des pseudonymes, qu'il est difficile de rattacher à des personnes.

**Le développement d'innovations liées à la blockchain (*privacy coins*, mixeurs, *layers* 2, *rollups*, *etc.*)[20] renforce, en outre, la capacité d'anonymisation des transactions**, rendant le travail d'enquête encore plus difficile, voire impossible. Par ailleurs, plus l'écosystème *blockchain* se développe, plus le risque de blanchiment croît car les sorties du monde « crypto », qui constituent des points de contrôle, sont de moins en moins nécessaires : si un criminel peut se procurer ce dont il a besoin dans le monde virtuel, grâce à des cryptomonnaies, alors le simple fait de se reposer sur les contrôles opérés lors des conversions entre cryptomonnaies et numéraire ne suffit plus.

**C'est pourquoi l'instauration d'un cadre de LCB-FT applicable aux cryptoactifs est nécessaire**. L'article 76(3) du règlement MiCA interdit aux plateformes de négociation de crypto-actifs d'admettre les jetons comportant des fonctions d'anonymisation intégrées (*privacy coin*), à moins que les détenteurs de ces cryptoactifs et leur historique de transactions ne puissent être identifiés par les CASP qui exploitent la plateforme.

Par ailleurs, le 20 juillet 2021, la Commission européenne a soumis un ensemble de quatre propositions législatives[21] relatives à la LCB-FT, incluant des enjeux liés à l'utilisation de cryptoactifs dans les opérations de blanchiment. À la date de rédaction du présent rapport, l'examen des propositions de textes par le Parlement européen est en cours.

Ces propositions ont pour principaux effets de :

- qualifier les CASP régis par le règlement MiCA d'entités assujetties au titre de la LCB-FT ;
- étendre aux transferts de cryptoactifs fongibles la « *travel rule* », c'est-à-dire l'**obligation pour les prestataires de services sur cryptoactifs de collecter puis d'échanger certaines informations sur les transferts qu'ils réalisent.**

[20] *Cf.* section 4 de l'annexe I et section 2.1 de l'annexe V pour l'explication de ces innovations techniques.

[21] Paquet composé d'une sixième directive « AMLD » (*anti-money laundering directive*), et de trois règlements dont le règlement instituant une agence européenne de lutte anti-blanchiment.

Ces différents textes ont ainsi bâti un cadre de régulation en matière de LCB-FT qui repose notamment sur les CASP. Pris dans leur ensemble, ils visent à instaurer au sein de l'environnement *blockchain* une délimitation entre un système régulé, dans lequel les transactions peuvent être tracées et leurs auteurs identifiés, et un système non régulé ne présentant pas ces garanties.

Trois problèmes demeurent non résolus à ce stade, et devraient susciter des réflexions en vue d'une révision future des textes européens :

- les plateformes d'échange de pair à pair n'étant pas soumises à MiCA (*cf.* 2.3.2), elles échappent à ces règles de LCB-FT, d'où l'intérêt d'intégrer des obligations en matière de LCB-FT dans le régime *ad hoc* que la mission recommande (*cf.* proposition n° 6) ;
- de même, les prestataires de service n'opérant que sur des jetons non fongibles au sens du règlement MiCA ne sont soumis à aucune obligation : l'inclusion des NFT dans le champ de MiCA (*cf.* proposition n° 4) doit remédier à ce problème ;
- les portefeuilles non hébergés par un CASP, dits « autohébergés », constituent des points de fuite potentiels, dans la mesure où ils ne sont pas contrôlés par des CASP.

Malgré ce nouveau cadre réglementaire, il reste relativement aisé, pour une personne détenant des fonds d'origine illicite, de les transférer entre un portefeuille hébergé par un CASP et un portefeuille autohébergé, à la suite de quoi les personnes physiques qui manipulent les flux ne peuvent plus être identifiées facilement et des services de brouillage peuvent être utilisés.

Afin de retracer plus facilement les flux entre l'univers régulé et l'univers non régulé, la mission recommande donc de rendre obligatoire la vérification de l'identité du détenteur du portefeuille autohébergé pour les transferts supérieurs à 1 000 €[22] avec un CASP ou ayant un caractère professionnel. La vérification de l'identité des détenteurs pourrait passer par des services d'identité numérique (*cf.* annexe III).

**<u>Proposition n° 9.A</u> : Étendre la *travel rule* aux cryptoactifs non fongibles[23] et aux transferts réalisés par le *Lightning Network*. Rendre obligatoire la vérification de l'identité du détenteur d'un portefeuille autohébergé pour un paiement supérieur à 1 000 € réalisé vers ou depuis un CASP ou ayant un caractère professionnel. Cette vérification d'identité pourrait être déléguée à un prestataire de service de confiance garantissant que le détenteur du portefeuille est identifié (*cf.* annexe V).**

Cette mesure ne permettrait néanmoins pas de remédier à tous les problèmes de blanchiment que posent les *blockchains*, car les flux entre portefeuilles autohébergés demeurent intraçables. Le caractère numérique, donc mobile et immatériel, des cryptoactifs les rend encore plus propices au blanchiment et pourrait justifier un traitement plus strict, si les mesures précédentes étaient considérées comme insuffisantes. Dans un tel cas, la mission propose d'étudier une interdiction de tout transfert de plus de 1 000 € entre un portefeuille hébergé par un CASP et un portefeuille autohébergé, rendant la frontière entre les univers régulé et non régulé encore plus étanche.

[22] Par parallélisme avec les articles L. 112-6 et D. 112-3 du CMF, qui interdisent les règlements supérieurs à 1 000 € en espèces.

[23] L'inclusion des jetons non fongibles dans le champ d'application de MiCA, recommandée par la mission en proposition n° 1, aura pour conséquence de leur appliquer aussi la *travel rule*, puisque leur exclusion du règlement sur les transferts est assise sur une référence à l'article de MiCA qui exclut les jetons non fongibles, lequel serait supprimé. Pour une meilleure légistique, une modification du règlement sur les transferts est néanmoins souhaitable.

Afin d'éviter un mouvement de concentration du marché autour des CASP (puisque seuls ces acteurs réaliseront, dans l'état actuel du droit, des contrôles de LCB-FT), cette recommandation devrait être accompagnée de la création d'un statut *ad hoc* pour des prestataires d'ouverture et d'hébergement de portefeuilles, sans conservation, permettant d'assimiler ceux-ci à des CASP, mais imposant des obligations allégées.

**<u>Proposition n° 9.B</u> : Si la proposition n° 9.A est jugée insuffisante en matière de LCB-FT, envisager d'interdire aux CASP de réaliser ou d'accepter des transactions de cryptoactifs depuis ou vers un portefeuille autohébergé pour un montant supérieur à 1 000 €. Pour l'application de cette règle, créer un statut pour les hébergeurs de portefeuille sans conservation (*non-custodial hosted wallets*) assimilé à celui des CASP (*cf.* annexe V).**

# 3. La France possède un écosystème « crypto » dynamique, leader dans l'Union européenne mais pas dans le monde

## 3.1. L'écosystème français, porté par deux « licornes », dispose de forts atouts mais demeure embryonnaire

L'écosystème crypto français compte plusieurs dizaines de startups, liées à des cas d'usage variés (*cf.* 1.1) : jeux, arts graphiques, musique, identité numérique, passeport numérique produit, finance décentralisée, infrastructure *blockchain*, *etc.* Les recensements dont la mission a eu connaissance donnent des nombres concordants : BPI France compte, au 1er avril 2023, 111 sociétés du secteur Web 3.0 ayant déjà levé des fonds (pour 2,2 Md€), tandis que la base de données *Dealroom* recense 80 sociétés en France associées au Web 3.0.

**L'écosystème est porté par deux « licornes », qui donnent à l'ensemble du secteur une visibilité plus importante : Ledger, qui commercialise des solutions de *wallets* sécurisés, et Sorare, une société de jeu sportif reposant sur des NFT.** D'autres projets connaissent une forte croissance et pourraient étoffer le nombre de succès de l'écosystème français, comme Kaiko (analyse de données sur blockchain), Coinhouse (plateforme d'échange) ou Morpho Labs (finance décentralisée).

La France possède des atouts majeurs qui forment un terrain propice au développement du secteur crypto :

- la **qualité des ingénieurs et des chercheurs** formés en France et leurs compétences en informatique et en cryptographie ;
- la **présence de grandes entités capables d'utiliser les solutions *blockchain*** et de porter un cas d'usage (leaders du luxe et du jeu vidéo, institutions culturelles de renommée mondiale) ;
- un **cadre réglementaire clair, établi par la loi PACTE, qui a l'avantage de réduire l'insécurité juridique** (en comparaison avec les États-Unis et le Royaume-Uni, notamment) et de préparer en avance[24] les acteurs économiques aux exigences du cadre européen, posées par le règlement MiCA et proches du cadre français. La mise au point du cadre règlementaire français a supposé une acculturation des parties prenantes (ministère de l'économie et de finances, et surtout Autorité des marchés financiers) qui a été saluée par les interlocuteurs de la mission : la maturité du régulateur sur le sujet est appréciée car elle constitue une garantie, pour les acteurs économiques, de voir les dossiers traités et les enjeux propres au secteur, compris.

[24] Un prestataire de services sur actifs numériques exerçant son activité en conformité avec le droit interne d'un État membre avant l'entrée en application du règlement MiCA bénéficie de 18 mois de plus pour se mettre en

Le dynamisme de l'écosystème français se traduit par le développement de prestataires de services liés à ce secteur (services de conseil, avocats, notamment), par l'engagement croissant de fonds d'investissement français sur des projets crypto et par l'installation, en France, d'acteurs étrangers (comme Binance, Crypto.com ou Circle). Les acteurs se sont structurés autour de deux fédérations professionnelles : l'Association pour le développement des actifs numériques (ADAN) et la Fédération française des professionnels de la *blockchain* (FFPB). Par ailleurs, Paris accueille deux événements annuels d'envergure mondiale pour le secteur : *NFT Paris* qui a attiré plus de 10 000 visiteurs en février 2023, et *Paris Blockchain Week*, qui a accueilli 8 500 visiteurs en mars 2023.

**Les forces, réelles, de l'écosystème français, ne doivent pas laisser penser que la France est le pays le plus avancé dans ce secteur en Europe. L'écosystème européen est dominé par la Suisse et le Royaume-Uni, très présents dans le développement de l'infrastructure du Web 3.0 et la finance décentralisée. La France se situe à un niveau comparable à l'Allemagne, notamment en matière de nombre de startups ayant levé des fonds (environ 110).** En France, seules 13 startups ont dépassé le stade du « *seed* », hors *Sorare* et *Ledger* : le dynamisme du secteur ne doit pas faire oublier qu'il est encore jeune et de taille modeste.

## 3.2. Deux obstacles freinent le développement de l'écosystème français crypto

Les échanges avec les acteurs économiques rencontrés par la mission ont permis d'identifier deux points bloquants, qui constituent une barrière pour le développement de l'écosystème français.

**En premier lieu, les sociétés du secteur lié aux *blockchains* et aux cryptoactifs relatent de grandes difficultés à ouvrir des comptes bancaires pour la gestion de l'entreprise, auprès des établissements bancaires traditionnels**[25]. Elles tiennent, d'après eux, à un refus des banques expliqué par les craintes de celles-ci en matière de lutte contre le blanchiment et le financement du terrorisme (LCB-FT). Le deuxième alinéa de l'article L. 312-23 du CMF vise à garantir l'accès aux comptes bancaires mais ne couvre que les PSAN enregistrés ou agréés. En revanche, les sociétés qui ne relèvent pas du régime des PSAN, par exemple celles dont l'activité porte sur les infrastructures techniques ou celles qui opèrent sur des jetons ne constituant pas des actifs numériques au sens du droit français, ne bénéficient pas de ces dispositions. Des entretiens menés par la mission, il ressort que celles-ci, pour pouvoir obtenir l'ouverture d'un compte bancaire, sont contraintes de ne pas révéler leur secteur d'activité exact. L'approfondissement des exigences en matière de LCB-FT au sujet des cryptoactifs, en cours de négociation à l'échelle européenne (*cf.* section 2.4), devrait être l'occasion de traiter cette barrière, en échangeant avec les régulateurs (AMF, Autorité de contrôle prudentiel et de résolution) et le secteur bancaire, représenté par la Fédération bancaire française[26].

**<u>Proposition n° 10</u> : Renouveler le dialogue entre régulateurs et secteur bancaire afin de garantir l'accès des entreprises du Web 3.0 à un compte bancaire (*cf.* annexe VII).**

conformité avec le régime de prestataire de services sur cryptoactifs (CASP), qui entre lui-même en application 18 mois après l'entrée en vigueur du règlement.

[25] Ce problème avait déjà été identifié par le rapport de France Stratégie, « Les enjeux des *blockchains* » (juin 2018).

[26] Un groupe de travail réunissant l'AMF et l'ACPR sur l'application des règles de LCBFT aux cryptoactifs avait rendu un rapport en octobre 2020, sans apporter de solution à ce problème.

**En second lieu, le financement de l'écosystème par des fonds français souffre d'une difficulté, pour eux, à investir en jetons, pratique pourtant très courante dans les modèles de financement du secteur.** Les startups du secteur ont pour habitude de lever des fonds à la fois par le biais de l'ouverture de leur capital (« *equity* ») et par l'émission de jetons (« *tokens* ») qui peuvent par la suite donner des droits de gouvernance à leurs détenteurs ou capter une part de la valeur créée en étant échangés sur des plateformes et en permettant aux investisseurs de dégager des plus-values.

Pour pouvoir investir dans ces jetons, les fonds de capital-risque gérés par des sociétés de gestion de portefeuille (SGP) agréées par l'AMF doivent soumettre à cette dernière une modification de leur programme d'activité. Plusieurs demandes de cette nature sont en cours d'examen.

Une difficulté supplémentaire freine le financement en jetons : la mission de conservation est, dans le cas des jetons, disjointe de celle de dépositaire. En effet, la conservation des clefs privées du portefeuille de la SGP est confiée à un prestataire spécialisé, mais le dépositaire demeure responsable et doit donc, en concertation avec l'AMF, expertiser les dispositifs de conservation de clés qui présentent des caractéristiques techniques inédites afin de s'assurer de leur sécurité et de leur conformité. Cette situation est source de risques pour le dépositaire, si bien que les entités prêtes à offrir ce service sont très peu nombreuses. Par ailleurs, les principaux prestataires de conservation (Fireblocks, Taurus, Metaco) sont situés en dehors de l'Union européenne, ce qui complique l'application de la règlementation et pose des problèmes de souveraineté.

**<u>Proposition n° 11</u> : Encourager l'émergence d'une solution de conservation française afin de faciliter l'investissement en jetons et de gagner en souveraineté. Une telle mission pourrait être confiée à la Caisse des dépôts et des consignations, qui a développé une expertise en la matière (*cf.* annexe VII).**

# CONCLUSION

Outre leur utilisation financière, les *blockchains* publiques et les cryptoactifs dont elles sont le support ont trouvé des cas d'usage commerciaux auprès du grand public dans trois principaux secteurs : les jeux vidéo, l'art et le luxe. Dans chacun de ces domaines, leur développement est porté par une même vision consistant à rendre le consommateur « *propriétaire* » de biens virtuels ou de données inscrits sur un registre décentralisé, principe qui se trouve au fondement du Web 3.0. La présence en France de deux « licornes » du Web 3.0 ainsi que d'entreprises traditionnelles d'envergure internationale dans chacun des trois secteurs, l'adoption d'un cadre réglementaire spécifique depuis 2019, le haut niveau de la recherche fondamentale en informatique et la formation des ingénieurs constituent des atouts pour l'écosystème national, qui se trouve en pointe à l'échelle de l'Union européenne.

Si les pouvoirs publics souhaitent favoriser le développement des JVC dans l'économie française, maîtriser les risques associés à ce développement et éviter des distorsions de concurrence par rapport à d'autres acteurs et d'autres technologies, plusieurs problématiques juridiques doivent être traitées. **Une telle initiative suppose de nombreuses modifications du droit et un important effort de coordination entre les différents acteurs concernés au sein de la sphère publique afin d'aboutir à des résultats cohérents** : les *blockchains* et les jetons soulèvent des enjeux multiples qui nécessitent une analyse d'ensemble. La mission émet des recommandations qui touchent à la fois à la protection des consommateurs (dans le périmètre de la DGCCRF), à la régulation financière (DGT et AMF), à la lutte anti-blanchiment (ACPR, TRACFIN), à la fiscalité (DLF), aux données personnelles (CNIL), à la valeur probatoire des *blockchains* (DACS). **Cette exigence de coordination est d'autant plus nécessaire que l'écosystème des *blockchains* et des JVC est concerné par plusieurs législations européennes en cours de négociation ou d'adoption** : règlement MiCA, règlement sur le transfert de fonds, règlement sur les données (*Data Act*), règlement sur l'écoconception.

**La construction d'un cadre réglementaire plus complet pour les *blockchains* et les JVC devrait s'inspirer de la méthode utilisée lors de l'élaboration de la loi PACTE**, associant, dans une logique de concertation, l'administration, les régulateurs (en l'espèce, l'AMF et l'ACPR mais d'autres régulateurs sectoriels peuvent être concernés par les JVC, comme le cas des jeux d'argent l'a montré avec l'ANJ) et les acteurs économiques. La rapidité d'évolution de l'écosystème *blockchain* suppose, enfin, d'accepter que le cadre réglementaire doit tenir compte.

À Paris, le 30 mai 2023

Les membres de la mission,

L'inspecteur des finances,

Ivan Salin

L'inspecteur des finances adjoint,

Valentin Melot

Sous la supervision de
l'inspecteur général des finances,

Marc Auberger

# LISTE DES PROPOSITIONS

**Droits et obligations associés aux jetons (*cf.* annexe IV)**

Proposition n° 1 : Rendre obligatoire l'association à tout jeton à vocation commerciale émis ou/et échangé dans l'Union européenne d'un document contractuel définissant les droits et obligations incorporés comme sous-jacent dont bénéficie le porteur du jeton.

Proposition n° 2 : Confirmer la compatibilité des dispositions du CPI relatives aux cessions de droit d'auteur (article L. 132-7) avec une licence de cession de droits à une personne identifiée par la détention d'un jeton, et envisager une modification de ces articles dans le seul cas où une incompatibilité serait identifiée. Fournir un modèle de contrat de licence qui pourrait être utilisé par les acteurs économiques.

**Fiscalité des jetons (*cf.* annexe VI)**

Proposition n° 3 : Appliquer aux plus-values réalisées sur jetons utilitaires le régime fiscal de leur sous-jacent, c'est-à-dire celui des biens meubles, et non le régime prévu pour les actifs numériques par l'article 150 VH bis du CGI.

**Champ d'application du règlement MiCA (*cf.* annexe V)**

Proposition n° 4 : Lors de la révision prévue du règlement MiCA, étendre son champ d'application aux jetons non fongibles. Appliquer aux jetons non fongibles un régime identique à celui des *utility tokens*. Préciser que la catégorie des *utility tokens* inclut les jetons qui constituent en eux-mêmes un bien ou un service déjà existant ou opérationnel.

**Lutte contre les abus de marché (*cf.* annexe V)**

Proposition n° 5 : Rendre applicables les interdictions du titre VI du règlement MiCA à l'ensemble des cryptoactifs, indépendamment du fait qu'ils soient ou non admis à la négociation sur une plateforme centralisée.

Proposition n° 6 : Astreindre les plateformes de mise en relation des offreurs et acheteurs autres que les CASP à un régime allégé prévoyant des obligations de loyauté, de transparence, de diligence et de vigilance quant aux opérations à risque en matière de LCB-FT et de manipulations de marché.

Proposition n° 7 : Interdire aux émetteurs de jetons à vocation commerciale et à toute personne agissant de concert de procéder au rachat des jetons émis en monnaie *fiat* ou en cryptomonnaie grand public (bitcoin, éther, *etc.*).

Proposition n° 8 : Étudier l'opportunité d'une obligation pour les dirigeants d'entités émettant des jetons de déclarer les opérations qu'ils effectuent pour leur compte propre sur ces jetons.

**Lutte contre le blanchiment de capitaux et le financement du terrorisme (*cf.* annexe V)**

Proposition n° 9.A : Étendre la *travel rule* aux cryptoactifs non fongibles et aux transferts réalisés par le *Lightning Network*. Rendre obligatoire la vérification de l'identité du détenteur d'un portefeuille autohébergé pour un paiement supérieur à 1 000 € réalisé vers ou depuis un CASP ou ayant un caractère professionnel. Cette vérification d'identité pourrait être déléguée à un prestataire de service de confiance garantissant que le détenteur du portefeuille est identifié.

Proposition n° 9.B : Si la proposition n° 9.A est jugée insuffisante en matière de LCB-FT, envisager d'interdire aux CASP de réaliser ou d'accepter des transactions de cryptoactifs depuis ou vers un portefeuille autohébergé pour un montant supérieur à 1 000 €. Pour l'application de cette règle, créer un statut pour les hébergeurs de portefeuille sans conservation (*non-custodial hosted wallets*) assimilé à celui des CASP.

**Écosystème (*cf.* annexe VII)**

Proposition n° 10 : Renouveler le dialogue entre régulateurs et secteur bancaire afin de garantir l'accès des entreprises du Web 3.0 à un compte bancaire.

Proposition n° 11 : Encourager l'émergence d'une solution de conservation française afin de faciliter l'investissement en jetons et de gagner en souveraineté. Une telle mission pourrait être confiée à la Caisse des dépôts et des consignations, qui a développé une expertise en la matière.

# ANNEXES ET PIÈCE JOINTE

# LISTE DES ANNEXES ET DE LA PIÈCE JOINTE

# ANNEXE I

# Principes de fonctionnement des *blockchains* et conséquences de la décentralisation

**Annexe I**

# SYNTHÈSE

**Inventées pour le projet de monnaie numérique décentralisée *Bitcoin*, les *blockchains* sont des infrastructures permettant de maintenir un registre de données distribué en ligne** dans lequel la lecture et l'écriture obéissent à des règles strictes : interdiction de dépenser des fonds que l'on ne détient pas, authentification des ordres de virement, maîtrise stricte du processus d'émission monétaire, *etc.*

**Alors que les systèmes en réseau traditionnels reposent, pour vérifier que les règles sont respectées, sur des tiers de confiance (banque, notaire, État, *etc.*), les *blockchains* sont conçues pour permettre de créer cette confiance *ex nihilo*** : l'utilisateur n'a pas besoin de présupposer que les participants au réseau sont dignes de confiance, ni même de connaître leur identité[1]. Cette propriété est atteinte grâce à un *protocole de consensus*, c'est-à-dire une méthode permettant aux validateurs de se mettre spontanément d'accord sur une liste de transactions jugées valides. Un système de vote à la majorité ne constituerait pas une solution à ce problème, car il serait trop facile pour un fraudeur de créer de faux votants et d'emporter la majorité. La *preuve de travail* constitue la première solution proposée et fonde *Bitcoin* : chaque validateur doit accomplir un certain travail (résolution d'énigmes cryptographiques complexes) et son poids est proportionné au volume du travail qu'il peut réaliser. La *preuve d'enjeu*, autre solution possible adoptée par la chaîne *Ethereum*, pondère les votes par la quantité de cryptomonnaie que le validateur est prêt à mettre sous séquestre comme garantie de sa bonne foi, jusqu'à ce son honnêteté ait été confirmée par ses pairs. Dans chacun des deux cas, une tentative de fraude (validation de transactions illicites) suppose un bourrage d'urnes, rendu artificiellement coûteux puisqu'il suppose de résoudre plus d'énigmes ou d'être prêt à séquestrer plus de cryptomonnaie que tous les validateurs honnêtes réunis.

Néanmoins, cette création *ex nihilo* de consensus se fait au prix d'une consommation élevée de ressources — en particulier, consommation électrique pour *Bitcoin*. Cette consommation est le coût d'une décentralisation en principe totale : les promoteurs du projet, d'inspiration libertarienne, estiment toutefois qu'elle est justifiée pour permettre de construire une économie ne reposant pas sur les États ni sur les banques centrales.

**La *blockchain Ethereum* innove par rapport à *Bitcoin* en ce qu'elle offre aux utilisateurs la possibilité de rendre le registre *programmable*.** Le registre ne sert plus uniquement à lister des transactions dans l'unité monétaire de la *blockchain*, mais peut accueillir des inscriptions arbitrairement complexes, dont les règles sont définies par des programmes autonomes — improprement appelés *smart contracts*. Ces derniers permettent par exemple de stocker dans le registre n'importe quel type de données, de procéder à des opérations financières complexes ou encore de créer un sous-registre de « jetons négociables » et divers types de « cryptoactifs ». Les cas d'usage de ces jetons et les enjeux juridiques associés sont développés dans les annexes II à VI.

[1] Cette idée est au cœur du projet *Bitcoin*, pensé par son créateur mythique, Satoshi Nakamoto, comme alternative à la monnaie étatique (« monnaie *fiat* ») en raison de la faible confiance qu'inspirent le système bancaire et la banque centrale dans leur gestion de cette monnaie. Le livre blanc à l'origine de *Bitcoin* a été publié le 31 octobre 2008, en pleine crise financière mondiale.

**Alors que les promoteurs des *blockchains* et des cryptoactifs présentent ceux-ci comme un moyen de décentraliser l'internet, cette promesse est contestable.**

En effet, d'une part, la décentralisation a un coût inhérent : consommation accrue de ressources (une consommation électrique instantanée pour le réseau *Bitcoin* de l'ordre de 15 GW[2], soit la puissance de dix réacteurs nucléaires EPR), coûts de transaction en résultant, complexité du système, impossibilité d'annuler des transactions erronées, impossibilité de forcer l'application de normes d'ordre public, difficulté à lutter contre les infractions, divulgation de données personnelles.

Or, il apparaît en pratique que **la majorité des applications commerciales des *blockchains* ne nécessitent pas que la validation du registre soit décentralisée, ce qui rend superfétatoires les coûts associés à la décentralisation**. Ceci découle en particulier du fait qu'il existe, pour la plupart de ces applications, des points critiques de confiance, c'est-à-dire des acteurs en lesquels il est indispensable d'avoir confiance en dernier ressort : créancier lorsqu'un jeton représente un titre de créance, état civil lorsque le registre traite des données d'identité, système judiciaire pour forcer l'exécution des créances ou le règlement des litiges, *etc.* Le fait d'inscrire les transactions dans une *blockchain* ne permet donc pas de se passer totalement de tiers de confiance, lesquels pourraient aussi assurer la tenue du registre puisqu'ils ont reçu la confiance des utilisateurs.

D'autre part, l'idéal de décentralisation totale se heurte en pratique à des contraintes opérationnelles :

- l'impossibilité, dans un système totalement décentralisé, de garantir un haut niveau de sécurité tout en se développant à grande échelle. Par exemple, *Bitcoin*, qui garantit un niveau élevé de sécurité, ne peut traiter que sept transactions par seconde au maximum. La croissance repose donc sur l'utilisation de surcouches techniques (« *layer 2* »), plus centralisées ou moins sécurisées que la chaîne principale ;
- la recentralisation de certaines étapes de la validation de transactions. En effet, les acteurs sont économiquement incités à mettre en commun certaines ressources pour éviter les duplications et réduire la variance des gains. En conséquence, en février 2023, le réseau *Bitcoin* est contrôlé à plus de 80 % par cinq coopératives (*pools*) de validateurs.

**L'interopérabilité des *blockchains* et l'effet de mode associé paraissent donc davantage expliquer le succès de cette technologie que ses fonctionnalités techniques.** Ainsi, exception faite de *Bitcoin*, toujours développé dans la perspective de créer une monnaie purement décentralisée et indissociable du protocole de création de confiance associé, l'utilité de l'innovation que constituent les *blockchains* par rapport à des bases de données centralisées mais rendues interopérables reste débattue et leur potentiel réel est aujourd'hui incertain.

[2] Estimation au 28 mars 2023 calculée par le modèle *Cambridge Bitcoin Electricity Consumption Index*, réalisé par le *Cambridge Centre for Alternative Finance* de l'université de Cambridge (https://ccaf.io/cbeci/index).

# SOMMAIRE

L'objet de la présente annexe est d'introduire les notions nécessaires à la compréhension technique des problématiques associées aux *blockchains* et aux différents types de jetons, parmi lesquels les jetons non fongibles.

La première partie présente des notions fondamentales d'informatique et de cryptographie utilisées dans l'ensemble du document, qui constituent un prérequis indispensable pour le lecteur non informaticien. La deuxième partie vise à présenter le concept général de *blockchain*, en se concentrant sur le fonctionnement de la *blockchain Bitcoin*. La troisième partie expose comment les *blockchains* peuvent être utilisées pour émettre des « jetons », fongibles ou non. Une étude plus détaillée du fonctionnement technique des jetons, au cœur de la mission, est proposée en annexe II. Enfin, la dernière partie s'intéresse à la problématique de la centralisation, de la sécurité et du passage à l'échelle de ces technologies ainsi qu'aux choix stratégiques qui se posent au sujet de leur développement.

# 1. Les technologies de l'univers *blockchain* reposent principalement sur deux outils mathématiques, que sont les fonctions de hachage et la cryptographie asymétrique

## 1.1. Bits, octets, hexadécimal et représentation de données informatiques

L'ensemble des données informatiques sont représentées sous une forme binaire, c'est-à-dire une succession de *zéros* et de *uns*, dans la mémoire des ordinateurs qui les traitent. Un **bit** (de l'anglais *binary unit*, unité binaire) est une donnée atomique, la plus petite possible, c'est-à-dire soit un 0, soit un 1.

De nombreuses conventions permettent de définir de quelle façon des données (textes, sons, images, vidéos, bases de données…) sont représentées sous la forme d'une suite de *bits*. Par exemple, la norme UTF-8 définit une façon de représenter du texte, parmi les plus fréquemment utilisées à cette fin en 2023 : la lettre minuscule ***a*** est représentée par la suite de huit bits **01100001**. La lettre majuscule accentuée ***É*** est représentée par la suite plus longue de seize bits **1100001110101001**. Différents standards permettent de représenter des couleurs (le système RVB), des images (par exemple les formats PNG et JPEG), des sons (MP3, OGG…), des vidéos (MP4), *etc.* ou encore de savoir quelle norme appliquer dans un contexte. Certaines suites de bits peuvent ne correspondre à aucune donnée dans une norme donnée : par exemple, dans la norme UTF-8, la suite **10010101** prise isolément ne représente aucun caractère autorisé.

Pour des raisons techniques, les bits sont le plus souvent traités par groupe de huit : huit bits définissent un octet. Un octet peut prendre $2^8 = 256$ valeurs différentes. Le nombre de données différentes qui peuvent être représentées croit exponentiellement avec le nombre de bits (ou d'octets) qui sont utilisés. Par exemple, avec un octet, il est possible de représenter 256 valeurs différentes, avec trois octets, 16,8 millions de valeurs différentes et avec 256 bits (32 octets), environ $10^{177}$ (un *un* suivi de 177 *zéros*) octets.

Pour des questions de lisibilité, il est fréquent de représenter les données par des suites de groupes de quatre bits. Les groupes possibles (0000, 0001, 0010, 0011, *etc.* jusqu'à 1101, 1110 et 1111), au nombre de seize, peuvent être représentés par les dix chiffres (de **0** à **9**) auxquels sont ajoutés six lettres, de **a** à **f**. Cette représentation est appelée la **représentation hexadécimale des données**. Il est fréquent, pour éviter toute ambiguïté, d'utiliser le symbole « 0x » pour indiquer que ce qui suit doit être compris comme de l'hexadécimal. Par exemple, la chaîne **0xc3a9** désigne selon cette convention la suite de deux octets (ou seize bits) **1100 0011 1010 1001**, qui elle-même représente selon la norme UTF-8 le texte « *é* ».

D'autres représentations que l'hexadécimal utilisant plus de caractères restent toutefois possibles.

## 1.2. Fonctions de hachage cryptographiques (*hash*) de données

### 1.2.1. Propriétés et utilité des fonctions de hachage cryptographique

Le **hachage** de données informatiques (en anglais *hash*) est une opération indispensable au bon fonctionnement de la plupart des traitements de données qui seront décrits par la suite. Une **fonction de hachage cryptographique** est une transformation mathématique prenant en entrée n'importe quelle donnée (sous la forme d'une suite de bits, *cf.* 1.1) et renvoyant en sortie une suite de bits de taille fixe, appelée **empreinte**, condensat ou ***hash***. Cette transformation a plusieurs propriétés :

- elle est déterministe : les mêmes entrées produisent de façon certaine les mêmes sorties ;
- elle est publique : toute personne peut donc retrouver la sortie à partir des données d'entrée si la fonction utilisée est précisée ;
- elle ne peut en pratique pas être inversée. Plus précisément, il n'est pas possible de retrouver l'entrée, même de façon approximative, à partir du *hash*. Pour atteindre ce résultat, la fonction a un « *effet avalanche* » : une perturbation infinitésimale en entrée donne lieu à une modification complète et imprévisible du résultat. Le résultat donne donc une illusion d'aléa, ce qui est essentiel pour les applications cryptographiques.

Il existe de nombreuses fonctions de hachage cryptographiques grand public. La suite de cette section se concentrera sur celle qui est utilisée pour la construction de la *blockchain Bitcoin* : **SHA256**. Cette fonction produit des *hashes* de 256 bits, c'est-à-dire de 32 octets. Le tableau 1 illustre l'« *effet avalanche* » en appliquant cette fonction à quelques données textuelles légèrement modifiées en entrée (changement de casse, ajout d'une lettre).

**Tableau 1 : Application de la fonction de hachage SHA256 à quelques textes similaires**

| Texte d'entrée | *Hash* SHA256 du texte d'entrée[3] (représenté en hexadécimal) |
|---|---|
| *Cryptographie* | `0073e8c7fe96e38eda71395f43511288c7b76108d45590a6f5570e4a5994f3d6` |
| *cryptographie* | `36f618abc7627af6b99f4189f45ccee95a0a80c9f3c088024820ec0ea153096e` |
| *Cryptographique* | `672ee2c9914a98984ee8db07875e15e7a971c5ce02feb6479b6fe77a3898e2d5` |

*Source : Mission, par l'utilisation du module* hashlib *de Python 3.*

Ces fonctions comportent de très nombreuses applications, parmi lesquelles[4] :

- la vérification de l'intégrité de données. Si un utilisateur dispose d'une copie d'un document et souhaite vérifier qu'il n'a pas été altéré, il lui suffit de calculer le *hash* du document (un document informatique étant toujours constitué d'une suite de bits) et de le comparer au *hash* de l'original. Une altération mineure, même d'un seul bit, est immédiatement détectable ;

[3] Formellement, le hachage est appliqué à la représentation UTF-8 du texte d'entrée, c'est-à-dire à la suite de bits associée.

[4] Les trois applications présentées sont en réalité assez simplifiées et comporteraient, si elles étaient mises en œuvre « naïvement », des failles de sécurité importantes. L'explication de ces failles et des moyens de les éviter est au-delà du champ de ce rapport et n'est pas nécessaire à la compréhension d'ensemble.

- le stockage de mots de passe. Le propriétaire d'un site internet, plutôt que de stocker les mots de passe de ses utilisateurs, préférera stocker leur *hash* : ce faisant, en cas de fuite de données, les mots de passe ne sont pas révélés. Lors de la connexion, l'utilisateur saisit son mot de passe ; le *hash* du mot de passe est calculé et le mot de passe est instantanément détruit. Il suffit de comparer que le *hash* du mot de passe communiqué correspond à celui stocké pour autoriser la connexion ;
- la preuve de détention d'un document. Supposons qu'Alice[5] détienne un manuscrit le 1er janvier qu'elle ne révélera au public que le 1er février, mais qu'elle veuille prouver qu'elle disposait déjà de ce manuscrit le 1er janvier. Il lui suffit de publier, le 1er janvier, le *hash* du document. Le 1er février, lorsqu'elle publiera le manuscrit, toute personne pourra calculer le *hash* et constater qu'il coïncide avec ce qu'avait annoncé Alice un mois plus tôt.

Ces applications comportent des enjeux de preuve d'identité, de conformité ou de droits, si bien que des personnes mal intentionnées pourraient avoir intérêt à les attaquer. La robustesse des protocoles décrits ci-dessus repose en grande partie sur le fait qu'**il est impossible, en théorie comme en pratique, de retrouver les données d'origine à partir du *hash***. Dans le deuxième exemple, si une attaquante Ève[5] pouvait « *inverser* » l'opération de hachage, alors elle pourrait retrouver le mot de passe d'Alice.

### 1.2.2. Attaques par force brute, collisions et recherches inverses

Deux jeux de données différents en entrée peuvent partager un même *hash* : on parle dans ce cas de **collision**. Une **attaque par force brute** consiste à essayer successivement toutes les données possibles jusqu'à générer une collision, ce qui donne une donnée d'origine possible. Par exemple, supposons qu'Ève connaisse le *hash* d'un mot de passe dont dispose Alice. Pour retrouver le mot de passe, Ève peut essayer de générer successivement de très nombreux documents différents, calculer leur *hash*, jusqu'à arriver à une collision.

Des collisions sont possibles en théorie, puisque « seuls » $10^{177}$ *hashes* différents sont envisageables lorsque la taille du *hash* est de 256 bits, alors qu'une infinité de données sont possibles en entrée[6]. Cependant, elles sont en pratique improbables et même presque impossibles : pour deux données différentes en entrée, une collision a une chance sur $10^{177}$ de survenir, un nombre tellement grand qu'il est impossible de se le représenter. On peut raisonnablement considérer qu'une telle collision ne surviendra jamais[7]. Par ailleurs, à ce stade, il est consensuel que les développements de l'informatique quantique ne remettent pas en cause ce principe – il suffit, pour maintenir un niveau de sécurité constant, de doubler la taille des *hashes*. D'éventuelles collisions ont beaucoup plus de chances d'être liées à un défaut de conception de la fonction de hachage.

---

[5] Il est d'usage, pour la présentation de problèmes de cryptographie, de nommer « Alice », « Bob » et « Charlie » des personnages fictifs souhaitant échanger des données et « Ève » une personne mal intentionnée cherchant à exploiter une faille du système. À noter que, dans le cadre d'une connexion à internet, Alice, Bob et Charlie peuvent représenter des machines, incluant des serveurs hébergeant des sites web, plutôt que des individus.

[6] Il s'agit du « principe des tiroirs » : si l'on dispose de 11 chaussettes et de 10 tiroirs, alors nécessairement un tiroir contient deux chaussettes ou plus. De même, si l'on ne dispose que de $10^{177}$ *hashes* possibles alors que davantage de données sont possibles en entrée, il existe nécessairement deux données d'entrée ayant le même *hash*.

[7] Supposons que l'on dispose d'un *hash* et que l'on essaye de provoquer une collision. En février 2023, la machine la plus performante pour calculer des *hashes*, conçue pour miner du *bitcoin*, peut calculer 250 000 milliards de *hashes* par seconde. Supposons que l'on puisse remplacer **chaque atome de l'univers** par une de ces machines et qu'on les fasse fonctionner pendant **un milliard de milliard d'années** (l'âge de l'univers étant estimé à environ 14 milliards d'années), alors, il y aurait seulement une chance sur un million qu'une collision ait été trouvée.

En revanche, des attaques par force brute sont possibles lorsque les données possibles sont peu nombreuses. Supposons qu'Ève connaisse le *hash* du numéro d'inscription au registre (NIR) d'Alice. Comme il existe seulement quelques dizaines de milliards de NIR possibles, Ève peut se contenter de calculer les *hashes* de tous les numéros envisageables, jusqu'à trouver le *hash* d'Alice. Avec un ordinateur de bureau de milieu de gamme en 2023, quelques heures lui suffiront. Avec une machine spécialement conçue pour cette tâche, la collision sera trouvée en quelques millièmes de secondes.

## 1.3. Principes élémentaires de la cryptographie asymétrique

### 1.3.1. Notion de cryptographie asymétrique et chiffrement de messages

Une notion fondamentale en cryptographie est la **cryptographie asymétrique**, parfois appelée **cryptographie à clefs publiques et privées**.

Dans les techniques de cryptographie simple, dite *symétrique*, un même code (parfois appelé « clef ») permet de chiffrer et, par l'opération inverse, déchiffrer un message. Au contraire, en cryptographie asymétrique, il est nécessaire de disposer de **deux** clefs, qui fonctionnent par paire et permettent d'accomplir indifféremment des opérations de chiffrement et de déchiffrement, jouant des rôles réciproques. Ces techniques reposent sur des outils mathématiques avancés (arithmétique modulaire et courbes elliptiques) dont la compréhension n'est pas nécessaire à la lecture du présent rapport.

Supposons qu'Alice veuille recevoir des messages chiffrés. Elle génère une paire **(clef publique, clef privée)**. Elle peut communiquer à tout le monde sa clef publique, mais doit impérativement conserver en sécurité sa clef privée. Intuitivement, cette technique revient à imaginer qu'Alice remette à toute personne qui en fait la demande un cadenas (clef publique) qui ne peut être ouvert que par une personne qui possède le code (clef privée). Bob et Charlie peuvent sécuriser leurs messages avec le cadenas et avoir la certitude que seule Alice pourra les lire puisqu'elle ne communique le code à personne.

Les clefs publiques et privées sont, en pratique, des suites de bits, que l'on peut représenter avec la notation hexadécimale (*cf.* 1.1) ou toute autre représentation pertinente. S'agissant d'*Ethereum* par exemple, les clés publiques ont une longueur de 512 bits, soit 128 caractères hexadécimaux.

Si Bob veut envoyer à Alice un message *M*, il peut le chiffrer en utilisant la clef publique d'Alice : il génère un message ***C* = chiffrer(*M*, clef publique Alice)**. Il peut ensuite envoyer à Alice le message *C*.

La transformation est conçue de telle sorte que si une attaquante, Ève, intercepte le message et essaye de le déchiffrer, même en connaissant la clef publique d'Alice, elle ne pourra rien faire. Il n'est pas possible de déchiffrer le message à partir de *C* et de la clef publique.

En revanche, Alice peut retrouver le message *M* par une opération ***M* = déchiffrer(*C*, clef privée Alice)**. Il est donc indispensable que personne ne connaisse sa clef privée : toute personne qui détient la clef peut lire les messages. En particulier, la clef privée ne peut pas être retrouvée à partir de la clef publique.

Par principe, la clef publique peut être diffusée librement, par exemple dans un annuaire public. Alice peut donc recevoir des messages de toute personne qui souhaite lui écrire. L'intérêt essentiel de cette méthode est qu'il n'est pas nécessaire qu'Alice et Bob se soient, par avance, mis d'accord sur un code secret pour échanger.

Cette technologie est notamment utilisée pour établir une connexion sécurisée à internet (protocole HTTPS/TLS) : dans ce cas, Alice et Bob peuvent représenter l'utilisateur du site et le serveur.

### 1.3.2. Application de la cryptographie asymétrique au problème de l'authentification

La cryptographie asymétrique ne sert pas uniquement à échanger des messages secrets. Les mêmes techniques permettent aussi d'**authentifier** un message. Ceci permet notamment de réaliser des contrôles d'accès, des signatures électroniques ou encore des autorisations d'ordres.

Une propriété de certains algorithmes de cryptographie asymétrique est en effet que la clef publique et la clef privée jouent des rôles identiques dans les processus de chiffrement. En principe, un message est chiffré avec la clef *publique* de son destinataire et déchiffré par le destinataire avec sa clef *privée* (*cf.* 1.3.1). Au contraire, si une personne chiffre un message avec sa clef *privée*, toute personne qui dispose de la clef *publique* correspondante peut le déchiffrer en utilisant cette dernière.

Par contre, dans ce dernier scénario, le déchiffrement échoue si les deux clefs ne correspondent pas. Notons ($\boldsymbol{K}_{\mathbf{pub}}$, $\boldsymbol{K}_{\mathbf{priv}}$) un couple (clef publique, clef privée). Pour qu'un message puisse être déchiffré avec la clef $\boldsymbol{K}_{\mathbf{pub}}$, alors il faut qu'il ait été chiffré avec la clef $\boldsymbol{K}_{\mathbf{priv}}$. Ce faisant, si une personne souhaite prouver qu'elle possède la clef $\boldsymbol{K}_{\mathbf{priv}}$ sans révéler cette clef, alors il suffit qu'elle émette un message pouvant être déchiffré avec $\boldsymbol{K}_{\mathbf{pub}}$. Le seul fait d'être en capacité de produire un message déchiffrable avec $\boldsymbol{K}_{\mathbf{pub}}$ prouve la détention de $\boldsymbol{K}_{\mathbf{priv}}$ et donc, l'identité de l'auteur du message.

Supposons par exemple qu'Alice souhaite envoyer un ordre de virement à son banquier Bob. L'ordre consiste en un message $\boldsymbol{M}$ = « *Vire 1 000 € à Charlie – Message envoyé par Alice le 01/03/2023 à 14 h 30.* ». Alice peut alors produire une signature électronique en calculant $\boldsymbol{S}$ **= chiffrer(**$\boldsymbol{M}$**,** $\boldsymbol{K}_{\mathbf{priv}}$**)**. Il suffit alors à Bob, pour authentifier le message, de calculer $\boldsymbol{M'}$ **= déchiffrer(**$\boldsymbol{S}$**,** $\boldsymbol{K}_{\mathbf{pub}}$**)** et de constater qu'il retombe bien sur le message $\boldsymbol{M}$. Il aura ainsi la garantie que la personne qui lui a expédié le message était bien Alice – sous réserve qu'elle ait bien gardée secrète sa clef privée. En effet, si son interlocuteur n'est pas Alice, alors ne possédant pas la clef privée, il est incapable de produire une signature $\boldsymbol{S}$ telle que **déchiffrer(**$\boldsymbol{S}$**,** $\boldsymbol{K}_{\mathbf{pub}}$**)** redonne bien le message $\boldsymbol{M}$.

Cette même technique peut être utilisée pour adjoindre une signature horodatée à n'importe quel document[8]. La signature a donc deux propriétés :

- elle ne peut être produite que par une personne qui avait en sa possession à la fois le document et la clef privée ;
- toute personne peut, si elle dispose du document, de la clef publique du signataire et de la signature, vérifier que les trois informations sont compatibles.

Il est également possible d'appliquer des signatures successives et même de garantir l'ordre des signatures. Dans tous les cas, il est essentiel, pour que l'authenticité soit garantie :

- qu'Alice soit bien la seule à détenir sa clef privée (problème de la conservation sécurisée des clefs) ;

[8] En pratique, la signature *S* étant au moins aussi lourde que le message ou le document initial, Alice ne signe pas le message en lui-même, mais un *hash* de ce message (*cf.* 1.2.1).

- que Bob soit sûr que la clef publique qu'il va utiliser est celle d'Alice, non celle d'un usurpateur. Supposons en effet que l'interlocutrice de Bob soit identifiée par la clef publique `0x123a11ce` : le protocole précédent pourra permettre à Bob d'être *certain* qu'il communique avec « *une* personne qui utilise la clef publique `0x123a11ce` ». Si de plus la clef privée a été conservée en sécurité, alors il pourra avoir *confiance* dans le fait que son interlocutrice est « *la* personne qui utilise la clef publique `0x123a11ce` ». En revanche, il est difficile d'être certain que cette personne est bien « l'individu Alice ». Si Bob a précédemment rencontré Alice de visu, alors il peut lui demander quelle est la clef publique qu'elle utilise, mais dans le cas contraire, le problème consistant à assurer que « l'individu Alice » et « *la* personne qui utilise la clef publique `0x123a11ce` » sont la même personne est un problème **difficile**.

  Les solutions apportées reposent principalement sur la création de réseaux de confiance ou sur des certifications déléguées (*cf.* encadré 5, p. 19). Cette problématique, qui a des conséquences juridiques en droit de la preuve, est étudiée en section 3 de l'annexe IV.

Dans certains contextes, notamment celui des *blockchains*, la clef publique d'un individu est appelée son *adresse*. Autrement dit, Bob peut avoir la certitude qu'il échange avec *la* personne à l'adresse `0x123a11ce`.

## 2. Les *blockchains*, parmi lesquelles *Bitcoin*, sont des registres distribués conçus pour permettre l'enregistrement et la vérification de transactions en l'absence de tiers de confiance

*Bitcoin* (avec une majuscule) constitue le premier exemple de *blockchain*, destinée à l'usage du grand public pour la réalisation de transactions dans une unité monétaire, le bitcoin (en minuscules). Cette *blockchain* est avant tout un registre destiné à l'enregistrement et à la validation de transactions (2.1). Son innovation réside dans le fait qu'elle incorpore un protocole de consensus, la *preuve de travail*, qui garantit la confiance même en l'absence d'autorité suprême chargée de vérifier la licéité des transactions (2.2), mais son intérêt est limité en dehors de ces cas (2.3)[9].

### 2.1. La *blockchain Bitcoin* consiste essentiellement en un registre distribué de transactions réalisées dans une monnaie numérique, le bitcoin

**Définie par les fonctionnalités qu'elle offre, une *blockchain* telle que *Bitcoin* est un registre de données distribué entre plusieurs machines.** *Bitcoin* est essentiellement un système d'enregistrement de transactions, dont l'historique n'est pas centralisé dans un seul serveur ou un petit nombre de serveurs bien identifiés, contrairement, par exemple, aux données bancaires.

L'architecture du système est entièrement ouverte et se veut décentralisée : toute personne peut décider de participer au réseau et conserve alors une copie, complète ou partielle, de l'historique des transactions. Pour obtenir une copie, il lui suffit de la demander à un ou plusieurs autres participants au réseau. Les différents acteurs du réseau peuvent à tout moment comparer et s'échanger la version du registre qu'ils possèdent. Un tel registre est qualifié de *dispositif d'enregistrement électronique partagé* (DEEP) ou *distributed layer technology* (DLT) en anglais.

[9] La source principale utilisée pour cette section est le livre blanc de *Bitcoin* : Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash* System, 2008

Toute personne qui en fait la demande peut utiliser le réseau pour passer ou recevoir des transactions. Un utilisateur du réseau génère une paire (clef publique, clef privée) au moment de rejoindre le réseau (*cf.* 1.3.1). **Chaque utilisateur est identifié par sa clef publique, qui constitue son « *adresse* »**[10], laquelle a typiquement une longueur de 256 bits pour *Bitcoin*, soit 64 caractères hexadécimaux. Sa clef privée est quant à elle indispensable pour autoriser les mouvements depuis le compte correspondant à son adresse.

L'unité monétaire est appelée bitcoin (symbole ₿ ou BTC). Les bitcoins sont divisibles jusqu'à la fraction de 1 / 100 000 000 (cent-millionième). Les nouveaux bitcoins sont mis en circulation par des utilisateurs particuliers du réseau appelés les *mineurs* (*cf.* encadré 2, p. 11), les règles de fonctionnement du réseau conduisant à ce que 21 000 000 bitcoins au maximum puissent être en circulation.

Supposons qu'Alice, dont l'adresse est `0x123a11ce`[11], souhaite passer une transaction de 1,2 ₿ à Bob, dont l'adresse est `0x12345b0b`. Pour cela, elle doit tout d'abord prouver qu'elle détient au moins 1,2 ₿. Elle commence donc par lister des transactions précédentes, figurant dans le registre, qui lui sont adressées (c'est-à-dire qu'elles sont destinées à l'adresse `0x123a11ce`) : par exemple la transaction n° 652, qui lui a rapporté 1 ₿, et la transaction n° 1 432, qui lui a rapporté 0,5 ₿. Pour passer une transaction, elle envoie un ordre de virement à l'ensemble des autres machines du réseau. Cet ordre peut être interprété comme :

> *« Je souhaite utiliser le produit des transactions n° 652 et n° 1 432, qui représente 1,5 ₿. Virez 1,2 ₿ à l'adresse `0x12345b0b`, laissez 0,299 ₿ à mon adresse `0x123a11ce` et prenez le reste, soit 0,001 ₿, en frais de transaction »*

**Cette transaction est horodatée et signée par Alice avec sa clef privée** (*cf.* 1.3.2), qui est appariée avec sa clef publique, de sorte que toute personne peut vérifier l'authenticité de l'ordre.

Les ordres sont envoyés à l'ensemble du réseau pour être exécutés. Après un délai de quelques dizaines de minutes nécessaire à la mise en œuvre du processus de validation (*cf.* 2.2.2 *infra*), ils sont pris en compte. La transaction d'Alice reçoit alors un numéro[12], par exemple n° 3 461. Alice pourra donc utiliser lors d'une transaction ultérieure les 0,299 ₿ qu'elle a conservés et Bob les 1,2 ₿ qui lui ont été virés, en visant la transaction n° 3 461. Les transactions n° 652 et n° 1 432 ayant été entièrement consommées, Alice n'a plus besoin de se souvenir que des fonds lui avaient été transférés. En outre, ces transactions ne pourront plus être réutilisées, ce qui rend impossible de repasser le même ordre ultérieurement de façon frauduleuse.

---

[10] En réalité, pour des raisons de mise en œuvre technique, l'adresse n'est pas la clef publique tout entière, mais un dérivé ou une fraction de celle-ci. Les auteurs font le choix de simplifier l'exposé en confondant, à dessein, l'adresse et la clef publique.

[11] Les adresses sont volontairement raccourcies et simplifiées à des fins de lisibilité.

[12] En réalité, un *hash* de l'ordre de virement.

Pour effectuer ces opérations, **Alice peut utiliser l'un des très nombreux logiciels[13] à sa disposition**, parfois présentés comme des « portefeuilles »[14]. Ces logiciels sont chargés d'envoyer les ordres de transaction et de surveiller leur bonne exécution. Ils peuvent ensuite afficher le solde associé à son adresse publique en recherchant cette information dans la *blockchain*. Ils proposent par ailleurs diverses solutions de sécurité pour permettre à Alice de signer des transactions avec sa clef privée : la clef peut être stockée sur son ordinateur ou son téléphone, dans une clef USB ne pouvant être lue qu'avec un logiciel spécifique, sur un appareil sécurisé spécifique ou encore sur le site d'une plateforme (*cf.* encadré 1). Le logiciel peut ne permettre de lire la clef qu'à la saisie d'un mot de passe ou proposer des solutions de récupération. Les éditeurs de ces « portefeuilles » — en fait, des logiciels d'intermédiation entre l'utilisateur et la *blockchain* — disposent d'une grande liberté.

**Encadré 1 : Problématiques liées à la détention des clefs**

La maîtrise d'un bitcoin, et plus généralement de tout cryptoactif, suppose la possession de la clef privée associée au compte qui le détient. Plus précisément, une personne a la maîtrise d'un cryptoactif si et seulement si cet actif est associé dans la *blockchain* à une adresse publique *A* et que la personne possède la clef privée *K* appariée avec *A*. En effet, la détention de la clef privée est indispensable pour signer un ordre de transaction lié à cet actif.

Un utilisateur du réseau pourrait en théorie conserver par ses propres moyens sa clef privée (qui consiste en une suite de bits) et réaliser à la main les calculs informatiques nécessaires pour les signatures électroniques authentifiant les transactions qu'il souhaite passer. En pratique, cette opération est réalisée par son logiciel de « portefeuille » (*Metamask*, *Ledger*, *Zengo*, *etc.*) ou par l'hébergeur (le plus souvent une plateforme d'échange telle que *Kraken*, *Binance*, *etc.*) qu'il utilise. Compte tenu de la sensibilité des clefs, elles ne sont jamais stockées « en clair », mais seulement sous une forme chiffrée (à l'aide d'un mot de passe). Lorsqu'il souhaite réaliser une transaction, l'utilisateur commence par autoriser le déchiffrement de la clef (par exemple en fournissant le mot de passe), puis le portefeuille ou l'hébergeur réalise les opérations de signature en utilisant la clef déchiffrée, et enfin détruit la clef déchiffrée, ne conservant que la version chiffrée.

Deux grandes catégories de solutions existent :

- les solutions *custodial* (avec détention), dans lesquelles l'éditeur du « portefeuille » ou la plateforme d'hébergement détient la clef privée. C'est donc l'éditeur ou la plateforme qui, à la demande de l'utilisateur, passe les ordres de transaction et les signe en son nom ;
- les solutions *non-custodial* (sans détention), dans lesquelles l'éditeur du « portefeuille » n'a pas accès à la clef privée. Dans ce cas, la clef privée peut être stockée sur l'ordinateur de l'utilisateur dans l'espace de stockage accordé au portefeuille, dans son téléphone, sur une clef USB lisible par le portefeuille ou encore imprimée sur une feuille de papier.

Déterminer qui a la maîtrise des actifs nécessite une analyse fine de ce que peut faire la plateforme ou l'éditeur du portefeuille sans action de l'utilisateur. Pour une solution *custodial*, il est en particulier nécessaire de déterminer si les opérations de signature sont réalisées sur un serveur de la plateforme ou de l'éditeur (qui a donc accès, même pendant un temps très limité à la clef privée) ou sur un appareil de l'utilisateur. De même, l'existence de solutions de récupération de mot de passe égaré peut impliquer, dans certains cas, que l'éditeur ou la plateforme dispose d'un moyen de connaître la clef.

Le choix d'une solution de sauvegarde des clefs repose donc sur un arbitrage entre le risque de perte et le risque d'usurpation d'identité par l'éditeur du portefeuille ou la plateforme.

[13] Incluant des applications web ou mobile, des logiciels embarqués sur des terminaux dédiés, *etc.*

[14] Contrairement à un portefeuille physique, un « *portefeuille* » *Bitcoin* (« *wallet* », en anglais) ne contient aucune donnée ni aucune valeur. Le « *portefeuille* » se contente de lire sur la *blockchain* le solde de l'utilisateur et s'apparente davantage au solde d'un relevé de compte.

Les transactions passées dans la *blockchain* sont entièrement publiques. L'ensemble des utilisateurs du réseau peuvent donc suivre les transactions, conserver une copie ou encore tenir à jour une balance des comptes[15]. Ils peuvent par ailleurs vérifier l'authenticité et la licéité des transactions. S'agissant de la transaction précédemment décrite, une telle vérification consiste à :

- vérifier que les transactions n° 652 et n° 1 432, qui ont apporté des fonds à `0x123a11ce` (c'est-à-dire Alice), existent réellement dans le registre ;
- vérifier que les fonds apportés à `0x123a11ce` par ces transactions représentaient bien au moins 1,5 ₿ ;
- vérifier que ces transactions n° 652 et n° 1 432 n'ont pas déjà été « consommées » par une autre transaction (dans le cas contraire, les fonds seraient dépensés deux fois) ;
- vérifier que l'ordre a bien été signé par Alice, c'est-à-dire que la signature est bien émise par une personne détenant la clef privée appariée avec la clef publique `0x123a11ce`.

Ainsi, **en matière d'utilisations possibles, la *blockchain Bitcoin* constitue avant tout un registre distribué de transactions**.

Ces transactions sont des écritures performatives : il suffit que l'ordre « *Alice vire 1,2 ₿ à Bob* » soit inscrit dans le registre pour qu'il soit vrai, ou autrement dit pour qu'Alice ait effectivement 1,2 ₿ de moins à sa disposition, et Bob 1,2 ₿ de plus à la sienne. Les bitcoins n'ont aucune valeur intrinsèque : leur désirabilité et l'utilité qu'Alice et Bob peuvent en retirer dépendent uniquement de l'offre et de la demande des bitcoins, sans qu'un sous-jacent (réserves d'or, créances…) soit garanti ou qu'une intervention étatique (obligation légale de recevoir des paiements en bitcoins…) affecte ce marché.

## 2.2. L'innovation des *blockchains* repose sur la possibilité de se passer d'intermédiaires de confiance centralisés, au prix d'une perte d'efficience

### 2.2.1. La validation des transactions sur des registres centralisés suppose d'avoir confiance dans l'organe centralisateur ou dans l'État

Une difficulté dans le schéma de transactions décrit en 2.1 est l'étape de validation et de prise en compte des transactions. Il est facile pour tout un chacun de vérifier *a posteriori* qu'une transaction est licite, sur le fondement des critères précédemment décrits. Cependant, plusieurs utilisateurs du réseau pourraient avoir un intérêt à ce que des transactions illicites soient validées. En particulier, les utilisateurs, à titre individuel, peuvent avoir un intérêt à passer des transactions frauduleuses à leur avantage (usurpation d'identité, dépense de fonds indisponibles, *etc.*).

**La solution la plus simple pour traiter ce problème est la désignation d'un tiers de confiance pour valider les transactions.** Ainsi, toute banque, en tenant ses livres de compte, autorise ses clients à passer des transactions entre eux et valide les transactions en vérifiant que celles-ci ont été authentifiées et que les comptes des clients sont créditeurs ou respectent les plafonds de découverts autorisés. Les transactions sont inscrites dans les livres dès que la banque a vérifié leur licéité. Un tel système est centralisé, avec une unique entité chargée de valider les transactions.

[15] Cette possibilité est absente de certaines *blockchains* grand public, qui intègrent des couches cryptographiques supplémentaires destinées à empêcher de reconstituer les transactions passées par une même personne, à l'exemple de *Zcash*. Ces *blockchains* sont exclues des développements qui suivent. Les conséquences de l'existence de ces *blockchains* anonymes, notamment en matière de lutte anti-blanchiment, sont étudiées en section 2 de l'annexe V.

Dans cette configuration, les fraudes des utilisateurs, à titre individuel, sont improbables. Plus exactement, elles ne pourraient survenir qu'à condition d'être couvertes par l'autorité centrale (par complicité ou par défaillance). Dans le cadre de transactions bancaires, un second niveau de confiance provient de l'État[16]: l'utilisateur a en principe confiance dans sa banque et dans l'État pour punir la banque dans le cas où celle-ci autoriserait malgré tout des transactions frauduleuses.

Des systèmes de confiance plus élaborés peuvent être conçus. Il est par exemple possible de prévoir que le pouvoir de valider les transactions soit réparti entre plusieurs acteurs : par exemple au tour-à-tour ou selon des critères liés aux auteurs des transactions. Il peut par ailleurs être envisagé un système de validations multiples, dans lequel une transaction n'est validée que si un certain nombre de personnes ayant ce pouvoir constatent sa licéité. De telles organisations supposent cependant toujours que les responsables de la validation soient identifiés, qu'ils aient établi des règles pour se coordonner et qu'ils puissent donc modifier ces règles s'ils trouvent un accord en ce sens.

**La qualité première des *blockchains* est, pour leurs promoteurs, de permettre de se passer d'organe centralisateur détenant le pouvoir de valider les transactions et de modifier les règles de validation.** Le cadre intellectuel qui a présidé à la mise au point des premières *blockchains*, notamment de la *blockchain* Bitcoin, est, en effet, celui des *cypherpunks*, proches de l'école libertarienne (Ludwig von Mises, Murray Rothbard, *etc.*) et critiques envers l'État, de manière générale mais en particulier en matière monétaire. La *blockchain* vise donc, à son origine, à fournir un système de paiement qui ne soit pas soumis au pouvoir discrétionnaire des banques, des États et des banques centrales, jugés trop peu soucieux de la vie privée des citoyens et trop laxistes dans la gestion de la monnaie. En effet, dans le régime monétaire actuel de monnaie *fiat*, sans contrepartie réelle, la création monétaire est potentiellement illimitée, ce qui peut provoquer de l'inflation et une perte de valeur de la monnaie. En vertu du monopole public de l'émission monétaire et du cours forcé, les citoyens ne peuvent faire autrement que de continuer à utiliser cette monnaie, pourtant dégradée aux yeux des libertariens. Il serait donc dans leur intérêt de pouvoir recourir à une monnaie autre, protégée des politiques discrétionnaires des États et régie par des règles immuables (dans le cas de *Bitcoin*, plafonnement de la masse monétaire, par exemple).

### 2.2.2. L'innovation des *blockchains* repose sur leur capacité à créer de la confiance dans le système sans qu'il soit nécessaire de faire confiance à aucun utilisateur pris individuellement

Les *blockchains* constituent une réponse à la problématique de la validation car elles ne supposent aucune autorité de confiance centralisée. L'hypothèse est au contraire celle d'une **défiance généralisée** entre tous les acteurs chargés de la validation. Dans le cas de *Bitcoin*, d'*Ethereum* et de la plupart des *blockchains*, **toute personne qui le souhaite peut participer à la validation des transactions** sans avoir à démontrer préalablement qu'elle est digne de confiance, ni même à révéler son identité. L'enjeu est alors de réussir, pour chaque acteur, à « convaincre » les autres que les transactions qu'il a validées sont correctes, autrement dit à créer un consensus autour de son travail de validation.

Une création de consensus par vote (le travail de validation est accepté si une majorité de validateurs l'approuve) ne permettrait pas de résoudre le problème sans autorité de centralisation. Le vote pourrait en effet facilement être falsifié, par exemple par un acteur malveillant qui participerait sous de nombreuses identités différentes pour bourrer les urnes, ce qu'il est impossible d'empêcher sans une autorité tenant la liste des votants.

[16] Sous ses différentes formes : administration, pouvoir judiciaire, autorités de contrôle, banque centrale.

Les *blockchains* dépassent cet obstacle en donnant un coût à la validation des transactions. Le mécanisme est conçu de façon à ce que de nombreux acteurs de bonne foi puissent, moyennant un investissement individuel, coopérer, tandis que des acteurs malveillants devraient mettre en jeu des ressources importantes pour réussir à valider des transactions frauduleuses.

*Bitcoin* innove pour cela en demandant aux acteurs de fournir une **preuve de travail** (*proof of work*). Une telle preuve de travail consiste en la résolution d'une énigme cryptographique difficile fondée sur la recherche de *hashes* (*cf.* 1.2) vérifiant certaines conditions. Le principe est alors que le mineur (nom donné aux validateurs dans le système) parvenant à résoudre une telle énigme fait accepter comme valide un ensemble de transactions qu'il a vérifiées (entre quelques centaines et quelques milliers), appelé un « bloc », et obtient en échange une récompense sous la forme de nouveaux bitcoins introduits dans le système et de frais de transaction. La résolution de l'énigme a pour but non pas de vérifier la validité des transactions, mais de démontrer que le mineur ayant vérifié cette validité est digne de confiance et en particulier de rendre artificiellement coûteuses les tentatives de fraude. Le bitcoin est ainsi à la fois l'objet des transactions et le « combustible », donné en récompense aux mineurs, nécessaire au fonctionnement de la *blockchain Bitcoin*. L'encadré 2 présente le travail que réalisent les mineurs pour valider des transactions.

À noter par ailleurs que, les ordres de transactions étant publics, un utilisateur qui le souhaite peut aussi se contenter de suivre les transactions qui ont lieu et s'assurer, pour lui-même, de leur validité. Autrement dit, la vérification de la validité des transactions peut intervenir sans participer à la création de consensus sur la chaîne.

**Encadré 2 : Le processus de minage de *bitcoins* par preuve de travail**

Pour la *blockchain Bitcoin*, la validation des transactions est répartie entre les mineurs. Les transactions sont validées par groupes, appelés blocs. Le mineur qui valide un bloc est sélectionné de façon aléatoire, selon le processus décrit ci-après, la probabilité d'être choisi étant, pour chaque mineur, proportionnelle à sa puissance de calcul.

**Le processus de minage**

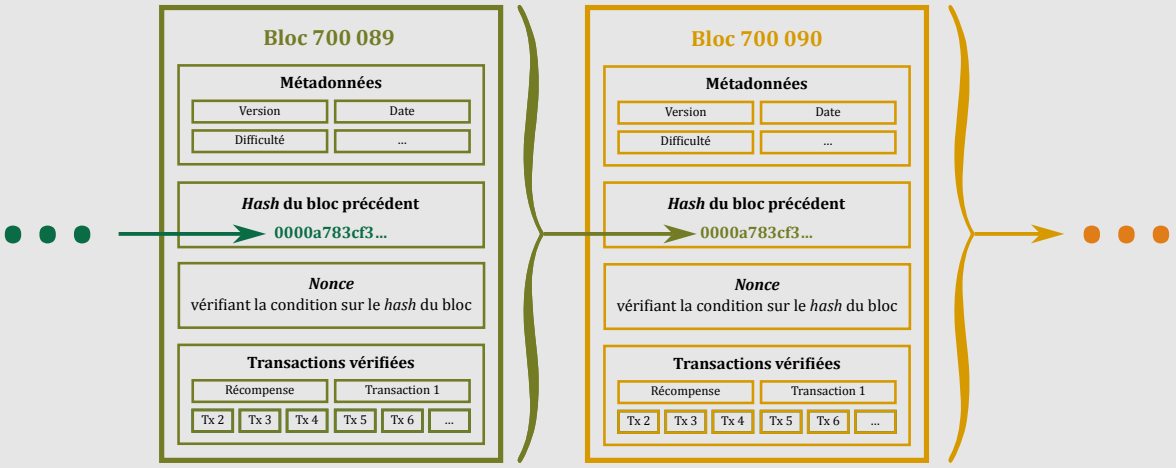
Chaque mineur, en permanence, essaye de construire un bloc dans sa mémoire vive. Pour ce faire, il commence par écrire diverses métadonnées (version du protocole *Bitcoin*, date de création, *etc.*), puis le *hash* (*cf.* 1.2) du dernier bloc validé dont il ait eu connaissance. Après ce *hash,* il laisse une place vide dans son projet de bloc, où il fera figurer ultérieurement un nombre, appelé le *nonce*. Il écrit ensuite une transaction spéciale consistant à accorder une récompense à sa propre adresse – il s'agit de la seule façon dont de nouveaux bitcoins sont mis en circulation. Le mineur espère pouvoir valider *son* projet de bloc, c'est-à-dire faire accepter par l'ensemble des autres acteurs ce projet de bloc de transactions comme étant légitime – incluant donc la transaction d'auto-attribution de récompense.

Il va, ce faisant, mener deux opérations en parallèle :

- d'une part, écouter le réseau pour recevoir des ordres de transaction. Pour chaque ordre de transaction, il vérifie si celle-ci doit être acceptée, c'est-à-dire si elle est correctement signée et si les fonds sont bien disponibles. Si les conditions sont réunies, alors il inscrit la transaction dans son projet de bloc, en orientant vers sa propre adresse les frais de transaction éventuellement prévus. Il peut décider de n'ajouter la transaction au bloc que si elle prévoit des frais de transaction suffisants (déterminés par la loi de l'offre et de la demande) et faire passer en priorité les transactions comportant les frais de transaction les plus élevés. Le projet de bloc grossit donc au fur et à mesure que le mineur reçoit et valide des transactions ;
- d'autre part, chercher une valeur du *nonce* qui lui permette de valider son projet de bloc. Le bloc ne peut en effet être validé que si celui-ci possède un *hash* vérifiant des conditions préétablies, qu'il est statistiquement très improbable de remplir (*cf. infra*). Le mineur essaye donc en permanence de remplacer le *nonce* par des valeurs aléatoires puis de calculer le *hash* du bloc, jusqu'à espérer trouver une valeur du *nonce* qui satisfasse la condition.

Lors de cette phase, les mineurs sont tous en concurrence : chacun essaie d'être le premier à trouver un *nonce* satisfaisant la condition pour son projet de bloc.

Ce processus s'arrête lorsque le mineur a trouvé un *nonce* qui permette de valider le bloc qu'il était en train de construire. Lorsque cet événement survient, le mineur diffuse sur le réseau le bloc qu'il vient d'achever en vue de le faire accepter par les tiers.




### La recherche d'un *nonce* correct et la difficulté du minage

La condition de validité d'un bloc est définie, en substance, comme le fait d'avoir un *hash* commençant par un certain nombre de bits égaux à zéro. Ce nombre évolue avec le temps et dépend d'un paramètre appelé la *difficulté* du minage. Au 8 février 2023, ce nombre est fixé à 77 : un bloc est donc validé seulement si les 77 premiers bits de son *hash* SHA256 (qui en contient 256) sont égaux à zéro. Plus le nombre de zéros exigé est élevé, plus il est rare qu'un *hash* respecte la condition, donc plus le problème est difficile.

Le *hash* d'un bloc dépend de l'ensemble de son contenu, notamment du *nonce* qu'il contient. Or, l'« effet avalanche » (*cf.* 1.2.1) rend le *hash* d'un bloc imprédictible en fonction du *nonce* choisi. Le tableau ci-dessous illustre ce phénomène sur un exemple : on considère un « bloc » simplifié à l'extrême dont le contenu est « *08/02/2023 - [nonce] - Alice 1 BTC à Bob, Charlie 2 BTC à Alice* », où *[nonce]* représente un nombre inconnu à six chiffres. On cherche un *nonce* de façon à ce que le *hash* du bloc commence par seize bits à zéro (donc quatre zéros en représentation hexadécimale). Dans cet exemple, en testant successivement toutes les valeurs possibles des *nonces* avec un programme informatique, comme le ferait un véritable programme de minage, on trouve que les plus petits *nonces* résolvant le problème sont 244 457 et 322 135 (la solution n'est pas unique).

| ***Nonce*** | **Bloc correspondant** | ***Hash* SHA-256** |
|---|---|---|
| 000000 | 08/02/2023 - 000000 - Alice 1 BTC à Bob, Charlie 2 BTC à Alice | `7865defcd8`... |
| 000001 | 08/02/2023 - 000001 - Alice 1 BTC à Bob, Charlie 2 BTC à Alice | `b048646796`... |
| 000002 | 08/02/2023 - 000002 - Alice 1 BTC à Bob, Charlie 2 BTC à Alice | `a913097d95`... |
| ... | ... | ... |
| 244456 | 08/02/2023 - 244456 - Alice 1 BTC à Bob, Charlie 2 BTC à Alice | `55da0cb15d`... |
| **244457** | **08/02/2023 - 244457 - Alice 1 BTC à Bob, Charlie 2 BTC à Alice** | **`00002e70e2`**... |
| 244458 | 08/02/2023 - 244458 - Alice 1 BTC à Bob, Charlie 2 BTC à Alice | `9c6e546dfd`... |
| ... | ... | ... |
| **322135** | **08/02/2023 - 322135 - Alice 1 BTC à Bob, Charlie 2 BTC à Alice** | **`00000f67fb`**... |
| ... | ... | ... |

*Source : Mission, par l'utilisation de la bibliothèque* hashlib *de Python.*

Grâce à l'« effet avalanche », les mineurs n'ont aucun autre moyen, pour trouver un *nonce* respectant la condition, que d'essayer successivement et le plus vite possible toutes les valeurs. Le fait qu'il n'existe pas d'autre façon de trouver un *nonce* permettant de valider le bloc rend le processus de validation réellement aléatoire, la probabilité de réussite d'un mineur étant proportionnelle à sa rapidité à essayer des *nonces*, donc à sa puissance de calcul.

## Annexe I

La **difficulté** du minage du bitcoin représente l'espérance du nombre d'essais de *nonces* nécessaires avant de réussir la validation d'un bloc. Au 8 février 2023, cette difficulté est d'environ **$1{,}8 \times 10^{23}$ essais** (180 000 milliards de milliards d'essais). Autrement dit, chaque essai d'un *nonce* a une chance sur $1{,}8 \times 10^{23}$ de rendre un bloc valide. Pour chaque essai, le mineur réalise une suite d'opérations, parmi lesquelles la plus complexe est le calcul du *hash* du bloc en cours de construction : la difficulté peut donc être interprétée comme le *nombre de* hashes *à calculer avant validation d'un bloc*. En utilisant les préfixes du système international d'unités, on parle de kilo*hashes* (kh), mega*hashes* (1 Mh = 1 000 kh), giga*hashes* (1 Gh = 1 000 Mh), tera*hashes* (1 Th = 1 000 Gh), peta*hashes* (Ph*, etc.*), exa*hashes* (Eh) et zetta*hashes* (Zh). Autrement dit, la difficulté d'un bloc au 8 février 2023 est de **180 Zh**.

Cette difficulté est fixée en fonction de la puissance de calcul totale disponible sur le réseau afin de garantir qu'en moyenne, un bloc sera miné toutes les dix minutes. Ainsi, au 8 février 2023, l'ensemble des mineurs sont capables de calculer collectivement environ **300 milliards de milliards de *hashes* par seconde (300 Eh/s)** : ensemble, ils réalisent $1{,}8 \times 10^{23}$ essais toutes les dix minutes. Tous les 2 016 blocs (soit toutes les deux semaines environ), sur la base de la performance du réseau observée au cours des 2 016 blocs précédemment minés, les mineurs recalculent le niveau de difficulté permettant de maintenir un rythme d'un bloc toutes les dix minutes. La difficulté du minage est inscrite parmi les métadonnées de chaque bloc.

### L'acceptation d'un bloc miné par le réseau

Supposons qu'un mineur ***M*** ait réussi à miner un bloc ***B***, c'est-à-dire à valider les transactions qu'il contient et à trouver un *nonce* vérifiant la condition imposée compte tenu de la difficulté en vigueur.

Il informe alors les autres mineurs en leur envoyant le bloc ***B***, qu'il souhaite faire reconnaître comme légitime. Dès ce moment, les autres mineurs vérifient eux-mêmes la correction du travail du mineur ***M*** sous plusieurs aspects : vérification du fait que les transactions que contient le bloc ***B*** sont toutes valides, vérification du fait que les métadonnées du bloc (en particulier le niveau de difficulté) et le montant de la récompense sont corrects, vérification du fait que le *nonce* vérifie bien la condition de validité. Alors que la recherche d'un *nonce* correct est un problème difficile et requiert plusieurs milliards de milliards d'essais, la vérification de la correction du bloc intervient en quelques millisecondes.

Deux possibilités existent alors :

- si un autre mineur ***N*** constate que le bloc ***B*** reçu est correct, alors il abandonne le projet de bloc sur lequel il travaillait et commence la construction d'un nouveau projet de bloc ***C***, qu'il espère pouvoir faire accepter à la suite de ***B***. Autrement dit, il accepte le bloc ***B*** comme légitime et espère quant à lui être le premier à valider le bloc ***C***. Pour marquer sa reconnaissance de la légitimité du bloc ***B***, il fait figurer le *hash* de ***B*** au début de son projet de bloc ***C***. Son intérêt est de commencer le travail de construction du bloc ***C*** le plus rapidement possible pour augmenter sa chance d'obtenir la récompense et donc d'acter au plus vite qu'il reconnaît le bloc ***B*** ;
- si, en revanche, ce mineur estime que le bloc ***B*** est frauduleux (parce que l'une des transactions n'était pas correctement signée, que les fonds n'étaient pas disponibles, que le montant de la récompense ne correspond pas à ce que prévoit le protocole, que le *nonce* du bloc ***B*** ne permet pas de valider le bloc, *etc.*), alors il l'ignore et poursuit son projet de bloc ***B'*** concurrent de ***B*** en cours, en espérant qu'il trouvera lui-même une solution valide, qu'il pourra faire accepter par les autres mineurs.

Dans tout ce processus, les mineurs sont mus par leur souhait d'obtenir la récompense pour un bloc. En effet, pour qu'ils puissent utiliser cette récompense, il est nécessaire que la transaction d'attribution de récompense soit inscrite dans un bloc reconnu comme légitime. Autrement dit, l'acceptation par les autres mineurs d'un bloc comme étant légitime est indissociable de la reconnaissance de la récompense associée à ce bloc. Pour dissuader certaines tentatives de fraude, le protocole *Bitcoin* prévoit que les récompenses, une fois attribuées, sont indisponibles pendant les cent blocs suivants. Il faut donc, pour qu'un mineur puisse effectivement utiliser sa récompense, qu'il ait réussi à valider un bloc puis que cent blocs aient été ajoutés à la suite du sien, chacun reconnaissant les précédents comme légitimes.

Dans la mesure où tous les mineurs agissent de la sorte, en parallèle (bien que sans coordination), les blocs frauduleux ne seront pas reconnus comme légitimes et une version de la *blockchain* contenant un éventuel bloc frauduleux ne prospérera pas, sauf à ce que la fraude soit couverte par une majorité (pondérée par la puissance de calcul) de mineurs.

Dans le cas où plusieurs versions de la chaîne circulent en parallèle, le protocole prévoit que les mineurs acceptent la version la plus longue, c'est-à-dire celle qui comporte le plus de blocs, donc pour laquelle le plus grand nombre d'énigmes cryptographiques ont été validées.

Ce processus permet de construire une chaîne de blocs (*blockchain*), dont chacun comporte une référence au bloc précédent (son *hash*), un *nonce* respectant les conditions de validation, ainsi que des transactions valides parmi lesquelles une transaction spéciale attribuant une récompense au mineur ayant trouvé la condition de validation du bloc. Par construction, ces blocs « font consensus », c'est-à-dire que les mineurs les acceptent comme légitimes.

**La rémunération des mineurs**

Les mineurs sont rémunérés par la récompense associée à la validation du bloc, exprimée en bitcoins et décroissante dans le temps. La récompense était de 50 ₿ par bloc validé à l'origine et est divisée par deux tous les 210 000 blocs, soit tous les quatre ans environ : depuis 2020, la récompense est de 6,25 ₿ par bloc validé. Début 2023, ces 6,25 ₿ représentent environ 150 000 $ ; la récompense maximale par bloc exprimée en dollars a été atteinte début 2021, avec 900 000 $ par bloc validé. Des frais de transaction sont également prélevés mais ceux-ci sont, pour l'instant, négligeables devant la récompense.

**Dans le système ainsi conçu, une fraude n'est en principe possible qu'à condition que le ou les attaquants qui se coordonnent disposent ensemble de strictement plus de 50 % de la puissance de calcul.**

Supposons en effet, pour simplifier, que le réseau compte 100 mineurs, qui disposent tous de la même puissance de calcul. Supposons que 30 mineurs malveillants se coordonnent pour tenter de faire accepter des transactions frauduleuses[17]. Partons d'un état dans lequel la chaîne compte 10 000 blocs valides. Nous présentons deux scénarios d'attaques.

Un premier scénario d'attaque consiste en la tentative d'ajouter des nouveaux blocs frauduleux. Dans ce scénario, les 30 mineurs malveillants construisent un projet de bloc n° 10 001 comportant une nouvelle transaction frauduleuse, qu'ils ajoutent à la chaîne. Comme chaque essai d'un *nonce* pour valider le bloc a les mêmes chances de réussite (du fait des propriétés des fonctions de hachage cryptographique, *cf.* 1.2.1), ils n'ont que 30 % de chances d'être les premiers à trouver un *nonce* valide pour le bloc n° 10 001. Supposons que ce soit le cas et que l'un des attaquants réussisse à produire un bloc $\boldsymbol{B_{10\,001}}$ avec un *nonce* correct mais qui comporte une transaction frauduleuse. En ce cas, chacun des 70 mineurs bien intentionnés[18] est capable de détecter la transaction frauduleuse et peut en déduire que le bloc $\boldsymbol{B_{10\,001}}$ doit être ignoré. Ils poursuivent donc le travail de construction du 10 001e bloc, jusqu'à ce que l'un d'entre eux parvienne à un *nonce* valide et présente aux autres un bloc $\boldsymbol{B'_{10\,001}}$ *sans* la transaction frauduleuse.

[17] Par exemple : une transaction non signée par le titulaire des fonds dépensés, une transaction pour laquelle l'émetteur ne possède pas les fonds ou encore l'octroi d'une récompense de minage illégitime.

[18] Cela reste valable y compris si parmi ces 70 mineurs, certains sont mal intentionnés mais ne se coordonnent pas avec les 30 attaquants. La réussite d'une attaque suppose une coordination entre attaquants.

À partir de ce point, les 70 mineurs bien intentionnés vont travailler sur une copie de la chaîne comportant le bloc $\boldsymbol{B'_{10\,001}}$ (version « intègre »), et les 30 mineurs mal intentionnés sur une copie comprenant le bloc $\boldsymbol{B_{10\,001}}$. Ces deux copies vont complètement diverger puisque le *hash* de chaque bloc se situe au début du bloc suivant : la différence se répercute en cascade entre les deux copies. Surtout, les 30 mineurs mal intentionnés, parce qu'ils sont moins nombreux, mineront les blocs suivants moins vite. La copie de la *blockchain* sur laquelle ils travaillent deviendra, de façon certaine, plus courte[19]. Tout nouveau participant au réseau pourra donc, en se fondant sur la seule longueur des copies de la chaîne en circulation, savoir laquelle est la version intègre (la plus longue) et travailler sur celle-ci. La transaction frauduleuse et les récompenses découvertes par les mineurs malicieux ne feront donc jamais consensus : elles ne seront jamais reconnues comme légitimes par les autres. En tout état de cause, en cas de doute, tout participant au réseau pourrait revérifier une par une les transactions à partir du bloc n° 10 000 (point de divergence) pour vérifier quelle version du registre est la bonne.

Un second scénario d'attaque consisterait à ce que les 30 mineurs modifient un bloc ancien de la chaîne pour y rajouter une transaction frauduleuse, par exemple dans le bloc n° 7 500. Ils pourraient alors espérer « diffuser » cette version frauduleuse. Cependant, sans même avoir à vérifier une par une toutes les transactions, les autres machines du réseau verraient immédiatement que le bloc altéré est falsifié[20], puisque son *hash* ne correspond pas à la valeur indiquée au début du bloc n° 7 501. Les attaquants auraient donc besoin de reconstruire une nouvelle suite de blocs pour « rattraper » les transactions survenues entre le bloc n° 7 501 et le bloc n° 10 000 et couvrir leur fraude. Néanmoins, la reconstruction de chacun de ces blocs suppose la résolution du problème cryptographique, elle-même chronophage. Les 70 mineurs honnêtes étant plus rapides pour produire de nouveaux blocs que les 30 mineurs malhonnêtes, ces derniers ne pourront jamais rattraper les blocs anciens.

**Dans chacun des deux cas, la corruption de la chaîne est impossible tant que les attaquants coordonnés ne sont pas en majorité (« attaque des 51 % »).** Dans le cas où les attaquants n'ont pas tous la même puissance de calcul, il est en fait nécessaire pour réussir une attaque de détenir la majorité de la puissance de calcul (la force des participants est pondérée par la puissance de calcul dont ils disposent). Cette situation est présentée comme impossible par les promoteurs de *Bitcoin*, quoique cette assertion soit contestable (*cf.* 4.2).

**L'usage de la preuve de travail permet donc de créer une version consensuelle de la chaîne** (transactions et récompenses octroyées pour la validation) **sans aucune hypothèse préalable**, sinon qu'il n'existe pas de majorité animée d'une volonté frauduleuse et coordonnée. Il est possible de faire confiance dans la licéité de ce qui figure dans la *blockchain* sans faire confiance en aucun des acteurs, ni même sans les connaître. Autrement dit, **la preuve de travail permet de créer de la confiance *ex nihilo***.

[19] Il est possible que les mineurs mal intentionnés, par chance, réussissent à valider les quelques premiers blocs plus vite. Cependant, il est *certain* que leur copie de la chaîne deviendra rapidement plus courte que celle des mineurs honnêtes (conséquence de la loi des grands nombres).

[20] Au 8 février 2023, environ 775 000 blocs ont été minés. Il suffit donc, pour assurer l'intégrité de toute la *blockchain*, de vérifier les *hashes* de ces 775 000 blocs. Une telle opération peut être accomplie en quelques millisecondes par un ordinateur de bureau grand public.

### 2.2.3. Cette création de confiance est en revanche très inefficiente : en 2023, une transaction sur le réseau *Bitcoin* consomme autant d'énergie électrique qu'un ménage français moyen pendant deux mois

Le processus de preuve de travail et de validations croisées est fortement consommateur de ressources. Chaque transaction, en effet, est vérifiée individuellement par chacun des validateurs. Surtout, ceux-ci consacrent des ressources importantes pour résoudre le problème cryptographique de validation des blocs et obtenir une récompense en contrepartie (minage et frais de transaction), indépendamment de la vérification des transactions.

La *blockchain Bitcoin* est conçue pour ne pas pouvoir traiter plus de sept transactions par seconde[21] — en pratique, elle en traite en moyenne deux à quatre par seconde[22]. Ce choix est destiné à lutter contre la centralisation du réseau : il permet de limiter le volume de données ajoutées à la *blockchain* chaque année et rend donc plus facile le fait de s'en procurer une copie complète. L'arbitrage entre efficience et niveau de décentralisation est discuté en 4.1.

Aussi, si de nouveaux utilisateurs souhaitent participer au processus de validation, la conséquence ne sera pas une augmentation du débit de transactions possibles, mais seulement une augmentation de la difficulté du minage pour maintenir la moyenne d'un bloc toutes les dix minutes (*cf.* encadré 2). Le nombre d'opérations est quant à lui régulé par des frais de transaction, fluctuants : ceux-ci s'élèvent à environ 1 $ par transaction en février 2023, mais ont atteint un maximum à 63 $ par transaction en avril 2021.

La puissance déployée dépend donc du point d'équilibre économique entre coût du minage et valeur de la récompense associée : début 2023, cet équilibre conduit à **une consommation électrique instantanée pour le réseau *Bitcoin* de l'ordre de 15 GW[23], soit la puissance de dix réacteurs nucléaires EPR, convertie en chaleur,** sans compter l'énergie nécessaire à la fabrication des machines utilisées pour le minage (*cf.* encadré 3). Début 2023, cette consommation directe représente donc pour le minage du réseau *Bitcoin*, environ 1 MWh par transaction. **Une transaction du réseau *Bitcoin* nécessite donc une consommation électrique équivalente à celle d'un ménage français moyen en deux mois**, soit encore 200 € d'électricité au tarif réglementé français de début 2023.

L'impact environnemental est difficile à comparer rigoureusement à celui d'autres technologies. En effet, les données sur les émissions de $CO_2$ associées à la production de l'électricité consommée par le minage sont difficiles à reconstituer. En outre, les estimations sont limitées en ce qui concerne l'analyse en cycle de vie des appareils nécessaires au minage. De plus, la puissance du réseau varie fortement avec le temps et a connu une augmentation importante entre 2018 et 2021, d'où des difficultés dans la mise à jour des données. Enfin, le choix du dénominateur (impact par transaction, par heure d'utilisation du réseau, par dollar de capitalisation boursière) peut conduire à des interprétations différentes.

[21] Joseph Poon et Thaddeus Dryja, *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*, janvier 2016.

[22] Statistiques du nombre de transactions confirmées par jour sur *Blockchain Explorer*. Au cours de l'année 2022, le nombre de transactions confirmées par jour varie entre 190 000 et 280 000. Le record, atteint le 1er mai 2019, est de 439 549 transactions dans la même journée, soit 5,1 transactions par seconde.

[23] Estimation au 28 mars 2023 calculée par le modèle *Cambridge Bitcoin Electricity Consumption Index*, réalisé par le *Cambridge Centre for Alternative Finance* de l'université de Cambridge (https://ccaf.io/cbeci/index).

## Annexe I

Pour réaliser des comparaisons sur l'empreinte carbone d'une transaction, la mission se fonde sur des estimations de la banque centrale des Pays-Bas[24], reposant sur des données de 2020 et ne tenant compte que des émissions liées à la production de l'électricité consommée par le minage (à l'exclusion, donc, de la fabrication des machines des mineurs). **L'empreinte d'une transaction en 2020 était estimée à 400 kg équivalent $CO_2$, soit :**

- 4 000 heures de visionnage de vidéos sur la plateforme *Netflix*[25] ;
- **un aller simple en avion entre Paris et New-York pour un passager ;**
- **20 % de la cible d'empreinte carbone par habitant nécessaire pour atteindre les objectifs de l'accord de Paris (2 tonnes par habitant et par an).**

Face à ce coût énergétique élevé, deux solutions sont envisagées par les promoteurs des *blockchains* :

- soit abandonner le protocole de preuve de travail pour le remplacer par d'autres protocoles de consensus nécessitant de déployer moins de puissance de calcul et donc de consommer moins d'électricité (*cf.* 4.1.3.1) ;
- soit éviter d'inscrire directement les transactions des utilisateurs dans la chaîne *Bitcoin*, mais intercaler entre l'utilisateur et la *blockchain* un système de « seconde couche » (*layer 2*), n'offrant pas les mêmes garanties de confiance et de décentralisation que la *blockchain Bitcoin*, et n'inscrire sur la *blockchain* que des transactions correspondant à des agrégats des opérations survenues dans le *layer 2*. Le *Lightning Network* et l'un des principaux *layer 2* utilisés pour *Bitcoin* (*cf.* 4.1.3.2).

**Encadré 3 : Consommation d'énergie de *Bitcoin***

Pour miner les bitcoins, les machines du réseau sont capables de réaliser, dans leur ensemble, au 8 février 2023, environ **300 milliards de milliards de *hashes* par seconde (300 Eh/s)**. Le minage est réalisé par des machines comportant des circuits intégrés spécialisés (ASIC). Les ASIC produits début 2023 sont capable de calculer de l'ordre de 100 Th/s (100 000 milliards de *hashes* par seconde)[26]. Les 300 Eh/s déployés par le réseau *Bitcoin* représentent **trois millions d'ASIC à 100 Th/s**.

**Un ASIC très efficient minant à 100 Th/s nécessite une puissance électrique de l'ordre de 2,5 kW**, soit autant qu'une grande plaque de cuisson grand public à puissance maximale[27]. Il dégage une chaleur identique. Compte tenu de ce qui précède, *Bitcoin* requiert une puissance électrique de 7,5 GW, convertie en chaleur. Cette valeur est en fait une sous-estimation, qui ne tient par exemple pas compte des besoins en climatisation des serveurs ni de l'usage de mineurs moins performants.

Le *Cambridge Center for Alternative Finance* de l'université de Cambridge développe un modèle, le *Cambridge Bitcoin Electricity Consumption Index*, permettant d'estimer la puissance effectivement consommée : au 28 mars 2023, cette puissance est de **16,09 GW, soit dix réacteurs EPR**[28]. L'estimation est accompagnée d'un minimum théorique correspondant au cas où tout le minage est réalisé par des mineurs ayant la plus haute efficacité énergétique disponible sur le marché (7,61 GW, ce qui correspond au calcul simplifié précédent), ainsi que d'un maximum théorique correspondant au seuil de rentabilité du minage hors amortissement du matériel dans les pays où l'électricité est la moins chère (26,33 GW).

[24] Juan Pablo Trespalacios et Justin Dijk (De Nederlandsche Bank), *The carbon footprint of bitcoin*, 2021.

[25] Damien Licata Caruso, « Combien une heure de streaming sur Netflix coûte-t-elle à la planète ? », *Le Parisien Aujourd'hui en France*, 21 avril 2021. L'estimation de 100 g équivalents $CO_2$ par heure de *streaming* tient compte de la consommation électrique des serveurs, infrastructures réseaux et supports appareils utilisés pour le visionnage.

[26] Cette valeur constitue un ordre de grandeur. Certaines machines beaucoup moins puissantes et moins onéreuses sont produites. Au contraire, les plus puissantes peuvent atteignent 255 Th/s.

[27] Données issues du site *ASIC Miner Value* consulté en février 2023.

[28] L'estimation est disponible en ligne et actualisée toutes les 24 h sur le site https://ccaf.io/cbeci/index.

## 2.3. La preuve de travail n'a d'utilité que dans un contexte d'adversité généralisée et n'est pas indispensable pour réaliser un registre décentralisé s'il existe un acteur de confiance

L'ensemble du processus de minage et de preuve de travail précédemment décrit a pour seule finalité de permettre la création de confiance *ex nihilo*. Il s'applique dans une situation dans laquelle les participants au réseau font preuve de défiance envers tous les autres et où il est supposé qu'aucune majorité ne pourra émerger pour corrompre le réseau. Dans cette situation bien spécifique, la preuve de travail fournit une solution au problème en permettant de créer un consensus autour des transactions valides. D'autres solutions sont envisageables pour répondre au même problème, en particulier la preuve d'enjeu (*cf.* 4.1.3.1) ; la preuve de travail est cependant la première à avoir été inventée et reste celle qui est considérée comme présentant l'un des plus faibles risques de corruption ou de centralisation.

**La preuve de travail étant un mécanisme extrêmement inefficient, elle n'a vocation à être utilisée qu'en dernier ressort, si des modalités plus simples de création de consensus n'ont pas pu être trouvées.** En particulier, s'agissant de transactions monétaires, l'usage du bitcoin — et plus généralement des cryptomonnaies à preuve de travail — ne répond qu'à une finalité : réaliser des transactions sans intervention des États, des banques centrales, ni d'aucun autre acteur ou réseau d'acteurs faisant autorité. Ce choix, outre le coût énergétique qu'il emporte, implique de nombreuses conséquences : privatisation de la monnaie, impossibilité de mener une politique monétaire, mais aussi impossibilité qu'une autorité judiciaire impose l'annulation de transactions[29].

**En dehors de ce cas d'usage très spécifique, les *blockchains* ne sont nécessaires ni pour gérer un registre ouvert, ni pour authentifier des transactions, ni pour créer un consensus.** En particulier, **ce n'est pas la preuve de travail qui rend les *blockchains* infalsifiables ou qui permet de réaliser des signatures électroniques fiables,** contrairement à une idée fréquemment répandue.

Il reste simple, sans *blockchain*, de créer un registre accessible publiquement, d'autoriser toute personne à écrire dedans et de retracer les modifications effectuées. Il est possible, si les écritures de ce registre correspondent à des transactions, de vérifier avant de les écrire que les fonds sont bien disponibles. Enfin, il est aisé, par des techniques de cryptographie éprouvées, de partager le contrôle de ce système entre plusieurs acteurs, par exemple entre plusieurs entreprises[30], plusieurs États, plusieurs autorités publiques d'un même État ou encore plusieurs officiers publics nommés par un État. L'encadré 4 et l'encadré 5 présentent des exemples d'outils préexistants pouvant être utilisés à cette fin.

**Encadré 4 : Le logiciel *git*, exemple de technologie de registre distribué public sans *blockchain***

Le logiciel *git*, créé en 2005, est conçu pour permettre le travail collaboratif sur des dossiers partagés. Il est en particulier utilisé pour le travail sur des codes sources de programmes dans des équipes de développeurs.

Un administrateur crée un répertoire authentique (*origin*) sur un serveur qu'il contrôle. Les données peuvent être mises à jour ; cependant, les anciennes versions restent toujours disponibles et chaque version est identifiée par un *hash*. Toutes les modifications sont donc publiques et traçables au besoin.

Dans le cas d'un programme en source ouverte (*open source*), l'administrateur autorise toute personne à télécharger une copie du répertoire. Tous les utilisateurs ont la possibilité, sur leur copie, de faire des modifications.

[29] Un État, ou plus spécifiquement l'autorité judiciaire de celui-ci, pourrait *enjoindre* à un acteur de passer une transaction, dans le but de compenser une transaction précédente, s'il était avéré qu'elle est illicite ou frauduleuse. En revanche, l'État ne pourrait pas *forcer* l'exécution de la transaction s'il ne connaît pas la clef privée requise.

[30] Plus exactement, plusieurs personnes accréditées par leur entreprise et qui la représentent.

Les utilisateurs peuvent alors proposer au serveur d'intégrer les modifications qu'ils ont réalisées (*pull request*). Si une modification est acceptée, alors elle devient la nouvelle version authentique, mise à disposition de tous les utilisateurs. Cette modification est également journalisée et traçable.

Il appartient à l'administrateur du répertoire *origin* de définir les règles selon lesquelles les propositions de modification sont acceptées. Par exemple, l'administrateur peut décider d'accepter automatiquement les modifications proposées par les développeurs *seniors* mais valider manuellement les modifications proposées par les développeurs *juniors*. Il peut conditionner l'acceptation à un vote ou encore ajouter une étape de vérification automatique (*hook*) qui rejette la proposition si certaines conditions ne sont pas remplies (par exemple, si le code source comporte une erreur de syntaxe).

Un répertoire partagé *git* est donc un répertoire distribué, ouvert et traçable mais centralisé puisque c'est *in fine* toujours l'administrateur qui fixe les règles permettant d'écrire dans le répertoire. Il serait possible, avec un répertoire *git* et un *hook* de vérification automatique astucieusement configuré, de créer un répertoire partagé contenant un fichier de « transactions » sur le même modèle que *Bitcoin*. Un tel répertoire aurait exactement les mêmes cas d'usages que *Bitcoin*, mais reposerait sur la confiance dans un seul acteur pour fixer ses règles de fonctionnement. **L'apport de *Bitcoin* à un tel système réside dans la possibilité de faire arbitrer collectivement la détermination de la version « authentique », sans que les utilisateurs aient besoin de se faire confiance ou de connaître leur identité ou leur nombre.**

**Encadré 5 : Des possibilités de partage de la confiance sans recourir à une *blockchain***

De nombreux systèmes, utilisés sur le *web* ou antérieurs à celui-ci, permettent, sans aller jusqu'à une hypothèse de défiance généralisée, de partager la confiance entre plusieurs acteurs.

Un premier exemple est l'institution notariale. Chaque notaire constitue un tiers de confiance à même de conserver des actes dont il garantit l'authenticité et la conservation.

Il en va de même s'agissant des technologies de signature électronique, fondée, sur la cryptographie asymétrique (*cf.* 1.3.2). Chaque acteur (université souhaitant authentifier les diplômes qu'elle délivre, fournisseur d'électricité souhaitant authentifier les justificatifs de domicile, *etc.*) est libre de produire des signatures. Toute personne ayant reçu un document signé est responsable de sa conservation. La confiance repose donc sur chaque signataire pour les documents qu'il a signés et seulement pour ceux-là.

Le problème du partage de la confiance se pose tout particulièrement quand il est question d'authentifier l'identité de personnes (*cf.* 1.3.2). Supposons que deux utilisateurs Alice et Bob souhaitent échanger de façon sécurisée. Alice peut écrire son message en utilisant la clef publique de Bob, par exemple `0x12345b0b`. Se pose cependant la question de l'obtention de cette clef. En effet, si une attaquante Ève souhaite intercepter les messages, il lui suffit d'expédier un message à Alice dans lequel elle se fait passer pour Bob et de joindre une clef publique (par exemple `0x67890e4e`) appariée à une clef privée qu'elle détient. La difficulté est donc pour Alice, si elle ne connaît pas *déjà* la clef publique de Bob, de vérifier l'absence d'usurpation d'identité. Deux principales solutions coexistent, sans recourir à des *blockchains* :

- des systèmes d'autorités de certification, utilisé par exemple, pour les protocoles de connexion à internet sécurisée HTTPS/TLS. Les ordinateurs et téléphones sont configurés pour nativement faire confiance à quelques autorités dites « racines » (principalement des entreprises de confiance telles que VeriSign, Amazon ou The Walt Disney Company) dont ils embarquent par défaut les clefs publiques. Bob peut se présenter à l'une de ces autorités « racines » et lui demander de certifier sa clef publique `0x12345b0b` : l'autorité racine vérifie l'identité de Bob (par exemple en lui demandant un titre d'identité émis par un État) puis émet un document certifiant que le titulaire de la clef `0x12345b0b` n'est pas un usurpateur, ce document étant lui-même signé par l'autorité racine.

  Pour éviter l'engorgement des autorités racines, d'autres prestataires (par exemple, en France, les entreprises Gandi ou Dhimyotis) peuvent fournir à Bob le même service après avoir eux-mêmes été certifiés par l'une de ces autorités. Pour s'assurer de l'identité de Bob, il suffit à Alice de vérifier le certificat délivré par la racine au prestataire, puis par le prestataire à Bob. La confiance peut ainsi être déléguée « en cascade », à partir des « racines » dont la fiabilité est présumée ;
- un système à toile, solution moins répandue. Dans un tel système, il n'existe pas d'autorité racine. Toute personne peut publiquement certifier l'identité de toute autre, après avoir contrôlé son identité. Il se forme ainsi un réseau de confiance, dans lequel il est difficile pour un usurpateur d'entrer. Des serveurs publics recensent en permanence les nouvelles signatures pour accroître la transparence de l'ensemble, permettre de retracer des chaînes de confiance, *etc.*

Telles que présentées, aucune de ces technologies ne repose sur un unique acteur central. Toutefois, en réalité, elles requièrent toutes en dernier ressort la garantie implicite de l'État et de l'autorité judiciaire. En effet, c'est le ministre de la justice qui nomme les notaires et peut les révoquer en cas de manquement déontologique. S'agissant des signatures de diplômes ou justificatifs, un émetteur frauduleux s'opposerait à des sanctions pénales. Enfin, les cascades et les réseaux de confiance reposent tous sur la possibilité de vérifier l'identité d'un individu et donc sur la sincérité de l'état civil et de l'agence nationale des titres sécurisées (pour les personnes) ou du greffe du tribunal de commerce (pour les entreprises).

## 3. Certaines *blockchains* peuvent être programmées pour inscrire des données plus complexes que des transferts de cryptomonnaies

La conception de *Bitcoin* rend indissociable deux aspects de cette *blockchain* : son objet, qui est de lister des transactions dans une unité de compte, et son fonctionnement décentralisé. En effet, d'une part, la participation au fonctionnement est rémunérée par des gains dans cette même unité de compte. D'autre part, la décentralisation constitue la raison d'être de cette unité de compte : elle est ce qui la rend désirable et permet donc de l'utiliser comme une *cryptomonnaie*.

Néanmoins, l'idée de disposer d'un registre électronique distribué et dont les règles sont immuables et établies par avance est à l'origine de nombreux autres cas d'usage. Elle rejoint la théorie des « *smart contracts* », c'est-à-dire l'idée de faire exécuter automatiquement par un ordinateur des contrats : une *blockchain* pourrait ainsi constituer un tiers de confiance dans lequel seraient codés ces « *smart contracts* ». En outre, un tel registre électronique pourrait accueillir des « sous-registres » dans d'autres unités de comptes destinées à des usages spécifiques, voire prévoir des règles précises de conversion, d'échange, d'usage, *etc.*

**Un axe de développement des *blockchains* a donc consisté à créer des registres *programmables*, c'est-à-dire pouvant accueillir une liste d'écritures représentant des opérations plus complexes que des transactions monétaires et selon des règles établies par un programme**. Cet objectif a notamment été atteint avec la *blockchain Ethereum*, opérationnelle depuis 2015 : celle-ci peut accueillir, outre des transactions dans la cryptomonnaie qu'elle définit (l'*éther*), des écritures correspondant à l'exécution de programmes informatiques autonomes (abusivement qualifiés de « *smart contracts* ») dotés d'une mémoire.

Ces programmes autonomes sur *blockchain* permettent d'exécuter des opérations *sur* le registre (*on chain*) : la bonne exécution des programmes résulte des règles de fonctionnement de la *blockchain*. Entraver l'exécution, par exemple en réalisant des opérations non prévues, suppose de passer des transactions frauduleuses, que les protocoles de confiance rendent en principe impossibles.

Surtout, leur mémoire peut constituer un sous-registre fonctionnant selon des règles prévues à l'avance. Ces registres peuvent accueillir des transactions de nouvelles unités de comptes : celles-ci sont appelées, en général, des « jetons ». Ces jetons sont différents de la cryptomonnaie de la chaîne (l'éther, pour *Ethereum*).

La souplesse permise par les programmes autonomes autorise à les doter de diverses propriétés *on chain*, par exemple leur associer des flux financiers au bénéfice de leur détenteur. Des conditions contractuelles peuvent par ailleurs permettre de garantir au détenteur d'un jeton des droits *off chain* : par exemple, l'émetteur peut s'engager à laisser le détenteur d'un jeton assister à un spectacle ou accéder à un espace privé sur un réseau social.

**Une définition plus rigoureuse et l'étude du fonctionnement technique des jetons font l'objet de l'annexe II du présent rapport.**

# 4. Le modèle de décentralisation maximale à l'origine de la technologie *blockchain* présente un bilan coûts-avantages contrasté pour les applications autres que les cryptomonnaies

En dépit de l'innovation que représentent les *blockchains* et des possibilités ouvertes par les programmes autonomes, ces outils comportent des limites théoriques qui empêchent leur développement à grande échelle (« scalabilité ») à technologie constante. Pour surmonter ces limites, émergent des solutions plus centralisées, moins sécurisées ou moins résilientes que les *blockchains* à preuve de travail telles que de nouveaux protocoles de consensus ou des « secondes couches » (*layer 2*) telles que le *lightning network* ou les méthodes de *sharding* (4.1). Cependant, même pour les modèles en théorie les plus décentralisés, les coûts afférents à la décentralisation sont importants et des comportements de reconcentration sont observés (4.2). Enfin, les usages des cryptoactifs nécessitent rarement cette décentralisation et ne justifient le plus souvent pas les coûts qu'elle implique : exception faite des cryptomonnaies en elles-mêmes dans une perspective libertarienne, les usages commerciaux des *blockchains* exploitent bien plus les technologies de signature et de registre ouvert que l'innovation *blockchain* en elle-même (4.3).

## 4.1. Les coûts inhérents à la décentralisation font obstacle au développement à grande échelle des *blockchains* et ont conduit à développer des solutions qui mettent davantage l'accent sur l'aspect de registre

### 4.1.1. Un réseau décentralisé et immuable tel que *Bitcoin* ne peut pas être étendu à grande échelle, en particulier pour des raisons liées au stockage de données

Le réseau *Bitcoin* a été conçu pour ne permettre qu'un nombre limité de transactions par seconde. Cette limite est en fait déterminée par celle de la taille des blocs (à l'origine un mégaoctet – 1 Mo –, depuis augmentée à 4 Mo). L'enjeu est d'éviter que les mineurs aient tous à conserver une quantité trop importante de données. Une taille de blocs de 4 Mo au plus, validés toutes les dix minutes en moyenne, conduit à ce que chaque année une copie de la *blockchain* voie son poids augmenter de 200 Go au maximum. Cette limite de taille autorise au maximum sept transactions par seconde.

En comparaison, l'entreprise Visa affirmait en 2017 pouvoir traiter 65 000 transactions par seconde[31]. Un tel nombre de transactions, passées sur le réseau *Bitcoin*, conduirait à générer environ 10 000 fois plus de données soit un alourdissement annuel de la *blockchain* d'environ 2 Po (pétaoctets, 1 Po = 1 000 To = 1 000 000 Go).

[31] *Visa Fact Sheet*, 2018 (https://www.visa.co.uk/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf).

Un tel flux de données est extrêmement important, mais peut être traité par des entités spécialisées. En revanche, il représente une sérieuse barrière à l'entrée pour une personne souhaitant obtenir une copie de la *blockchain* – supposée constituer un registre vérifiable par tous – dans le but de connaître l'historique des transactions et constater l'absence de fraude. *A fortiori*, le minage serait rendu plus difficile, puisqu'il est toujours nécessaire de pouvoir accéder à une copie complète de la chaîne pour pouvoir miner. Chaque personne souhaitant lire la chaîne (que ce soit pour miner ou pour d'autres usages) devrait donc soit investir des montants très importants dans le stockage de données, soit accepter de se reposer sur un tiers. **Dans tous les cas, se poserait le problème de la recentralisation du réseau**, puisque l'historique des transactions validées ne serait conservé que par quelques individus ou entités. Cette problématique est la principale raison pour laquelle les développeurs de *Bitcoin* ont choisi de limiter la taille des blocs et donc le débit maximal théorique du réseau.

Cet arbitrage entre capacité de traitement et décentralisation prévaut également pour d'autres briques de fonctionnement que le stockage. Par exemple, il est difficile et coûteux de disposer d'infrastructures de réseaux capables de vérifier ou même de recevoir et d'enregistrer 65 000 ordres de transaction par seconde. Le problème n'est pas spécifique à la *blockchain* et se pose pour tout système devant traiter un tel volume de requêtes : système d'information d'une banque, réseau social, *etc.* Cependant, pour un système centralisé, les infrastructures capables de traiter un tel volume de requêtes ne doivent être déployées qu'une fois, alors que pour une *blockchain*, chaque nœud doit être équipé. Le coût de la décentralisation est donc extrêmement élevé. La barrière à l'entrée pour le minage s'en trouve rehaussée, puisqu'une machine sous-dimensionnée serait saturée de requêtes et ne pourrait en traiter aucune en temps utile : elle ne pourrait ni vérifier les transactions, ni *a fortiori* participer au minage.

Dans un cas comme dans l'autre, les barrières à l'entrée sont **critiques** : une personne qui ne s'acquitte pas du coût d'entrée ne peut pas du tout participer au fonctionnement du réseau, soit parce qu'elle n'a pas accès aux données historiques nécessaires à la validation des transactions, soit parce qu'elle ne peut pas traiter les requêtes. Il en va différemment de la barrière à l'entrée qu'est le coût de l'électricité et du matériel nécessaires au minage : certes, un utilisateur qui ne réaliserait pas l'investissement suffisant pour disposer d'une capacité élevée à calculer des *hashes* aurait très peu de chances de pouvoir effectivement miner des blocs, mais il en garderait la possibilité théorique et pourrait, en tout état de cause, vérifier les transactions et renforcer sa propre confiance dans l'intégrité du registre. Les barrières critiques, au contraire, diminuent le nombre d'acteurs capables de participer au réseau et provoquent donc une tendance à la recentralisation.

En l'état actuel, les arbitrages réalisés par les développeurs de *Bitcoin* permettent donc à toute personne qui le souhaite, avec un ordinateur de très faible puissance (type *raspberry pi*) et un disque dur de quelques gigaoctets, de disposer d'une copie complète et de suivre en direct toutes les transactions et constater leur intégrité — une machine d'une si faible puissance aurait en revanche des chances quasiment nulles de réussir à miner un bloc si elle essayait de le faire.

### 4.1.2. Plus généralement, le « trilemme des blockchains » empêche d'allier décentralisation, sécurité et passage à l'échelle

La problématique du stockage illustre le fait qu'à niveau de sécurité et de confiance donné, la décentralisation d'un système technologique fait obstacle à sa montée en puissance. Autrement dit, **un arbitrage est nécessaire entre le niveau de sécurité, le niveau de décentralisation et la capacité du système**.

Le choix opéré en matière de taille de blocs vise ainsi à préserver le niveau de sécurité (toutes les transactions sont publiques et conservées sans limite de temps) et le niveau de décentralisation (le coût à l'entrée pour les mineurs est faible), au prix d'une limitation de la capacité du réseau (il ne peut traiter plus de sept transactions par seconde). Certes, des innovations technologiques pourraient permettre d'augmenter légèrement la capacité sans sacrifier ni la sécurité ni la décentralisation, par exemple par un changement de méthode de compression des données. Cependant, de telles évolutions ne permettraient pas de multiplier la capacité du réseau par 10 000, comme il serait nécessaire pour rendre *Bitcoin* utilisable dans la vie courante et remplacer le système bancaire.

Ce « trilemme » s'exprime également en ce qui concerne l'algorithme de création de consensus. La preuve de travail est conçue pour être extrêmement sécurisée, puisque la réussite d'une attaque suppose d'avoir concentré 51 % de la puissance de calcul, ce qui est particulièrement coûteux. Elle permet également de favoriser la décentralisation, puisqu'il suffit à une personne de disposer d'un peu de puissance de calcul pour pouvoir, en théorie, participer à la validation des transactions. Toutefois, sa diffusion s'est accompagnée d'une hausse considérable de la consommation électrique du réseau, en pure perte (*cf.* 2.2.3).

Enfin, un autre triangle d'incompatibilités réside dans l'impossibilité d'allier décentralisation, traçabilité et respect de la vie privée. La traçabilité des transactions, réalisée par exemple par les banques dans le cadre de la lutte contre le blanchiment, suppose une concentration de données personnelles dans le registre. La décentralisation implique alors nécessairement une dissémination de ces données personnelles, avec un risque fort d'atteintes à la vie privée. La commission nationale de l'informatique et des libertés (CNIL) recommande ainsi de ne pas inscrire de données personnelles sur des *blockchains* compte tenu de l'impossibilité pour les personnes concernées de faire respecter leurs droits à la rectification et à l'effacement (*cf.* section 4 de l'annexe V).

### 4.1.3. Diverses technologies mises au point à la suite de *Bitcoin* visent à déplacer l'arbitrage entre les trois sommets du triangle d'incompatibilités, à l'exemple de la preuve d'enjeu (*proof of stake*) et des secondes couches (*layer 2*)

Pour permettre le développement à grande échelle, de nombreuses innovations technologiques ont été proposées : soit par des modifications du fonctionnement des *blockchains* en elles-mêmes et en particulier de leurs algorithmes de consensus, soit par le déploiement d'outils complémentaires aux *blockchains* sous la forme de « secondes couches » (technologies dites *layers 2*). Ces technologies ne parviennent cependant pas à s'émanciper du « trilemme » et supposent toutes de réduire le niveau de sécurité ou d'accepter une plus forte centralisation.

#### *4.1.3.1. Les* blockchains *peuvent reposer sur des protocoles de consensus autres que la preuve de travail, en particulier la preuve d'enjeu*

**En ce qui concerne le fonctionnement des chaînes, la principale innovation réside dans le protocole de preuve d'enjeu (*proof of stake*, PoS, aussi appelé preuve de participation)** pour la création de consensus. Ce protocole repose sur l'idée de pondérer la probabilité d'être tiré au sort pour valider un bloc de transactions non pas par la puissance de calcul comme pour *Bitcoin*, mais par le montant de cryptomonnaie détenu. Le présupposé est que les personnes détenant le plus de cryptomonnaie ont le plus à perdre en cas de diminution de la valeur de leur monnaie qui ferait suite à une perte de confiance des utilisateurs, et ont donc le plus grand intérêt au bon fonctionnement de la chaîne.

Une mise en pratique de la preuve d'enjeu est notamment proposée par la *blockchain Ethereum* depuis 2020 ; après une période de coexistence entre les deux protocoles de preuve de travail et de preuve d'enjeu jusqu'au 15 septembre 2022 (date de « *The Merge* »), *Ethereum* repose désormais exclusivement sur la preuve d'enjeu.

Sur *Ethereum*, la cryptomonnaie de la chaîne porte le nom *d'éther* (symbole ETH ou Ξ). Participer à la validation de transactions suppose d'être capable de miser (*staker*) au moins 32 Ξ, soit environ 50 000 € au cours de l'éther en mars 2023. Un utilisateur souhaitant participer à la validation des transactions commence donc par mettre sous séquestre et miser 32 Ξ, ce qui lui donne le droit d'exécuter un programme appelé « validateur ». Il peut exécuter simultanément autant de validateurs qu'il le souhaite, chacun requérant de séquestrer exactement 32 Ξ : ses chances de succès dans le processus de validation sont multipliées par le nombre de validateurs qu'il exécute simultanément. Autrement dit, en première approximation, **le poids d'un individu ou d'une organisation dans le processus de validation est proportionnel au montant qu'il séquestre**. En revanche, il n'est pas nécessaire de déployer une puissance de calcul importante pour pouvoir faire fonctionner un validateur.

Pour créer du consensus sur les transactions valides, *Ethereum* repose sur un processus complexe de sélection aléatoire et équiprobable d'un validateur parmi ceux qui sont actifs. Une fois sélectionné, le validateur doit produire un bloc de transactions correctes (bien signées et pour lesquelles les fonds sont disponibles), soumis ensuite à un comité de 128 validateurs également désigné aléatoirement[32].

La production par le validateur sélectionné d'un bloc valide et la participation au comité de validation rapportent des récompenses sous la forme de nouveaux éthers mis en circulation. Au contraire, le défaut de production d'un bloc par le validateur sélectionné, la production d'un bloc comprenant des transactions incorrectes ou certaines tentatives de fraude[33], donnent lieu à une pénalité pouvant aller jusqu'à la perte des 32 Ξ mis sous séquestre.

**Un tel mécanisme de preuve d'enjeu a le mérite de diminuer la consommation énergétique de la création du consensus** : il n'est ainsi plus nécessaire pour les validateurs de prouver leur capacité à faire des calculs fortement consommateurs en énergie. Les promoteurs d'*Ethereum* annoncent[34] ainsi que le remplacement de la preuve de travail par la preuve d'enjeu entre 2020 et 2022 aurait permis une division par plus de mille de la consommation électrique de la *blockchain*. Par ailleurs, le fait que les personnes chargées de la validation des transactions soient sélectionnées *a priori* permet d'éviter que des travaux similaires soient menés en parallèle.

**En revanche, d'éventuels inconvénients restent sujets à controverse au sein de la communauté des utilisateurs de cryptoactifs.** Le principal risque théorique cité pour ce protocole est qu'il ne repose pas sur des données objectives et extérieures à la *blockchain* (la capacité à résoudre une énigme cryptographique), mais sur le contenu de la *blockchain* en elle-même (la somme d'éthers précédemment acquis et mis sous séquestre). La capacité du protocole de preuve d'enjeu à créer de la confiance est donc, d'un point de vue mathématique, beaucoup plus fragile que celle de la preuve de travail.

---

[32] Contrairement au mécanisme de preuve de travail, le tirage aléatoire ne repose pas sur une logique de concurrence entre les acteurs (le premier mineur à résoudre un problème est sélectionné), mais est réalisé par l'exécution d'un code reproductible et imprévisible permettant de déterminer le validateur choisi (on parle de « pseudo-aléa »).

[33] Par exemple, le fait d'émettre un vote allant à l'encontre d'une quasi-unanimité sur un projet de bloc.

[34] Ces annonces sont fondées sur un rapport de l'entreprise *Crypto Carbon Rating Institute* (CCRI) publié en septembre 2022 immédiatement avant *The Merge* et affirmant que le passage à la preuve d'enjeu réduirait la consommation énergétique de 99,988 % (https://carbon-ratings.com/dl/eth-report-2022, consulté le 5 avril 2022). La mission n'a pas d'autres sources confirmant ou infirmant ce chiffre ni sa méthodologie.

Le risque de centralisation qui découle du système est quant à lui difficilement apprécié, compte tenu de la complexité des incitations économiques auxquelles font face les acteurs. Par conception, le mécanisme de preuve d'enjeu est ploutocratique (le pouvoir est proportionné à la richesse disponible). Les petits porteurs, qui ne peuvent atteindre le seuil de 32 Ξ, ont la capacité de mettre en commun leurs disponibilités, mais un seul validateur pourra être exécuté avec les sommes qu'ils réunissent : ils doivent donc nécessairement trouver un tiers de confiance qui assurera le *staking* pour leur compte. Dans les faits, les plateformes d'échange (*exchanges*) et d'hébergement de portefeuille qui conservent les liquidités sont particulièrement à même de fournir ce service, d'où une centralisation forte. Enfin, la centralisation du *staking* auprès d'acteurs de confiance découle de la possibilité qu'ils ont de créer de la liquidité : une société spécialisée dans le *staking* peut ainsi réunir les fonds et certifier le montant séquestré. Si la société spécialisée est effectivement digne de confiance, alors les fonds séquestrés seront restitués de façon certaine au déposant lorsqu'il en fera la demande, si bien que le certificat peut être accepté comme collatéral pour d'autres opérations financières.

En tout état de cause, le protocole de preuve d'enjeu a, à date de rédaction du présent rapport, été moins testé en pratique que la preuve de travail ; il est donc difficile de prévoir le comportement économique des *stakers* et les schémas potentiels de fraude.

**Outre la preuve de participation, divers autres algorithmes de consensus sont envisagés et étudiés**, mais ont des niveaux de maturité encore faibles. La *blockchain Solana* repose par exemple sur la « preuve d'historique », qui utilise des fonctions de hachage cryptographiques successives pour démontrer que des opérations se sont produites dans un ordre donné ; ce protocole de consensus a cependant un niveau de maturité moindre que la preuve de travail et la preuve d'enjeu. D'autres protocoles de confiance décentralisés restent au stade de la recherche et développement.

#### *4.1.3.2. Les « secondes couches » (*layer 2*) constituent des interfaces plus centralisées ou moins sécurisées s'intercalant entre l'utilisateur et la* blockchain *à proprement parler*

Les solutions de *layer 2* consistent, sans modification de la chaîne en elle-même, à déployer un autre outil à l'interface entre la chaîne et l'utilisateur. Cet outil est conçu pour permettre le développement à grande échelle en sacrifiant une partie de la sécurité ou de la décentralisation du système : il est principalement destiné à des opérations fréquentes ou à faible enjeu. La *blockchain* est ensuite régulièrement mise à jour pour tenir compte des opérations survenues sur le *layer 2*.

Il existe plusieurs catégories de *layer 2*, dont le seul point commun est qu'ils s'appuient sur une *blockchain* grand public pour leur fonctionnement en dernier ressort.

**L'idée la plus simple de *layer 2* consiste simplement en l'utilisation d'intermédiaires centralisés faisant office de chambres de compensation.** Les systèmes les plus simples en la matière sont mis en pratique par certaines plateformes d'échange de cryptomonnaies (*exchanges*) : plutôt que de disposer directement d'un portefeuille dans la *blockchain*, l'utilisateur dispose d'un compte chez un tiers, qui lui-même détient des cryptomonnaies en son nom. Les échanges entre utilisateurs d'une même plateforme ne nécessitent aucune inscription sur la *blockchain*, mais seulement des écritures dans les comptes de la plateforme. Des échanges entre utilisateurs de plateformes distinctes peuvent par la suite faire l'objet d'une compensation. Une telle situation s'inspire du fonctionnement du système bancaire – la cryptomonnaie de la chaîne jouant alors le rôle de la monnaie centrale. Une telle solution repose sur une centralisation maximale, qui rend sa sécurité aisée à assurer, au prix d'une totale dépendance à la confiance placée par l'utilisateur dans la banque ou dans la plateforme d'échange. Pour cette raison, de tels systèmes ne sont pas présentés comme des solutions au problème de la scalabilité de la *blockchain* par les défenseurs de cette dernière.

**Les *rollups* constituent un premier type de « layer 2 » fournissant une solution à cette dernière problématique.** Les transactions sont réalisées dans un système centralisé et efficient (par exemple une base de données centralisée ou une « *blockchain* privée » – *cf.* encadré 6). Lorsque les utilisateurs en font la demande, le résultat agrégé de leurs transactions est ensuite inscrit sur le *layer 1,* c'est-à-dire la *blockchain* associée. Selon les variantes, soit les utilisateurs disposent d'une période de temps pour contester les transactions inscrites (*optimistic rollup*), soit le gestionnaire du *layer 2* émet une preuve cryptographique du fait que les opérations qu'il inscrit sont valides (*zero knowledge proof*). Ainsi, toute personne peut, à l'aide de cette preuve, avoir la certitude que l'opération agrégée est bien issue de la somme d'opérations qui sont toutes valides, sans que lui soient révélées les opérations individuelles.

La scalabilité est rendue possible par une plus grande centralisation des opérations, tout particulièrement adaptée pour des transactions qui n'ont pas vocation à être rendues publiques ou sont d'un enjeu trop faible pour justifier l'utilisation de la *blockchain layer 1* — par exemple, s'agissant de jetons représentant des objets de jeux vidéo ou de transactions comportant des enjeux en matière de vie privée.

**En deuxième lieu, les utilisateurs peuvent s'appuyer sur des canaux d'états**. Ces outils consistent à permettre aux utilisateurs d'ouvrir des « canaux » (en règle générale bilatéraux) et à réaliser des opérations de gré à gré dont ils inscrivent la somme dans la *blockchain*. Contrairement à la solution précédente, les transactions restent en principe décentralisées, mais ne sont possibles qu'entre deux utilisateurs. Un défi consiste ensuite à pouvoir interconnecter les canaux pour permettre à des transactions de survenir potentiellement entre tous les utilisateurs tout en limitant le nombre de canaux — puisque chaque ouverture et clôture de canal requiert des inscriptions sur la *blockchain*. **Le protocole *Lightning Network*** (*cf.* encadré 7)**, développé depuis 2016, est ainsi le *layer* 2 sur *Bitcoin* le plus mûr technologiquement** et est considéré comme la solution permettant à moyen terme le développement de *Bitcoin* à grande échelle pour une utilisation grand public.

De telles solutions pourraient permettre le passage à l'échelle et le maintien d'un haut niveau de décentralisation — bien que celle-ci doive encore être démontrée en pratique, *cf.* 4.2. La sécurité reste toutefois plus complexe à garantir, puisqu'il est nécessaire de pouvoir résoudre les différends en cas de contestation d'une transaction qui n'a jamais été inscrite sur la *blockchain*. Le *Lightning Network* apporte en principe une solution, mais sa complexité peut poser des problèmes de résilience[35]. Par ailleurs, le fait que les transactions surviennent hors de tout registre public (seuls les concernés conservent une trace des transactions qui les concernent) complique d'éventuels audits, notamment en cas d'allégations de fraude, et favorise le blanchiment de capitaux (*cf.* section 2 de l'annexe V).

**En troisième lieu, les solutions dites de *sharding* (« éclatement ») consistent à répartir les opérations entre plusieurs *blockchains*.** La *blockchain* grand public de premier niveau, historique (tels que la *blockchain Bitcoin* créée en 2009 ou la *blockchain Ethereum* créée en 2014), est qualifiée de « *blockchain*-phare » (*beacon* ou *layer 1*). D'autres opérations sont ensuite réalisées sur des « chaînes latérales » (*sidechains*), qui forment le *layer 2*.

Ces *sidechains*, parce qu'elles n'ont pas la prétention d'être des registres aussi décentralisés, ouverts et grand public que la chaîne de *layer 1*, arbitrent en faveur d'une plus grande scalabilité en renonçant à la décentralisation ou à la sécurité. Il peut par exemple s'agir de *blockchains* dites « permissionnées », dans lesquelles seul un petit nombre d'acteurs prédéterminés ont la possibilité de réaliser des transactions (*cf.* encadré 6). Elles peuvent également reposer sur un protocole de preuve de travail ou de preuve d'enjeu ayant un coût d'accès allégé.

En recourant à un tiers de confiance pour créer un « *bridge* » (*cf.* encadré 3 de l'annexe II), les jetons peuvent ensuite être déplacés de l'une à l'autre des chaînes lorsque cela est jugé nécessaire.

**Une technologie peut enfin combiner des aspects de plusieurs des principes précédents**, par exemple un *rollup* peut être utilisé pour agréger sur le *layer 1* les transactions ayant eu lieu sur une *sidechain*.

[35] Par exemple, le protocole prévoit dans certaines situations que les utilisateurs connectés à travers un canal doivent rester joignables en permanence. Lorsqu'un utilisateur cesse d'être joignable, il est difficile de déterminer si cela est lié à une défaillance du réseau ou à un comportement non coopératif devant entraîner sanction.

### Encadré 6 : Les *blockchains* « permissionnées » (privées ou de consortiums)

Les *blockchains* telles que *Bitcoin* et *Ethereum*, conçues pour que n'importe quel utilisateur puisse en principe prendre part à la validation des transactions, sont dites « publiques ».

Par opposition, on qualifie parfois de « *blockchains* permissionnées » des registres distribués imitant les *blockchains* publiques mais sur lesquels le pouvoir de validation des transactions n'appartient qu'à quelques acteurs prédéterminés. Une *blockchain* permissionnée peut par exemple se fonder sur les mêmes logiciels et spécifications que la *blockchain Ethereum* : les ordres de transaction prendront la même forme que pour *Ethereum*, le registre pourra être lu avec les mêmes logiciels et les programmes autonomes prévus pour *Ethereum* pourront s'exécuter de la même façon.

En revanche, seuls les acteurs préalablement déterminés (un seul pour une *blockchain* privée, plusieurs pour une *blockchain* de consortium) interviendront pour valider les opérations, rendant inutile le recours à la preuve de travail ou à la preuve d'enjeu. **La confiance repose donc sur l'autorité des validateurs, présumée *a priori* :** entreprises, greffiers ou encore particuliers se connaissant et acceptant de se faire confiance entre eux.

Ces *blockchains* privées et de consortiums peuvent donc être vues comme des bases de données centralisées, le cas échéant partagées entre plusieurs acteurs, mais dont le principal intérêt est qu'elles sont rendues interopérables avec les *blockchains* publiques. Comme pour toute base de données, les administrateurs de la *blockchain* permissionnée peuvent enfin décider de rendre les informations figurant dans le registre publiques ou, au contraire, de restreindre leur accessibilité.

### Encadré 7 : Le *Lightning Network* de *Bitcoin*

Le *Lightning Network* est la principale solution déployée aujourd'hui pour contourner la limitation du nombre de transactions possibles sur *Bitcoin*. Il repose sur l'idée d'externaliser en dehors de la chaîne une partie des transactions en laissant aux utilisateurs le soin de maintenir des « ardoises » (au sens de comptes non apurés) entre eux jusqu'au dénouement.

**Canaux de micropaiement**

La brique de base du *Lightning Network* est le canal de micropaiements bilatéraux. Deux utilisateurs Alice et Bob peuvent décider d'ouvrir un « canal » entre eux leur permettant de passer des transactions hors-chaîne. Plus précisément, ils créent, par un *smart contract*, un séquestre dans lequel ils introduisent une somme d'argent correspondant à leur ardoise initiale, par exemple 1 ₿ chacun. La transaction de mise sous séquestre est écrite sur la chaîne, ce qui rend les fonds indisponibles sur le réseau *Bitcoin* classique. Le séquestre ne peut être levé qu'avec l'accord des deux parties.

Par la suite, Alice et Bob peuvent, hors de la chaîne, décider d'un commun accord de modifier leur ardoise dans le cadre d'un paiement. Si par exemple Alice envoie 0,1 ₿ à Bob, alors l'ardoise sera modifiée à 1,1 ₿ pour Bob et 0,9 ₿ pour Alice. Pour cela, ils échangent des **ordres de transaction signés** permettant à Bob de retirer 1,1 ₿ du séquestre et à Alice de retirer 0,9 ₿, mais s'astreignent à ne jamais diffuser sur la chaîne les ordres de levée du séquestre. Il n'y a donc pas de minage, de frais de transaction ni de délais de traitement. Sur le registre public, les fonds sont toujours sous séquestre, mais les patrimoines respectifs d'Alice et de Bob sont modifiés. Si, par la suite, Alice vire à nouveau 0,1 ₿ à Bob, ils échangent de nouveaux ordres de levées de séquestre (0,8 ₿ pour Alice et 1,2 ₿ pour Bob) et détruisent les précédents. **Un parallèle dans la vie réelle consisterait à ce qu'Alice et Bob s'échangent des reconnaissances de dettes successives, chacune remplaçant la précédente.** Ils peuvent échanger par leur canal tant qu'aucun des deux ne devient endetté : les ardoises doivent toujours rester positives.

La fermeture d'un canal intervient lorsqu'Alice ou Bob décide de se retirer, en diffusant le dernier ordre de transaction échangé (ce qui équivaudrait à forcer l'exécution d'une reconnaissance de dette précédente) : le séquestre est levé et les fonds redeviennent disponibles *on chain*. Toutefois, en théorie, Alice pourrait se montrer non coopérative et diffuser un ordre obsolète, correspondant à une situation plus avantageuse pour elle. Ainsi, dans l'exemple précédent, elle pourrait diffuser l'ordre de retrait de 0,9 ₿ qui ne tienne pas compte de la dernière transaction (ce qui équivaudrait à forcer l'exécution d'une reconnaissance de dette ancienne en reniant la parole donnée à Bob).

Toutefois, le programme autonome définissant le séquestre est codé pour prévoir un temps de contestation, pendant lequel Bob peut prouver une éventuelle fraude d'Alice. Supposons en effet qu'Alice essaie de retirer 0,9 ₿ du séquestre en diffusant l'ordre obsolète. À partir du moment où cet ordre est inscrit sur la chaîne (et est donc détectable par Bob), Alice doit attendre toute la durée de contestation pour pouvoir effectivement récupérer les fonds. Pendant ce temps, si Bob peut prouver l'existence d'un ordre plus récent, alors le programme autonome du séquestre lui attribue l'intégralité des fonds, incluant ceux qui appartiennent théoriquement à Alice. La tentative de fraude de cette dernière est donc sanctionnée par la perte de l'ensemble de ses dépôts.

**Réseau de canaux**

Dans le schéma qui précède, deux opérations sont diffusées sur la *blockchain* : l'ouverture du canal et sa fermeture. Tous les autres échanges sont instantanés et sans frais.

Cependant, il ne présente aucun intérêt d'ouvrir un canal pour réaliser une seule transaction. L'idée du *Lightning Network* consiste à interconnecter ces canaux. Supposons par exemple qu'Alice souhaite envoyer 0,15 ₿ à David, mais n'ait pas de canaux ouverts avec lui. Si elle a un canal ouvert avec Bob, qui lui-même a un canal ouvert avec Charlie, qui lui-même a un canal ouvert avec David, alors la transaction peut avoir lieu en modifiant les trois ardoises, comme indiqué dans le tableau suivant (chaque ligne représentant un canal propre) :

| **État initial** | | | | **Après envoi de 0,15 ₿ par Alice à David** | | | |
|---|---|---|---|---|---|---|---|
| Alice | 2,10 | 0,50 | Bob | Alice | 1,95 | 0,65 | Bob |
| Bob | 0,15 | 0,75 | Charlie | Bob | 0,00 | 0,90 | Charlie |
| Charlie | 1,50 | 4,00 | David | Charlie | 1,35 | 4,15 | David |

Le patrimoine global de Bob et Charlie n'est pas modifié, mais l'état de leur ardoise avec chacun de leurs correspondants l'est. La définition des programmes autonomes assurant le séquestre assure qu'aucun des intermédiaires ne peut frauder en détournant les fonds reçus. Par ailleurs, le protocole *Lightning Network* peut être mis en œuvre de façon à rendre les transactions réellement anonymes : il est possible de faire en sorte que Bob et Charlie ignorent quelle est l'origine et la destination des flux dont ils sont intermédiaires. S'en suivent de sérieux enjeux en matière de lutte anti-blanchiment (*cf.* section 2 de l'annexe V).

À l'issue de cette transaction, David peut laisser les 0,15 ₿ qu'il a reçus dans le canal d'échange avec Charlie et aura la possibilité de les dépenser à nouveau (en utilisant Charlie comme intermédiaire). Il peut aussi fermer le canal ouvert avec Charlie pour récupérer *on chain* les 4,15 ₿ dont il dispose (incluant les 0,15 ₿ envoyés par Alice).

À noter qu'à la suite de ces opérations, Bob ne peut plus envoyer d'argent à Charlie par son canal. La transaction n'aurait pas pu avoir lieu par cette « route » si Alice avait cherché à envoyer à David une somme supérieure à l'encours dont disposait Bob dans son canal avec Charlie. **Le fonctionnement du réseau suppose donc qu'un niveau de liquidités suffisant soit garanti** pour qu'il existe toujours des « routes » entre les personnes souhaitant échanger un montant donné. Ainsi, pour le bon fonctionnement du réseau, des utilisateurs acceptent d'ouvrir un grand nombre de canaux et d'y placer des liquidités importantes. Le protocole permettra, à l'avenir, que les intermédiaires reçoivent une rémunération proportionnée aux montants déplacés, permettant de rentabiliser les bitcoins immobilisés pour le fonctionnement du réseau.

Du point de vue de l'utilisateur, l'ensemble de ces opérations sont gérées par son logiciel de portefeuille, sous réserve qu'il soit compatible avec le *Lightning Network* – c'est, en 2023, le cas de la majorité des portefeuilles grand public. L'utilisateur doit autoriser les ouvertures et fermetures de canaux (inscrits sur la *blockchain* et qui emportent donc des frais de transaction) et les montants avec lesquels il initialise lesdits canaux, qui sont séquestrés et rendus inutilisables sur le *layer 1 Bitcoin* en attendant la fermeture. Si, à l'avenir, les intermédiaires choisissent de demander des frais de transaction, alors les logiciels de portefeuille auront aussi pour objet de rechercher les « routes » les plus économiques au sein du réseau.

*Source : Joseph Poon et Thaddeus Dryja,* The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*, 2016 (livre blanc du* lightning network*).*

### 4.2. Même les solutions conçues pour être décentralisées font face à des phénomènes de concentration, ce qu'illustrent par exemple les coopératives de mineurs de *Bitcoin*

Le « trilemme de la *blockchain* » montre qu'un arbitrage est toujours nécessaire entre décentralisation, sécurité et scalabilité. Toutefois, **même des technologies conçues dans l'optique d'un haut niveau de décentralisation peinent à tenir leur promesse**, notamment en raison des fortes économies d'échelle qui incite naturellement à la centralisation.

En ce sens, un premier constat empirique peut être réalisé au sujet de *Bitcoin* : bien que le protocole de preuve de travail soit conçu pour permettre à toute personne de participer au minage et de gagner une récompense avec une probabilité de succès proportionnelle à la puissance de calcul mise à disposition, donc potentiellement très faible mais non nulle, **les mineurs se regroupent en pratique en « coopératives » concurrentes**.

Ces regroupements sont motivés par une logique d'économies d'échelle. En effet, la probabilité pour chaque mineur ou coopérative de miner un bloc, à supposer qu'il ait correctement réalisé le travail de validation, est proportionnelle à la puissance de calcul exprimée en nombre de *hashes* par seconde (*hashrate*). Les *hashrates* des différents mineurs d'une même coopérative s'ajoutent, tandis que leur travail de vérification et de conservation de l'historique des transactions est dupliqué. Il est donc économiquement profitable pour les mineurs de mutualiser le travail de validation *stricto sensu* en le confiant à un seul d'entre eux et de se concentrer sur la recherche de *nonces* permettant le minage de nouveaux blocs — et l'obtention de récompenses. Incidemment, la formation de coopératives permet des économies d'échelle sur la gestion matérielle du parc de minage (fabrication, livraison, installation, refroidissement, négociation de prix d'électricité de gros, *etc.*) et une mutualisation du gain, donc une réduction de la variance de la rentabilité sans modifier son espérance.

**Ainsi, en pratique, en février 2023, le minage sur *Bitcoin* est fortement dominé par cinq coopératives de mineurs** qui cumulent plus de 85 % de la puissance de calcul. Parmi celles-ci, deux (*Foundry USA* et *AntPool*) cumulent un peu plus de 51 % de la puissance de calcul (*cf.* graphique 1), ce chiffre étant en hausse continue depuis le début de l'année 2023. Or, la maîtrise de plus de 50 % de la puissance de calcul sur un réseau rend en principe possible une prise de contrôle qui ne peut pas être évitée sans intervention extérieure à la *blockchain*[36] (*cf.* 2.2.2).

Dans la mesure où la vérification de la validité des transactions n'est le plus souvent pas réalisée par chaque mineur individuellement, mais mutualisée à l'échelle de la coopérative et donc potentiellement concentrée sur peu de machines, la corruption de la chaîne s'en trouve facilitée : il suffit pour cela d'attaquer l'un des points de concentration.

D'un point de vue historique, l'existence de coopératives puissantes ne constitue pas une nouveauté ; les coopératives dominantes évoluent par ailleurs régulièrement au cours du temps. *Foundry USA* représentait ainsi moins de 1 % du *hashrate* en 2020, tandis que GHash.io, qui représentait 36 % du *hashrate* en juin 2014, a aujourd'hui disparu[37]. La concentration à un instant donné constitue cependant une faiblesse du réseau.

[36] Par l'exclusion des attaquants ou par la réalisation d'une scission.

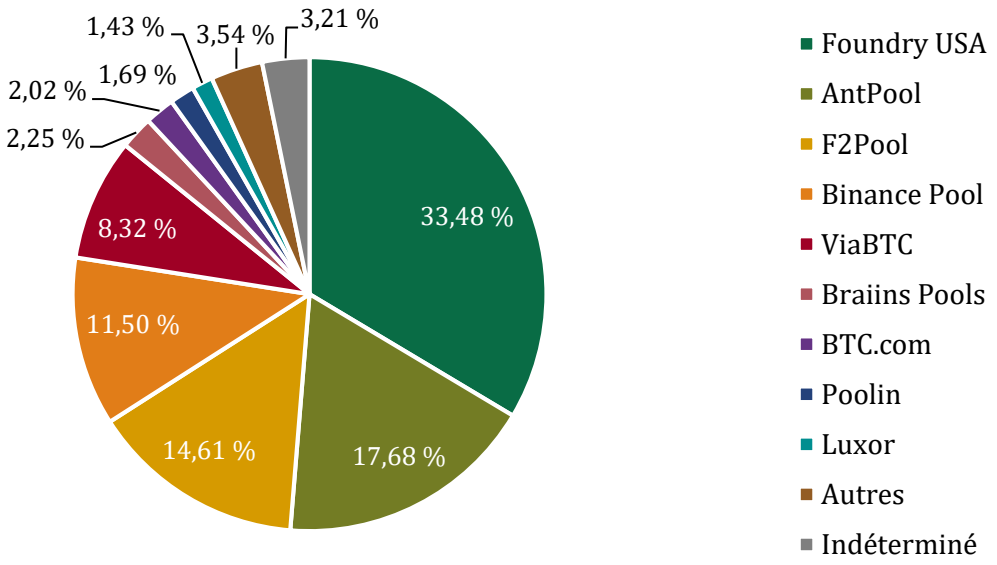
[37] Historique de la répartition du nombre de blocs minés par coopératives sur BTC.com (https://btc.com/stats/pool?percent_mode=latest#pool-history, consulté le 30 mars 2023).

**En ce qui concerne *Ethereum*, un phénomène similaire est observé, bien que son ampleur soit, en mars 2023, moindre.** Pour *Ethereum*, la puissance respective des coopératives se mesure par le nombre de « validateurs » qu'elles exécutent, c'est-à-dire par le nombre de programmes de validation lancés, chacun supposant d'avoir immobilisé 32 Ξ (*cf.* 4.1.3.1). Le potentiel cumulé de validation des cinq premières équipes de *staking* représente 48 % du total du réseau (*cf.* graphique 2).

La concentration du potentiel de validation du réseau *Ethereum* s'explique en partie par les raisons théoriques inhérentes au modèle du *staking* présentées en 4.1.3.1 et en partie par la réduction de variance dans la rentabilité des investissements. Il n'existe en revanche pas d'économies d'échelle liées à la gestion matérielle du minage (fabrication des mineurs, achat d'électricité, *etc.*). **Il est par ailleurs significatif que, parmi les cinq équipes les plus importantes, deux (Kraken et Binance) soient des plateformes d'échange, disposant des liquidités de leurs utilisateurs.**

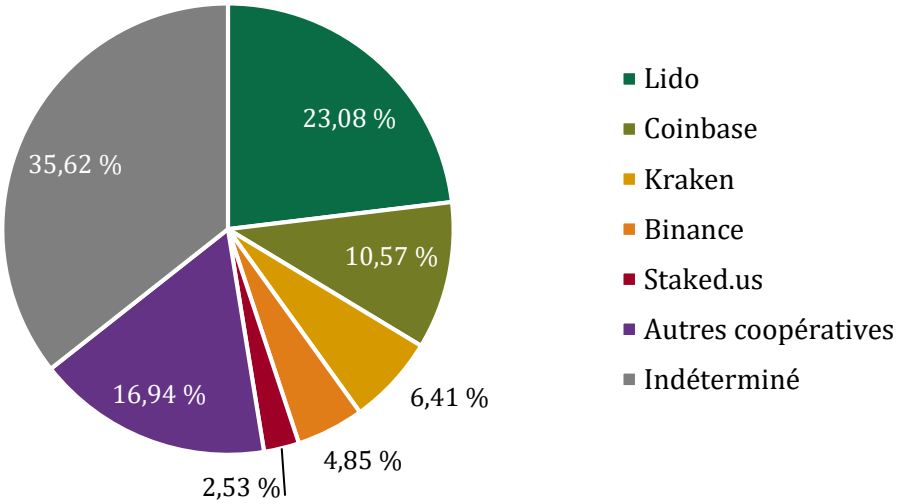
**Le potentiel réel de décentralisation de certaines technologies émergentes est par ailleurs inconnu.** Ainsi, en ce qui concerne le *Lightning Network*, présenté comme solution décentralisée au problème de scalabilité de *Bitcoin* (*cf.* encadré 7), il est incertain que la contrainte de liquidité nécessaire au bon fonctionnement du réseau puisse être résolue autrement que par l'apparition de quelques « nœuds dominants », c'est-à-dire des participants au réseau fournissant des liquidités importantes et acceptant d'ouvrir un très grand nombre de canaux avec des tiers, qui demanderont une rémunération pour ce service.

**Graphique 1 : Répartition de la puissance des coopératives de mineurs de *Bitcoin* en février 2023**




*Source : Répartition du nombre de blocs minés par coopérative en février 2023, données historiques de BTC.com (https://btc.com/stats/pool?percent_mode=latest#pool-history, consulté le 30 mars 2023).*

**Graphique 2 : Répartition des montants immobilisés par des coopératives de *stakers* sur *Ethereum* au 30 mars 2023**




*Source : Répartition du nombre de validateurs par coopératives de* staking *au 30 mars 2023, données beaconcha.in (https://beaconcha.in/charts/pools_distribution, consulté le 30 mars 2023).*

## 4.3. La pertinence même d'un système complètement décentralisé repose sur des hypothèses qui sont le plus souvent contestables

### 4.3.1. La décentralisation et l'immuabilité des transactions ont pour conséquence une négation de l'ordre public

Le fait que les registres soient fondés sur des protocoles de confiance décentralisés implique que des contraintes extérieures à la *blockchain* ne peuvent pas être intégrées de force dans celle-ci.

Ainsi, il est totalement impossible pour l'institution judiciaire de forcer l'application de la loi. En particulier, un juge ne peut pas prononcer l'annulation d'une transaction qui conduirait à la perte définitive de jetons (brûlés ou séquestrés de façon irréversible dans un programme autonome). Il ne peut pas non plus annuler un contrat mis en œuvre par l'exécution d'un programme autonome qui contreviendrait à l'ordre public, par exemple parce qu'il comprendrait des clauses illicites ou qu'il serait entaché d'un vice du consentement, et peut seulement ordonner des dommages et intérêts. Les seules possibilités d'arbitrage au sein d'une *blockchain* supposent que les utilisateurs y aient consenti, par exemple en intégrant des fonctions d'annulation dans le code source d'un programme autonome. **De tels effets, bien que problématiques en matière de respect de l'État de droit, sont recherchés, dans une perspective libertarienne, par certains promoteurs des *blockchains*.**

### 4.3.2. Dans la mesure où l'exécution des droits repose presque systématiquement sur des tiers de confiance identifiés, la pertinence d'un modèle totalement décentralisé est contestable

*Bitcoin* a été développé comme une proposition de solution à un problème spécifique, à savoir celui de la défiance envers les États et les banques centrales pour gérer correctement la monnaie (*cf.* 2.3). La solution adoptée repose donc sur une décentralisation, une transparence et une traçabilité complètes. Cependant, peu de cas d'usage des *blockchains* supposent d'aussi fortes contraintes, en particulier les usages impliquant des « *smart contracts* » ou des jetons représentant des droits sur des tiers (*cf.* annexe II).

Il en va ainsi des jetons qui représentent des créances (financières ou sous la forme de prestations de service) vis-à-vis de tiers. En effet, les tiers débiteurs constituent des points de centralisation critiques dans la chaîne de confiance : le dénouement d'une transaction devra donc *quoi qu'il en soit* les impliquer. Le détenteur du jeton-créance devra donc *quoi qu'il en soit* accepter de faire confiance au débiteur pour exécuter ses obligations.

Lorsque le jeton représente une « possibilité technique » (*cf.* section 2 de l'annexe IV), par exemple la possibilité d'utiliser un objet numérique dans un jeu vidéo ou dans un métavers, le tiers de confiance centralisé est l'éditeur du jeu vidéo ou du métavers en lui-même : il est nécessaire d'avoir confiance dans le fait que le comportement attendu pour le détenteur du jeton (accès à un niveau, détention de l'objet, *etc.*) aura bien lieu. Si le jeton représente un titre sur un bien ou un certificat d'authenticité, c'est l'émetteur qui doit être digne de confiance — il pourrait émettre un jeton représentant des droits qu'il n'a pas ou présentant comme authentique un objet qui ne l'est pas.

De même, s'agissant des « *smart contracts* » reposant sur des conditions survenant *off chain*, dans la vie réelle (par exemple un contrat d'assurance ou un contrat de titrisation), il est nécessaire qu'un tiers de confiance, appelé oracle, introduise *on chain* une trace des événements. Les personnes acceptant de faire confiance « à la *blockchain* » pour la bonne exécution du programme doivent en fait précédemment accepter la prémisse selon laquelle l'information introduite par l'oracle est correcte : cet oracle constitue donc un tiers de confiance critique.

En matière d'identité numérique, le tiers de confiance critique est toujours en dernier ressort une personne habilitée à certifier une identité reconnue comme authentique : l'État civil pour l'identité des personnes physiques, le greffe du tribunal de commerce pour l'identité des personnes morales.

Enfin, en tout état de cause, **l'institution judiciaire constitue toujours un tiers de confiance ultime**, car elle a vocation à trancher les différends éventuels dans le cas où l'un des tiers de confiance de premier niveau serait défaillant. Elle est ainsi responsable de forcer l'exécution des transactions, d'annuler celles qui seraient intervenues en violation des principes d'ordre public, d'ordonner la réparation des préjudices causés ou en encore d'établir la vérité judiciaire.

**L'hypothèse d'une décentralisation maximale ignore donc le caractère inévitable de ces intermédiaires de confiance critiques.**

**Ainsi, la totalité des cas d'usage rencontrés par la mission** — qui s'est concentrée sur les utilisations non financières des jetons — **ne supposent pas la décentralisation du système. Leur utilisation des *blockchains* est en réalité principalement fondée sur l'interopérabilité technique liée à une standardisation apparue *de fait* et sur l'effet de mode accompagnant ces technologies.**

### 4.4. Le gain en maturité des technologies liées à la *blockchain* pourrait conduire à mieux distinguer la fonctionnalité de registre et celle de création de confiance *ex nihilo*

Puisque l'hypothèse de décentralisation totale fait obstacle à un développement à grande échelle sauf à diminuer la sécurité des systèmes, qu'elle est en pratique très difficile à atteindre et qu'elle repose sur des hypothèses contestables autant en théorie (persistance de points critiques de centralisation dans les chaînes de confiance) qu'en pratique (concentration observée des mineurs), deux axes de développement technologiques sont principalement suivis à l'heure actuelle :

- un axe consistant à conserver cette hypothèse de décentralisation forte pour une finalité limitée, à savoir la fonction monétaire à l'origine du projet *Bitcoin* ;
- un second axe acceptant au contraire de transiger sur le niveau de décentralisation.

Le premier axe, soutenu principalement par les partisans de l'école de pensée libertarienne, se concentre sur le développement de *Bitcoin* et du *Lightning Network* pour les transactions de montant limité. Il refuse la dissociation de la finalité du registre (les transactions monétaires) et la preuve de travail, puisque l'intérêt même de l'unité monétaire sous-jacente au registre repose, pour ses promoteurs, sur la création de confiance *ex nihilo* dans sa stabilité et dans sa valeur.

Le second axe est principalement suivi par *Ethereum*, dans le cadre du projet « *Ethereum 2.0* » engagé en 2020. Celui-ci a conduit dans un premier temps à éliminer la preuve de travail et développer le *sharding*. *Ethereum*, contrairement à *Bitcoin*, ne se conçoit plus principalement comme un système monétaire, mais avant tout comme un **registre programmable**. Dans leur communication publique, les promoteurs d'*Ethereum* distinguent désormais complètement la finalité de registre ouvert et la question de la validation des opérations qui y sont inscrites d'une part, de la question de la création de confiance d'autre part. La validation des opérations a vocation à être opérée de différentes façons et à consommer des ressources plus ou moins intenses en fonction de leur sensibilité : dans le cadre du *sharding*, des *sidechains* contrôlées par un acteur centralisé peuvent être envisagées, par exemple pour les échanges de jetons représentant des obligations pour lesquelles ce même acteur est un tiers de confiance critique. Cet arbitrage a permis de réduire fortement le coût énergétique des transactions et permet d'entrevoir une montée en puissance forte pour le système *Ethereum* dans son ensemble incluant les *sidechains*. Les promoteurs d'*Ethereum* communiquent sur une division par plus de 1 000 de la consommation d'énergie à l'occasion de la bascule vers le protocole de preuve d'enjeu et sur la possibilité de valider à terme 100 000 transactions par seconde.

Un débat persiste, entre les promoteurs de ces technologies, quant à l'intérêt respectif des deux axes de développement. La critique du second axe de développement repose en particulier sur une remise en cause de la plus-value réelle que présente une architecture complexe comme celle d'*Ethereum* par rapport à une recentralisation complète de la *validation*[38] du registre auprès d'un petit nombre d'acteurs de confiance : États, représentants de l'institution judiciaire ou encore nouvelle institution *ad hoc* sous contrôle public destinée à garantir l'intégrité des transactions de ce registre — sorte d'« institution notariale numérique ».

Ce débat s'accompagne, enfin, d'un désaccord terminologique quant à ce que doit recouvrir la notion de *blockchain* : soit, dans une acception large, un registre de transactions avec un protocole permettant d'arbitrer sur une version authentique, soit dans un sens plus strict, un registre nécessairement accompagné d'une capacité à créer de la confiance *ex nihilo* par un protocole au moins aussi fiable que la preuve de travail.

[38] Et uniquement de la validation : une telle recentralisation peut intervenir tout en laissant le registre accessible publiquement.

# ANNEXE II

# Principes de fonctionnement des jetons et des NFT

**Annexe II**

# SYNTHÈSE

Alors que la *blockchain Bitcoin* a été prioritairement conçue comme un projet de registre destiné à enregistrer des transactions en monnaie électronique décentralisé (*cf.* annexe I), d'autres *blockchains* développées par la suite ont permis de rendre le registre programmable. Autrement dit, sur ces *blockchains*, il est possible non seulement de réaliser des transactions dans une cryptomonnaie, mais aussi de concevoir et exécuter des programmes autonomes, improprement appelés « *smart contracts* ». *Ethereum* est la *blockchain* grand public la plus connue conçue à cet usage.

Un tel programme autonome, dont le code source est public, adopte un comportement entièrement déterministe et peut interagir avec les utilisateurs de la *blockchain*. Il peut être utilisé pour stocker sur la *blockchain* des données rendues inaltérables ou encore pour sécuriser une chaîne d'opérations financières telles qu'une session d'enchères ou un échange.

**Surtout, il comporte une mémoire permanente qui peut être utilisée comme un sous-registre de détention de « jetons ».** Dans un tel cas d'usage, la mémoire comporte une liste de balances[1] et le programme inclut des fonctions permettant de transférer des jetons, le cas échéant contre de la cryptomonnaie. Les spécifications d'*Ethereum* permettent une créativité importante dans la conception de programmes, par exemple pour autoexécuter des droits de suite sur les reventes de jetons (transfert d'une fraction du prix de vente à l'émetteur du jeton) ou pour créer des produits dérivés financiers complexes. La revente peut intervenir de gré à gré ou sur une plateforme, indépendamment de l'émetteur original. Les détenteurs des jetons sont donc parfois présentés comme « propriétaires » des droits associés.

Parmi les jetons, certains sont émis en un unique exemplaire, indivisible, distinct des autres et pouvant être suivi individuellement. **Un tel jeton est dit *non fongible* (en anglais, *non fungible token*, NFT).** Ce jeton est le plus souvent associé à diverses métadonnées ou à une ressource externe : lien vers une œuvre d'art disponible sur internet ou vers toute représentation d'un objet virtuel tel qu'un objet de jeu vidéo. Le détenteur du jeton est parfois présenté comme « propriétaire » de l'œuvre ou de l'objet.

Dans certains cas, les programmes autonomes permettent de mettre en œuvre des obligations auxquelles s'engagent mutuellement l'émetteur d'un jeton, son détenteur et d'éventuels tiers consentants. Par exemple, un programme autonome peut être conçu pour répartir des flux financiers et organiser un vote entre détenteurs de jetons d'une même série : le jeton est dans ce cas assimilable à une action d'une société dont la gouvernance intervient sur la *blockchain* (*on chain*). Toutefois, cette situation est assez rare : le plus souvent, les droits et obligations s'exécutent en dehors de la *blockchain* (*off chain*). Le détenteur d'un jeton peut par exemple accéder à un service tel qu'une place de concert (pour un NFT représentant son billet) ou encore avoir le droit d'être affiché comme mécène d'un projet (le NFT représentant alors une preuve de mécénat).

[1] C'est-à-dire l'état des comptes à un instant donné (indiquant qui possède quels jetons).

**Compte tenu de ce qui précède, la nature exacte des droits et obligations du détenteur d'un jeton relève d'une appréciation au cas par cas.** Elle est susceptible de dépendre de nombreux paramètres, tels que le contenu du programme autonome gérant les jetons, les éventuelles métadonnées auxquelles il renvoie, un contrat de vente *off chain* lié à l'émission, les conditions générales d'utilisation du site du vendeur ou encore l'intention des parties. De cette qualification dépend ensuite la réglementation applicable : code monétaire et financier si le jeton représente un actif financier (*security token*), règlement européen sur les marchés d'actifs numériques s'il représente des droits ou une valeur autres, code de la sécurité intérieure si le jeton donne accès à un jeu d'argent et de hasard, code de la consommation si le jeton est vendu par un professionnel à un consommateur, code de la propriété intellectuelle si le droit d'auteur est mis en jeu, *etc.*

Dans ce contexte, une difficulté majeure et transversale à tous les cas d'usage des jetons consiste en l'identification exacte des obligations réciproques des parties, voire parfois de la territorialité. Le flou constaté pour la plupart des jetons émis constitue un déséquilibre lourd entre l'émetteur et le vendeur. Par exemple, la présentation du détenteur d'un NFT comme le propriétaire de l'œuvre ou de l'objet associé est le plus souvent trompeuse. En outre, de nombreux jetons ne sont en fait représentatifs d'aucun droit opposable.

# SOMMAIRE

Les *blockchains* sont des systèmes technologiques permettant à un ensemble d'utilisateurs d'écrire et de maintenir un registre décentralisé dont toute personne peut obtenir une copie et qui évolue selon des règles définies à l'avance. Lancé en 2008, *Bitcoin*, dont le fonctionnement est exposé en annexe I, constitue la première expérimentation d'un tel système. Sur cette *blockchain*, le seul objet du registre était, initialement, de compiler des transactions dans une unité de compte *ad hoc* appelée le bitcoin entre des utilisateurs identifiés par une adresse. Un protocole complexe de création de consensus, appelé la preuve de travail (*proof of work*), permet aux participants à la *blockchain* (les « mineurs ») de contrôler collectivement la licéité des transactions sans avoir à se reposer sur une autorité centrale (*cf*. annexe I). *Bitcoin* a donc été pensé comme une monnaie décentralisée et potentiellement désintermédiée.

L'idée de disposer d'un environnement totalement décentralisé est pourtant susceptible, en théorie, d'avoir une utilité dans d'autres domaines que la monnaie. Pour accroître les possibilités techniques des *blockchains*, une idée a consisté à rendre les registres *programmables*.

## 1. *Ethereum* permet l'exécution de programmes autonomes sur la chaîne, autorisant entre autres l'émission de nouveaux types de jetons

Conçue en 2014, la *blockchain Ethereum* repose à l'origine sur des principes similaires à ceux de *Bitcoin* décrit en section 2 de l'annexe I[2]. La cryptomonnaie de la chaîne, utilisée pour récompenser les personnes validant les transactions, est appelée l'éther (symbole ETH ou Ξ). L'économie de l'éther diffère de celle du bitcoin par plusieurs aspects : le stock de cryptomonnaies pouvant être mis en circulation est illimité (avec un maximum de 18 millions d'éthers supplémentaires par an), chaque éther peut être divisé en davantage d'unités (jusqu'au milliardième de milliardième d'éther, le *wei* : 1 Ξ = $10^{18}$ w) et un nouveau bloc est produit toutes les douze secondes en moyenne. Le processus de création de consensus, originellement identique à celui de *Bitcoin*, a par ailleurs été remplacé par étapes par un processus de preuve d'enjeu (*proof of stake*), la transition étant achevée depuis fin 2022. Cette différence, sans enjeu significatif pour la présente annexe, est discutée en section 4 de l'annexe I.

### 1.1. La *blockchain Ethereum* permet l'utilisation de *smart contracts*, c'est-à-dire de programmes autonomes exécutés sur la *blockchain*

La principale innovation d'*Ethereum*, du point de vue de l'utilisateur final de la *blockchain*, est que les opérations pouvant être enregistrées sur la chaîne ne sont pas limitées à de simples transactions de nature bancaire (ordre de transfert de fonds d'un compte à un autre)[3].

[2] Les principales sources de cette section sont le livre blanc *d'Ethereum* (Vitalik Buterin, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*, 2014) et la documentation du langage de programmation *Solidity*.

[3] Il était possible, dès *Bitcoin*, d'utiliser la technologie pour passer des transactions représentant plus que de simples virements monétaires. Le protocole n'était cependant pas conçu à cette fin et les possibilités restaient donc limitées.

En effet, un utilisateur dispose de deux possibilités supplémentaires :

- il peut, d'une part, donner un ordre de **création d'un programme autonome sur la chaîne**. Un tel programme se compose d'un certain nombre de fonctions, qui reçoivent en entrée des paramètres et peuvent agir sur un espace mémoire. La chaîne d'instructions du programme est publique[4] et distribuée entre tous les participants à la *blockchain*, ce qui permet aux validateurs de la *blockchains* d'exécuter le programme. Il en va de même pour son espace mémoire à un instant *t* ;
- il peut, d'autre part, **interagir avec un programme autonome en *appelant* l'une de ses fonctions, c'est-à-dire en demandant aux validateurs de l'exécuter**.

Un tel programme autonome est qualifié de « contrat intelligent », en anglais *smart contract*. Cette appellation provient du fait que de tels programmes peuvent notamment être utilisés pour permettre l'exécution automatique des termes d'un contrat entre plusieurs parties. Ce n'est cependant que dans certaines conditions précises que le programme pourrait représenter un contrat entre plusieurs parties ; même dans ce cas, la qualification juridique reste incertaine. Par la suite, la mission privilégiera donc l'expression de **programme autonome sur *blockchain*** à celle de « *smart contract* »[5].

**Le programme autonome reçoit une adresse et peut interagir avec son environnement de la même façon qu'un utilisateur humain.** En particulier, le programme possède, comme un humain, un compte en éthers à son adresse. Il peut donc recevoir des transactions financières, conserver des éthers et en envoyer à d'autres. Il peut également émettre des « signaux », c'est-à-dire des messages publics destinés à être lus par tous. Enfin, il peut lui-même interagir avec les autres programmes en appelant les fonctions qui les composent.

Certaines fonctions peuvent être « payantes », c'est-à-dire que leur exécution implique le transfert d'une certaine somme d'éthers de l'appelant au programme. Lorsque l'une des fonctions du programme autonome est exécutée, le programme a accès à l'identifiant (c'est-à-dire l'adresse publique) de l'utilisateur qui l'a appelé, au montant en éthers passé au programme à cette occasion ainsi qu'à d'éventuelles informations qui lui sont envoyées.

En conséquence, **le programme autonome se comporte de la même façon qu'un utilisateur humain de la *blockchain*, mais son comportement est déterministe et entièrement transparent**. L'exécution du programme intervient dans le cadre du processus de validation du bloc : concrètement, pour traiter une transaction de type « appel de fonction d'un programme autonome » et l'intégrer au bloc, un validateur doit exécuter la fonction dudit programme, c'est-à-dire suivre une par une les instructions qui composent le programme et qui peuvent chacune manipuler des éthers ou altérer la mémoire du programme. Les frais de transaction sont proportionnés aux ressources (mémoire et temps de calcul) mobilisées pour l'exécution de chaque instruction ; ils sont qualifiés de « frais de gaz » (*gas fees*).

Il existe donc, sur la *blockchain Ethereum*, deux types de comptes et d'adresses :

- les **comptes à propriétaire externe** : les fonds détenus par ces comptes peuvent être transférés sur autorisation du propriétaire du compte, donnée par l'apposition d'une signature. Autrement dit, le compte est contrôlé grâce à l'usage de la clef privée ;

---

[4] La chaîne d'instructions dite « compilée » est destinée à être directement exécutée par les programmes chargés de valider les transactions sur *Ethereum* et est souvent inintelligible pour un humain. Le code source du programme écrit par son auteur et exprimé dans un langage intelligible peut être rendu public, mais cela n'est pas obligatoire.

[5] Une telle qualification est notamment cohérente avec la définition retenue par la Commission européenne dans la proposition de règlement du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données (*Data Act*), du 23 février 2022 : un *smart contract* désigne « *un programme informatique stocké dans un système de registre électronique, le résultat de l'exécution du programme étant enregistré dans le registre électronique* » (article 2, paragraphe (16)).

- les **comptes de programmes automatiques** (ou comptes de contrats) : les fonds détenus ne peuvent être transférés que dans le cadre de l'exécution du programme, conformément à la chaîne d'instructions communiquée à la création du compte.

**Le caractère déterministe des programmes automatiques implique en particulier que d'éventuelles erreurs de programmation puissent emporter des conséquences irréversibles** : il n'est *jamais* possible de « déboguer » le programme pour corriger les comportements erronés. Les seules modifications de l'état du programme et les seules transactions possibles sont celles qui étaient prévues à la conception du programme.

Les programmes autonomes sur *blockchain* peuvent être émis dans différents langages de programmation, le langage *Solidity* étant l'un des plus utilisés, en pratique, pour *Ethereum*.

**Encadré 1 : Exemple simple d'un programme autonome sur *blockchain* d'achat sécurisé**

Un exemple simple de programme autonome, proposé par la documentation du langage *Solidity*, est un programme de mise sous séquestre de fonds dans l'attente du déroulement d'une transaction (« double arrhes »). Ce programme est initialisé avec en mémoire les adresses publiques d'un vendeur et d'un acheteur. Le vendeur définit un prix de vente $p$ et active le programme en lui virant $2\times p$ (en éthers). Tant que l'achat n'a pas été confirmé, le vendeur peut récupérer ses $2\times p$ pour annuler la vente. L'acheteur confirme l'achat en virant au programme $2\times p$ également. À ce stade, les sommes sont consignées jusqu'au dénouement de la transaction. Ce dénouement intervient lorsque l'acheteur confirme bonne réception du bien : le programme vire alors $p$ à l'acheteur et $3p$ au vendeur. Chacune des deux parties a donc un bon intérêt au dénouement de la transaction.

Un tel programme ressemblerait, en version simplifiée et en pseudocode, à ce qui suit (les textes précédés de `//` sont ignorés lors de l'exécution et ne servent qu'à expliquer le code) :

```
contrat AchatConsigné {
    //Définition des variables en mémoire du programme
    variable nombre prix_vente;
    variable adresse vendeur;
    variable adresse acheteur;
    variable texte état ;

    //Cette fonction « payante », lorsqu'elle est appelée,
    //doit obligatoirement être accompagnée d'un montant en éthers
    fonction payante initialiser() {
        //Pour engager la transaction, le vendeur met sous séquestre une garantie
        //correspondant au double du prix de vente
        vendeur = ADRESSE_APPELANT;
        prix_vente = MONTANT / 2;
        état = "initialisé";
    }
    fonction annuler_transaction() {
        //Si l'une des conditions n'est pas remplie, alors l'appel
        //de la fonction échoue et ses effets sont ignorés
        condition (ADRESSE_APPELANT == vendeur) ;
        condition (état == "initialisé");
        envoyer_fonds(vendeur, 2*prix_vente);
        état = "annulé";
    }
    fonction payante confirmer_achat() {
        //Pour confirmer l'achat, l'envoyeur séquestre des arrhes correspondant
        //au double du prix de vente
        condition (MONTANT == 2*prix_vente);
        condition (état == "initialisé");
        acheteur = ADRESSE_APPELANT;
        état = "achat confirmé" ;
    }
    fonction dénouer_transaction() {
        condition (ADRESSE_APPELANT == acheteur);
        condition (état == "achat confirmé");
        envoyer_fonds(vendeur, 3*prix_vente);
        envoyer_fonds(acheteur, prix_vente);
        état = "dénoué";
    }
}
```

Concrètement, pour initialiser le contrat, le vendeur appelle la fonction **initialiser** et doit joindre un montant qui correspond à sa consignation. Il peut annuler et obtenir remboursement en appelant **annuler_transaction**. L'acheteur confirme l'achat en appelant **confirmer_achat** et en joignant la même consignation. Il lui appartient d'appeler **dénouer_transaction** lorsqu'il a reçu le bien.

L'intérêt de l'usage du programme autonome provient du fait qu'aucun autre mouvement de fonds que les quatre opérations précédemment décrits ne peut intervenir et que les fonctions ne sont exécutées que sous des conditions bien précises. En revanche, cela implique que des erreurs puissent potentiellement être irréversibles. Par exemple, si le vendeur envoie une somme d'argent au programme précédent alors que la transaction est déjà dénouée, alors cette somme est perdue à jamais : aucune fonctionnalité du programme ne permet de récupérer les fonds.

Compte tenu du grand nombre d'actions et d'interactions possibles entre comptes, les programmes autonomes sur *blockchain* offrent de nombreuses possibilités. Quelques exemples simples sont :

- un programme de stockage de données. Un tel programme, très simple, ne peut pas manipuler d'argent, mais possède seulement une case mémoire comportant des données stockées de façon permanente, par exemple à des fins de preuve ;
- un programme d'enchères. Un vendeur active le programme autonome avec une enchère minimale. Toute personne peut formuler une enchère ou rehausser son enchère précédente en adressant une somme au programme. À une heure prédéterminée, les enchères s'arrêtent, le vendeur reçoit la valeur de l'enchère la plus élevée et les autres participants sont remboursés ;
- un pari mutuel sur un événement extérieur. Le programme comporte notamment une fonction payante **miser** (avec en paramètre l'issue sur laquelle le joueur entend miser) et une fonction **répartir_gains** prenant l'issue constatée de l'événement en paramètre. Le code de la fonction **répartir_gains** définit la façon dont ces gains seront répartis selon l'issue. Par ailleurs, elle comporte une condition qui autorise une seule personne prédéterminée à l'appeler : cette personne est l'« oracle », c'est-à-dire celui qui fait entrer sur la *blockchain* une information sur l'état du monde réel (en l'espèce, l'issue de l'événement extérieur).

De tels programmes autonomes permettent de se passer d'un intermédiaire de confiance manipulant les fonds. Dans le programme d'enchères par exemple, le code du programme étant entièrement public, il n'existe pas d'incertitude sur le fait que les montants des enchères seront correctement réalloués aux participants. De même, dans le programme de pari, l'oracle n'a pas besoin de manipuler de fonds lui-même.

Dans ces exemples, il reste toutefois nécessaire de faire confiance à des acteurs particuliers. Dans le premier, en effet, il est nécessaire de s'assurer que le vendeur délivrera *physiquement* le bien ou le service qui a fait l'objet de l'enchère. Dans le second, l'oracle doit être supposé honnête.

## 1.2. Des programmes autonomes sur *blockchain* permettent de créer des « jetons » virtuels dont le registre des « propriétaires » figure sur la chaîne

**Parmi les applications simples des programmes autonomes, figure la possibilité de créer, au sein-même de la *blockchain Ethereum*, des « sous-registres » identifiant les titulaires d'une famille de « jetons ».** Un jeton est un objet numérique, sans réalité autre que l'identification informatique d'un titulaire par un programme autonome sur *blockchain,* auquel peuvent éventuellement être associés des droits.

Un tel programme dispose, en mémoire, d'une structure de données permettant d'associer une balance (au sens d'état de propriété) à des adresses. **balance[addr]** désigne la balance de l'adresse **addr** pour le jeton considéré. Pour pouvoir utilement représenter des jetons cessibles, le programme autonome doit notamment comporter des fonctions permettant de :

- émettre de nouveaux jetons (***mint***), c'est-à-dire augmenter unilatéralement la balance d'une adresse ou, autrement dit, le nombre de jetons associés à l'adresse. La personne ayant le droit d'activer cette fonction est appelée le *minter* ;
- transférer des jetons. Cette opération prend la forme d'une fonction de transfert de jetons ayant pour paramètres un destinataire et un montant. La fonction augmente la balance du destinataire du montant et diminue la balance de l'émetteur de la transaction de ce même montant, sous réserve que la balance de l'émetteur le permette.

Comme les transactions du réseau *Bitcoin*, ces écritures sont performatives : le seul fait d'exécuter les fonctions d'émission et de transfert revient effectivement à émettre ou transférer des jetons.

L'intégrité des transactions est garantie par le code du programme autonome et par le processus de validation des transactions, qui ne peut intervenir que si le validateur a correctement exécuté la suite d'instructions qui correspond au code.

Une fois ces jetons définis, il est possible d'effectuer des échanges de valeurs de façon sécurisée, *via* un mécanisme de consignation[6]. Ainsi, si Alice souhaite envoyer 19 jetons à Bob contre 3 Ξ, elle peut créer un programme représentant un contrat de vente, qui aura par exemple l'adresse `0xc09712a7`. À la création, elle peut transférer 19 jetons au programme, c'est-à-dire exécuter la fonction **transférer_jetons**(`0xc09712a7`, 19). Le programme comporte par ailleurs une fonction payante **exécuter_vente** ne pouvant être appelée que par Bob, supposant que Bob paye au moins 3 Ξ (c'est-à-dire transfère 3 Ξ à l'adresse `0xc09712a7`) et exécutant à la suite deux transferts indissociables : celui des jetons à Bob et celui des éthers à Alice.

Pour faciliter l'interopérabilité des jetons, un standard, intitulé ERC20, définit des règles de programmation des registres de jetons. Pour respecter ce standard, le programme jouant le rôle de registre doit comporter certaines fonctions dont le nom et le comportement sont définis. Lorsque le standard est respecté, la plupart des logiciels de « portefeuille » présentent les jetons comme étant *dans* le « portefeuille » de l'utilisateur, au côté de ses éthers et des éventuels autres types de jetons.

Du moment qu'il respecte les spécifications minimales du standard ERC20, le programme peut comporter de nombreuses fonctionnalités supplémentaires. Typiquement, la fonction de transfert (qui, dans le standard, porte le nom ***transfer***) peut être, dans le respect du standard ERC20, modifiée pour mettre en pratique un « droit de suite », c'est-à-dire le versement automatique d'une partie des frais de transaction à un portefeuille donné, à chaque cession du jeton. Elle peut également être conçue pour n'autoriser qu'un nombre limité de transferts dans la vie de chaque jeton, *etc.*

Les possibilités ouvertes par les programmes autonomes sur *blockchain* ne sont cependant pas limitées à l'émission de jetons, ni *a fortiori* au standard ERC20.

[6] En réalité, le standard ERC20 prévoit un mécanisme légèrement différent de celui présenté. Le programme « contrat de vente » (`0xc09712a7`) ne se voit pas transférer les jetons, mais Alice indique au programme « jetons », *via* une fonction **allow**, qu'elle autorise le programme « contrat de vente » à manipuler jusqu'à 19 jetons pour son compte.

**Encadré 2 : La destruction et la mise sous séquestre de jetons**

Les jetons ERC20 n'ayant pas d'existence physique, il n'est pas possible de les « détruire ». Il serait envisageable de sortir des jetons de la circulation en réduisant la balance d'un compte sans augmenter celle d'un autre en contrepartie. Cependant, le mode opératoire retenu est plutôt la consignation irréversible : un jeton est envoyé à l'adresse `0x00000000`, dont personne ne possède la clef privée. Un tel jeton est dit « brûlé » (*burn*), c'est-à-dire retiré de la circulation.

Une mise sous séquestre (*escrow*) peut par ailleurs intervenir en transférant les fonds à un programme automatique dédié à cet effet, qui en devient propriétaire. Le séquestre peut être levé dans un second temps lorsque des conditions prévues par le code du programme sont remplies : ordre de mainlevée donné par une personne autorisée, intervention d'un paiement, *etc.* Lorsque la condition de levée survient en dehors de la *blockchain*, alors un tiers de confiance doit jouer le rôle d'oracle, c'est-à-dire garantir que la condition prévue s'est bien réalisée et donner l'ordre de mainlevée en conséquence.

**Encadré 3 : Le transfert de jetons entre deux *blockchains***

Plusieurs *blockchains* permettent de mettre en œuvre des programmes autonomes. En revanche, les interactions entre *blockchains* sont en principe impossibles, du moins pas dans le cadre des transactions sécurisées garanties par les processus de validation au fondement des *blockchains*. Par exemple, un programme autonome de la *blockchain Ethereum* ne peut pas transférer de jetons vers l'adresse d'un utilisateur de la *blockchain Tezos*.

Des programmes appelés « *bridges* » (ponts) peuvent permettre un transfert, mais ils nécessitent de faire confiance à un intermédiaire centralisé jouant le rôle d'oracle. Un *bridge* peut consister, par exemple, à d'abord brûler *n* jetons d'un utilisateur sur *Ethereum* puis à réémettre *n* jetons sur *Tezos*. Cependant, cette nouvelle émission doit n'intervenir que si la première étape a bien été exécutée. C'est donc le *minter* (personne ayant le droit d'émettre les nouveaux jetons) du programme autonome sur la *blockchain Tezos* qui certifie avant la nouvelle émission que la destruction préalable de jetons est bien intervenue : il joue le rôle d'« oracle », sur la *blockchain Tezos*, du fait que la destruction de jetons sur la *blockchain Ethereum* est bien advenue. Plutôt que de brûler les jetons sur *Ethereum*, le pont peut les séquestrer, ce qui permettra dans un second temps de rapatrier les jetons sur cette chaîne : l'oracle devra alors certifier qu'ils ont bien été retirés de la circulation sur *Tezos*.

Un tel exemple illustre la difficulté à se passer totalement d'intermédiaires de confiance pour l'interaction entre une *blockchain* et le monde extérieur à celle-ci.

## 1.3. La nature des droits dont bénéficient les titulaires des jetons ne peut être appréciée qu'au cas par cas

**Le standard ERC20 ne comporte aucune prévision quant à l'effet qu'a la détention d'un « jeton ».** Pour être conforme au standard ERC20, un programme autonome doit, en effet, simplement comporter certaines fonctions dont les noms et paramètres sont définis par le standard (par exemple, « connaître la balance d'un utilisateur », « transférer des jetons » *etc.*). Le comportement exact de ces fonctions et les droits associés à la détention des jetons ne sont pas définis par le standard.

Les programmes ont une double nature :

- d'une part, ils peuvent être comparés à l'*instrumentum* d'un contrat : il s'agit de supports permettant de formuler les droits et obligations (le *negotium*), mais l'usage du support est indépendant de ce que sont les droits et obligations. En particulier, le jeton ERC20 peut n'être le support d'aucun droit ni obligation, ou bien le support de droits et obligations illicites qu'un juge déclarerait nuls en cas de contentieux ;
- d'autre part, ils constituent une modalité d'exécution dudit contrat puisqu'ils permettent la mise en œuvre automatisée d'une partie des droits et obligations.

### 1.3.1. Les jetons peuvent être catégorisés selon la nature des droits qu'ils procurent

Une première classification possible des jetons repose sur la nature des obligations auxquels s'engagent l'émetteur et le détenteur. Ainsi :

- l'objet des jetons peut être la perception de flux financiers futurs, ce qui les assimile à des actifs financiers (jetons valeurs, *security tokens* – *cf.* encadré 4 pour un exemple de programme de titrisation) ;
- ils peuvent permettre la participation à la gouvernance de l'entité ayant émis les jetons ou d'un projet associé à l'émission (jetons de gouvernance, *governance tokens*) ;
- ils peuvent donner accès à un bien ou à un service fourni par cette entité, c'est-à-dire apporter une utilité (jetons utilitaires, *utility tokens*) ;
- ils peuvent avoir une contrepartie fixe, garantie par l'émetteur. Un jeton peut, par exemple, être convertible contre un euro. Dans ce cas, le jeton est destiné à être utilisé comme un actif représentant sa contrepartie sur la *blockchain* : il fait office de monnaie stable (*stablecoin*) ;
- plusieurs de ces caractéristiques peuvent coexister, par exemple dans le cas de jetons émis par une entreprise qui donneraient simultanément droit à des services futurs que fournira l'entreprise et à la participation aux décisions stratégiques concernant ces services ;
- enfin, certains jetons peuvent n'ouvrir aucun droit vis-à-vis d'une personne déterminée. Cette catégorie combine de nombreux autres types de jetons :
  - des jetons utilisés à des fins purement techniques pour représenter non pas des droits juridiques, mais des droits techniques vis-à-vis d'un système informatique ou d'une entité décentralisée (jetons de protocoles),
  - des supports alternatifs d'échange dépourvus de parité fixe avec une autre contrepartie (contrairement aux *stablecoins* dont le cours est fixé par une garantie de convertibilité). Cette catégorie inclut en particulier certaines monnaies de jeux vidéo,
  - des objets virtuels de collection (lesquels peuvent avoir une valeur potentiellement très spéculative).

Cette première classification a un caractère purement technique et informel : les ensembles précédemment définis ne sont pas des catégories juridiques bien définies. En outre, de nombreux jetons ont une nature mixte.

À noter que les cryptomonnaies de chaînes (bitcoin, éther, *etc.*) ne sont pas, d'un point de vue strictement technique, des jetons au sens de ce qui précède. En effet, leur gestion ne repose pas sur un programme autonome gérant leur stock, mais directement sur les règles de base de fonctionnement de la *blockchain*. Toutefois, d'un point de vue économique, ces cryptomonnaies de chaîne s'apparentent à des jetons de protocole, puisqu'elles donnent des droits techniques vis-à-vis de l'ensemble des utilisateurs de cette *blockchain* (droit de passer des transactions sur le stock de cryptomonnaies détenues, au moins).

**Encadré 4 : Un exemple simple de programme autonome de titrisation**

Un programme autonome de titrisation d'actifs peut par exemple être défini de la façon suivante :

- le programme agit comme une banque de jetons, c'est-à-dire qu'il respecte le standard ERC20 ;
- il reçoit une adresse, par exemple `0x0071712e` ;
- les flux financiers générés par le collatéral sont virés à l'adresse du programme `0x0071712e` ;
- à intervalles réguliers (chaque trimestre ou à la réception de chaque flux financier), le contrat `0x0071712e` retransfère les flux reçus aux détenteurs des jetons, au prorata du nombre de jetons détenus.

Les jetons du programme décrit précédemment constituent des titres adossés à un actif (*asset-backed securities*, ABS) très simples, représentatifs d'un droit de créance. Les flux associés à la détention du jeton peuvent par ailleurs eux-mêmes être à nouveau titrisés.

En revanche, une difficulté réside dans le fait d'assurer que les flux du collatéral seront bien versés au programme `0x0071712e`. Ce versement peut être automatisé sur la *blockchain* dans le cas où le flux est lui-même issu d'un autre programme (contrat de vente sur la chaîne, ABS adossé à un autre ABS, *etc.*). En revanche, s'ils sont issus du monde réel (dividendes associés à des actions, coupons d'obligations, *royalties* sur un bien immobilier, *etc.*), alors l'entrée des flux dans le système n'est pas garantie. Cette problématique illustre à nouveau la difficulté à faire interagir la *blockchain* avec le monde extérieur.

### 1.3.2. Une distinction fondamentale résulte dans le fait de savoir si les droits sont définis dans un programme autonome sur *blockchain* ou en dehors

Indépendamment de la classification par nature de droits, une distinction doit être faite selon que les droits et obligations conférés sont définis sur la *blockchain* ou en dehors de celle-ci :

- d'une part, il est possible qu'une partie des droits et obligations que confère la détention du jeton soient assurés automatiquement par l'exécution de programmes autonomes. Autrement dit, l'exécution des obligations réciproques intervient **sur la *blockchain* elle-même (« *on chain* »), par la mise en œuvre du programme autonome**. Cette situation peut par exemple se produire si un programme autonome sur *blockchain* est utilisé à des fins de titrisation (il est possible de prévoir automatiquement que les titulaires des jetons recevront une fraction des flux financiers – *cf.* encadré 4), pour autoriser la participation à un vote organisé directement sur la *blockchain* ou encore pour un programme d'enchères dont l'objet est le transfert d'un jeton inscrit sur la *blockchain* ;
- d'autre part, ces droits et obligations peuvent être **extérieurs à la *blockchain* (« *off chain* »)**. C'est le cas si le programme gère des jetons conférant le droit d'accéder à un service n'étant pas fourni sur la *blockchain*, tel qu'un concert, ou de se faire livrer un bien qui n'est pas un cryptoactif de cette même *blockchain*.

**Le fait que les droits et obligations soient définis *on chain* ou *off chain* a des conséquences significatives sur leur identification et sur la façon dont ils sont mis en œuvre, indépendamment de leur nature.**

Dans le cas où les droits et obligations sont définis *on chain*, la lecture du code source du programme autonome et le cas échéant des éventuels autres programmes auxquels il renvoie suffit en principe à connaître précisément les droits et obligations associés et à savoir de quelle façon ils seront exécutés. Le ou les codes sources des programmes, s'ils ont été rendus publics, peuvent alors être apparentés à des conditions générales de vente ou d'utilisation des jetons, autoporteuses. **Il peut alors être argué que l'achat des jetons constitue une approbation du contrat d'adhésion sous-jacent.**

Cette vision comporte toutefois certaines limites. En effet, le consommateur peut ne pas être capable de comprendre précisément la nature des engagements, ce qui affecte donc le caractère libre et éclairé du consentement. Par ailleurs, l'exécution du programme est automatique et ne peut pas être annulée : il est donc impossible, pour le juge du contrat, d'intervenir dans sa mise en œuvre, par exemple pour sanctionner une clause abusive ou une transaction obtenue par erreur, dol ou violence. La rétractation du consommateur est en outre impossible, sauf si le programme le prévoyait explicitement.

Au contraire, dans le cas où les droits et obligations sont *off chain*, leur définition n'est pas toujours certaine. Ainsi, au cours de ses investigations, la mission a rencontré de nombreuses entreprises ayant procédé à l'émission de jetons présentés comme associés à des droits *off chain*, sans que ces droits soient formalisés par un quelconque acte écrit, par exemple dans les conditions générales d'utilisation des services de l'entreprise les ayant créés. Une difficulté réside en particulier dans le fait que la créance associée à un jeton peut avoir été exécutée — c'est-à-dire que l'utilité peut avoir été « consommée » — sans que l'information figure sur la *blockchain*. C'est le cas, par exemple, si un jeton donne le droit à son détenteur de se voir livrer un bien physique une unique fois et si la livraison est intervenue auprès d'un précédent titulaire du jeton.

En outre, **dans le cas où les droits sont définis et exécutés *off chain*, les transactions intervenant sur la *blockchain* auront rarement un caractère performatif**. Supposons en effet qu'Alice réalise une opération économique *X* et émette 100 jetons, chacun représentant un droit pour le détenteur à 1 % du résultat de cette opération. Si Bob possède un jeton, alors il peut le donner à Charlie par une simple écriture sur la *blockchain* (appel de la fonction **transfer**). L'écriture, qui peut être interprétée comme signifiant « Bob transfère un jeton à Charlie », est performative. En revanche, elle ne peut pas être assimilée à une écriture « Bob transfère à Charlie 1 % des droits sur l'opération *X* » : il ne suffit pas, en effet, de l'écrire sur la *blockchain*, encore faut-il qu'Alice remplisse sa promesse de donner 1 % du résultat au détenteur de chaque jeton ou, à défaut, que l'exécution de cette obligation puisse être forcée par l'autorité judiciaire. Les obligations *off chain* supposent ainsi, pour être exécutées, des intermédiaires de confiance, à rebours du principe de décentralisation.

### 1.3.3. Les pouvoirs publics pourraient inciter ou imposer une plus grande transparence quant aux droits et obligations précis associés aux jetons émis

Le standard ERC20 et ses équivalents pour les *blockchains* autres qu'*Ethereum* ne prévoient aucune façon standardisée de définir les droits et obligations *off chain* associés à un jeton. Ainsi, **en cas de contentieux, la qualification exacte des droits et obligations associés à un jeton doit être déterminée au cas par cas et peut parfois dépendre de l'appréciation souveraine du juge** — étant précisé que l'identification de la juridiction compétente et de la loi applicable sont elles-mêmes source de difficulté. Cette situation est donc à l'origine d'une réelle insécurité juridique et d'un déséquilibre défavorable au détenteur du jeton, qui ignore l'étendue — ou plutôt l'étroitesse — de ses droits.

Ce déséquilibre apparaît difficile à résorber en toute généralité par des dispositions d'ordre public. Aussi :

- d'une part, la mission a-t-elle étudié la situation propre à différents cas d'usage des jetons et proposé des ajustements législatifs sectoriels. Ces propositions sont présentées :
  - dans un rapport distinct de l'Inspection générale des finances, « Donner un cadre juridique aux jeux à objets numériques échangeables » (n° 2022-M-062-02, janvier 2023), en ce qui concerne les jeux utilisant des jetons ;
  - en section 4 de l'annexe IV en ce qui concerne les NFT « artistiques » ;

- d'autre part, de façon transversale, les émetteurs de jetons pourraient-ils être incités, lorsqu'ils entendent donner aux jetons le caractère d'un titre de droit, à systématiquement associer au programme autonome (*on chain*) un document écrit[7] comportant une explication claire et en français des droits et obligations associés *off chain* ainsi que de la juridiction compétente pour connaître des conflits. Cette incitation pourrait par exemple intervenir dans le cadre d'un effort de normalisation (norme dérivée du standard ERC20) ou *via* une obligation pour les émetteurs ou les plateformes d'échanges de jetons de mettre en œuvre une telle fonctionnalité. Elle serait plus effective si elle intervenait sur l'ensemble du marché européen.

Sur ce dernier point, le projet de règlement européen sur les marchés de cryptoactifs (règlement MiCA) prévoit l'obligation d'émettre un livre blanc (*white paper*) à chaque émission de jetons couverts par le règlement, lequel doit notamment préciser les droits et obligations associés au jeton (*cf.* en particulier article 5(1)(d)).

**Toutefois, ce règlement a été conçu pour encadrer des cryptoactifs émis comme supports d'investissement ou comme solutions de substitution à des monnaies plutôt que des cryptoactifs conçus comme biens de consommation.** Ainsi, le formalisme du livre blanc s'inspire de celui exigé pour les prospectus à publier en cas d'offre au public de valeurs mobilières. Par ailleurs, cette obligation ne s'applique pas à de nombreux cryptoactifs destinés à la consommation, en particulier les *utility tokens*, les jetons non fongibles (*cf.* section 2 *infra*) et les jetons qui sont distribués à moins de 150 personnes dans chaque État membre ou qui représentent à leur émission une offre de moins de 1 M€ par an (*cf.* article 4).

Une intervention des pouvoirs publics pour imposer une communication sur les droits et obligations associés à chaque jeton, moins lourde que l'obligation du livre blanc, mais applicable à l'ensemble des jetons à vocation commerciale pourrait donc être justifiée (*cf.* section 2 de l'annexe IV).

[7] Ce document pourrait figurer dans la mémoire du programme. Cependant, pour des raisons de disponibilité de l'espace mémoire, en pratique, il serait plus simple de faire figurer un *hash* du document.

# 2. Les jetons non-fongibles (NFT) sont un type particulier de jetons ayant pour particularité d'exister en un unique exemplaire indivisible

## 2.1. Un NFT est un jeton émis en un unique exemplaire identifiable

Les jetons conformes au standard ERC20 sont indivisibles, mais sont la plupart du temps émis en plusieurs exemplaires. Ils sont conçus pour être *fongibles* : il n'est pas possible d'identifier individuellement les jetons. En effet, les transactions ne prennent pas la forme d'un déplacement de jetons un par un, mais seulement d'une variation des balances. En réalité, en dépit de leur dénomination, leur comportement n'est pas celui de jetons (unités physiques pouvant être suivies), mais s'apparente davantage à celui de comptes bancaires dans des unités *ad hoc*.

Il reste possible, pour un émetteur, de *minter* plusieurs séries de jetons comportant des propriétés différentes mais voisines. Par exemple, un programme autonome de titrisation peut prévoir trois tranches A, B et C de séniorités différentes et émettre trois séries de jetons compatibles ERC20 en conséquence, correspondant aux titres des trois tranches. Cependant, les jetons de chaque série restent bien, entre eux, fongibles.

Au contraire, un jeton non fongible (en anglais *non fungible token*, NFT) est rendu identifiable de façon individualisée. Les utilisateurs ne détiennent pas seulement une balance de jetons, mais chaque jeton est identifiable individuellement. Cette situation est identique au cas où un jeton de type ERC20 est émis avec une seule unité en circulation : à tout instant, au plus un utilisateur peut en être détenteur. Les détenteurs successifs peuvent ensuite être tracés au cours de la vie du jeton. Une telle situation peut par exemple correspondre au cas où le jeton est associé à un droit d'accès à une place de spectacle.

Rien n'interdit, par ailleurs, d'émettre des jetons similaires correspondant à des droits proches. Par exemple, 500 jetons correspondant à 500 places d'un même spectacle peuvent être émis et gérés par le même programme automatique :

- si chaque place donne droit à un siège donné, alors chaque jeton ouvre un droit distinct des autres et les jetons sont par nature non fongibles ;
- si le spectacle est à placement libre, alors les 500 jetons donnent les mêmes droits. Il est donc raisonnable de définir des jetons fongibles. Rien n'interdit non plus de maintenir une non-fongibilité entre ces jetons : cela est équivalent à, par exemple, numéroter les billets d'entrée à la salle de spectacle. En principe, le billet n° 4 a un usage identique au billet n° 465, bien qu'ils soient physiquement distinguables. Toutefois, un *fan* pourrait par exemple désirer posséder le billet portant le numéro 1 et être prêt à payer davantage pour le détenir : la non-fongibilité crée donc une unicité des objets, même si ceux-ci peuvent être ressemblants. Cette non-fongibilité peut être appréciée d'un point de vue technique (possibilité matérielle de distinguer les jetons) ou économique (attention portée par les acteurs économiques aux différences matérielles).

Sur *Ethereum*, le standard ERC721 définit les spécifications attendues pour un programme automatique de gestion de NFT. Les programmes autonomes conformes à ce standard peuvent en fait gérer non pas un unique NFT, mais une série de NFT, dont chacun porte un identifiant unique[8]. Tout NFT est donc identifié par deux éléments :

- l'adresse du programme automatique sur *blockchain* qui le définit ;
- le cas échéant, l'identifiant unique du NFT au sein de ce programme automatique.

[8] Un autre standard, le standard ERC1155, permet de gérer des jetons dits *semi-fongibles*, c'est-à-dire en réalité plusieurs séries de jetons qui sont fongibles au sein de leur série, mais dont les différentes séries sont non-fongibles entre elles.

Au minimum, **le programme de gestion du ou des NFT comporte donc en mémoire l'adresse du détenteur de chacun des jetons et propose des fonctions permettant de transférer la détention de ces NFT, dans des conditions similaires aux ERC20**. Autrement dit, le transfert d'un NFT implique seulement de changer l'adresse du détenteur inscrite dans la mémoire du programme autonome, ce qui ne peut être autorisé que par le détenteur actuel.

**La notion de fongibilité est en revanche difficile à définir précisément au-delà de cette approche technique.** Par exemple, des billets de banque libellés en euros sont en pratique fongibles, mais en théorie bien identifiables grâce à leur numéro de série ; de la même façon, deux jetons *techniquement* non fongibles peuvent devenir *économiquement* fongibles si les utilisateurs sont indifférents à leur identifiant exact.

Le projet de règlement MiCA comporte des considérants initiaux (considérants 10 et 11) sur les indices à prendre en compte pour définir la fongibilité, propriété qui sert de critère pour exclure les jetons non fongibles du périmètre du règlement. Ainsi, les jetons non fongibles sont écartés du règlement dans la mesure où l'absence de comparaison avec un marché existant limite la possibilité de les utiliser à des fins financières ainsi que les risques associés. **Les considérants écartent une définition technique de la non-fongibilité au profit d'une approche économique** : ils invitent les autorités nationales à se fonder sur une analyse concrète des fonctionnalités offerte par les cryptoactifs plutôt que sur la forme ou les apparences[9]. Le fait que des actifs aient été émis en grandes séries ou sous forme de collections ou que les droits et actifs sous-jacents soient eux-mêmes fongibles font entrer les cryptoactifs dans le champ du règlement. Selon la direction générale de la stabilité financière de la Commission européenne (DG FISMA), cette définition pourra être précisée par des actes délégués ultérieurs, mais la qualification dépendra *in fine* du juge du fond.

**Encadré 5 : Comparaison entre les principaux standards de définition de jetons sur la *blockchain Ethereum* : ERC20, ERC721 et ERC1155**

Les standards ERC (*Ethereum request for comment*) 20, 721 et 1155 constituent les trois principaux standards techniques définissant les jetons utilisés sur la *blockchain Ethereum*.

Le standard ERC 20 constitue la première norme de jetons. Un programme conforme à cette norme doit tenir dans sa mémoire une liste des adresses des détenteurs de jetons et le solde de chacun d'entre eux. Transférer des jetons consiste à réduire le solde du vendeur et à augmenter d'autant le solde de l'acheteur. Dans une telle situation, les jetons sont en principe fongibles : si un utilisateur détient deux jetons, il est impossible de les différencier.

L'ERC 721 vise uniquement les séries de jetons non fongibles, destinés à être différenciables. Le programme doit comporter dans sa mémoire une liste des jetons en circulation et, pour chaque jeton, l'adresse de son détenteur. Le transfert d'un jeton donné consiste à modifier l'adresse de son détenteur. À noter qu'il est équivalent de créer un programme ERC 721 pour un unique jeton et un programme ERC 20 dont le stock de jetons est plafonné à 1.

L'ERC 1155, enfin, permet la création de « jetons semi-fongibles ». Le programme autonome gère plusieurs séries de jetons, étant précisé que les jetons au sein d'une même série sont fongibles, mais que les jetons de séries différentes sont distinguables.

L'intérêt de disposer de telles normes est que certains programmes (sur *blockchain* aussi bien qu'*off chain*) peuvent traiter les jetons de façon abstraite, sans considération pour leurs spécificités. Par exemple, un programme destiné à automatiser la mise sous séquestre d'un jeton ERC20 appellera la fonction « transfert » de ce jeton, saura exactement quels paramètres passer à la fonction et dans quelle ordre, mais n'aura pas à se préoccuper du reste du fonctionnement du jeton (par exemple, si celui-ci implique le versement de frais financiers, ou encore des modalités selon lesquelles de nouveaux peuvent être émis). Ces standards favorisent donc l'interopérabilité des jetons.

[9] « *This Regulation should also apply to crypto-assets that appear unique and not fungible, but whose de facto features or features linked to de facto uses would make them either fungible or not unique. In this regard, when assessing and classifying crypto-assets, competent authorities should adopt a substance over form approach, under which the features of the asset in question should determine the qualification, not its designation by the issuer.* »

## 2.2. Les NFT sont le plus souvent destinés à représenter un bien virtuel unique, désigné par des métadonnées d'un programme autonome sur *blockchain*

D'un point de vue technique, tout jeton identifiable de façon individuelle constitue un NFT. Des jetons utilitaires (*utility tokens*), jetons de gouvernance (*governance tokens*) ou jetons-valeurs (*security tokens*), s'ils sont émis en un seul exemplaire, constituent donc par nature des NFT.

Toutefois, dans le cas d'usage le plus fréquent, les NFT « pointent » vers des données, dans un sens qui sera précisé ultérieurement. **Les promoteurs des NFT voient de cette façon dans le NFT un titre de propriété sur ces données ou sur ce qu'elles représentent — qualification juridique toutefois impropre et qui sera précisée par la suite.**

Un exemple simple est celui d'un NFT correspondant à une image. Le programme autonome sur *blockchain* qui gère ce NFT comprend alors deux cases mémoires :

- une première, immuable, qui peut contenir l'image — ou plus exactement sa représentation binaire (*cf.* section 1.1 de l'annexe I) ;
- une seconde qui contient l'adresse du détenteur actuel du jeton et qui peut être modifiée si le détenteur l'autorise dans le cadre d'une transaction.

Toutefois, en pratique, les frais associés à l'écriture de données *on chain* sont extrêmement élevés : en février 2023, la création d'une case mémoire d'un kilooctet de données (1 ko) sur *Ethereum* coûte 0,032 Ξ, soit environ 50 € au cours de ce même mois. L'inscription sur la blockchain d'une photographie de qualité intermédiaire coûterait donc plus de 200 000 € de « frais de gaz » au moment de la création. Aussi, **dans l'immense majorité des cas, la mémoire du programme autonome NFT ne contient pas l'image en elle-même, mais un lien internet pointant vers l'image**, par exemple `https://alice.com/images/chaton.jpeg`.

Le fonctionnement est similaire dans le cas où les données associées au NFT ont d'autres formats, par exemple s'il s'agit de sons, de vidéos ou de documents textuels. En règle générale, le lien pointe vers un fichier représentant soit un objet artistique, soit un autre actif numérique (objet de jeu vidéo par exemple).

Sur la *blockchain Ethereum*, les programmes autonomes de gestion de ce type de NFT sont définis par **le standard ERC721Metadata, qui prévoit, comme le standard ERC20, un certain nombre de fonctions. Dans le cas des NFT, le programme doit comporter une case mémoire dans laquelle se trouve un lien internet (URI**, *cf.* encadré 6**)**. La ressource correspondante doit être un jeu de données textuelles (dans un format lisible par un humain appelé JSON) désignant un certain nombre de « propriétés » du NFT : son nom, sa description, un lien vers une éventuelle image qui le représente, *etc.* Le plus souvent, les images sont stockées de façon décentralisée et accessibles *via* un protocole appelé « *interplanetary file system* » (IPFS, *cf.* encadré 7). Grâce à cette standardisation, les plateformes d'échange de NFT peuvent afficher une représentation de l'actif lié au NFT (le plus souvent une image), sa description et ses diverses propriétés.

Considérons par exemple le NFT n° 4985 de la collection *Doodles*, émise par *Doodles_LLC*, collection d'images de 10 000 personnages. Le programme autonome sur *blockchain* tenant le registre des détenteurs des NFT se situe à l'adresse *Ethereum* `0x8a90cab2b38dba80c64b7734e58ee1db38b8992e`. Les NFT de la collection pointent tous vers une adresse `ipfs://QmPMc4tcBsMqLRuCQtPmPe84bpSjrC3Ky7t3JWuHXYB4aS/[numéroduNFT]`, correspondant à une ressource accessible *via* l'IPFS.

Ainsi, à l'emplacement `ipfs://Qm…aS/4985` se situe une liste de données, énumérées dans le tableau 1.

## Annexe II

**Tableau 1 : Métadonnées du NFT « *Doodles #4985* »**

| Champ | Valeur |
|---|---|
| `image` | `ipfs://QmXT5b66AiB9pQ9rxJUTALsrU2i4y2jKy6GWYf5cr7BLn6` |
| `name` | Doodle #4985 |
| `description` | A community-driven collectibles project featuring art by Burnt Toast. Doodles come in a joyful range of colors, traits and sizes with a collection size of 10,000. Each Doodle allows its owner to vote for experiences and activations paid for by the Doodles Community Treasury. Burnt Toast is the working alias for Scott Martin, a Canadian–based illustrator, designer, animator and muralist. |
| `trait: face` | designer glasses |
| `trait: hair` | halo |
| `trait: body` | orange puffer |
| `trait: background` | yellow |
| `trait: head` | green |

*Source : Données disponibles à l'adresse `https://ipfs.io/ipfs/QmPMc4tcBsMqLRuCQtPmPe84bpSjrC3Ky7t3Jw-uHXYB4aS/4985`.*

L'image correspondant au NFT est également stockée sur l'IPFS et peut être téléchargée à l'adresse précédemment citée. Le NFT est présenté comme représentant cette image, les autres attributs permettant de définir diverses propriétés de l'objet (en l'espèce, les « traits caractéristiques » du personnage représenté). Sur *OpenSea*, l'une des principales plateformes d'échanges de NFT, il est possible de visualiser le NFT qui, au 21 février 2023, est mis aux enchères. La page d'enchères permet d'afficher l'image et les « traits caractéristiques » du NFT avant l'achat.

**Encadré 6 : Adresses internet, noms de ressources et identifiants de ressources (URI)**

La navigation sur internet suppose, pour un utilisateur, d'obtenir des ressources électroniques qu'il peut afficher. Une ressource prend la forme d'un document électronique (texte, son, image, mélange de plusieurs de ces contenus au sein d'une page web). Cette ressource doit être téléchargée par l'utilisateur auprès d'un tiers (qualifié, selon les cas, de *serveur* ou de *pair*).

De nombreuses conventions existent pour désigner une ressource. Sur le web, les ressources sont identifiées par une ***adresse*** (*uniform resource locator*, URL). L'URL `https://www.igf.finances.gouv.fr/sites/igf/accueil.html` peut être interprétée comme : « *l'unique ressource qui peut être obtenue, en utilisant le protocole de communication internet HTTPS, auprès du serveur ayant pour nom* `www.igf.finances.gouv.fr` *et qui se situe dans l'arborescence interne à ce serveur à l'emplacement* `/sites/igf/accueil.html` ». Pour télécharger cette ressource, l'utilisateur (plus précisément, le logiciel de navigation qu'il utilise) sait précisément comment procéder : il doit d'abord prendre contact avec le serveur ayant pour nom `www.igf.finances.gouv.fr`, puis établir une communication avec lui selon le protocole HTTPS, et enfin lui demander de lui envoyer la ressource `accueil.html` située dans le dossier `igf`, lui-même situé dans le dossier `sites`. S'il existe une ressource à cette adresse, alors le serveur enverra le document électronique correspondant, qui en l'espèce est une page web. Sinon (par exemple, si la ressource a été supprimée), il renverra une erreur, qui porte le code 404 *file not found*.

Un intérêt de ce système est que le document disponible à une adresse donnée peut changer : par exemple, une page peut être mise à jour. Un inconvénient est qu'au contraire, les versions successives ne sont pas archivées ; en outre, si un document est déplacé, l'utilisateur ne connaît pas forcément sa nouvelle adresse.

Ainsi, alternativement, il est possible de désigner des ressources par un ***nom***, qui n'a jamais vocation à changer. Par exemple, l'*international standard book number* (ISBN) permet de désigner sans ambiguïté des livres publiés, y compris en format numérique. Ainsi, le nom : `isbn:978-2-13-060728-1` désigne une édition précise d'un livre précis. En revanche, disposer de cette ressource ne permet pas de savoir comment obtenir le livre, ni au format électronique, ni en bibliothèque. Il est nécessaire de disposer d'un catalogue ou d'un annuaire pour savoir à quelle adresse obtenir la ressource ayant ce nom.

Un ***identifiant de ressource*** peut être soit une adresse, soit un nom de ressource. La norme RFC3986 définit un format standard pour les *uniform resource identifiers* (URI), qui permet d'englober les deux types d'identifiants (URL et URN).

**Encadré 7 : L'*interplanetary file system* (IPFS)**

Pour rendre une image publiquement accessible sur internet, une première solution est de la stocker sur un serveur web classique, par exemple le serveur d'Alice portant le nom `alice.com`. Alice peut ainsi communiquer l'adresse de l'image, par exemple `https://alice.com/images/chaton.jpeg`. Le défaut de cette solution est que si le serveur d'Alice est en panne, si elle déplace l'image ou encore si elle cesse de payer les frais du nom de domaine, alors la ressource devient indisponible. Ainsi, la disponibilité de l'image dépend d'une seule machine. Des solutions existent pour ajouter de la redondance, mais elles restent dépendantes d'une seule personne ou d'une seule entité.

Le « système de fichier interplanétaire » (*interplanetary file system*, IPFS), développé par Protocol Labs, est une proposition de réponse à ce problème. Les utilisateurs du système forment un réseau. Chaque nœud peut proposer des ressources (images, vidéos, dossiers de ressources…) envoyées à toute personne qui en fait la demande. Les ressources proposées sur le réseau se voient attribuer un identifiant (URI, *cf.* encadré 6), qui est en fait une représentation de leur *hash* SHA256 (*cf.* section 1.2 de l'annexe I). Un fichier peut par exemple avoir pour URI : `ipfs://QmXT5b66AiB9pQ9rxJUTALsrU2i4y2jKy-6GWYf5cr7BLn6`.

La ressource peut ensuite être dupliquée, c'est-à-dire qu'elle peut être hébergée par plusieurs nœuds du réseau. Lorsqu'un utilisateur cherche à accéder à un fichier *via* l'IPFS, il envoie à l'ensemble du réseau une requête de la forme : « je souhaite accéder à la ressource `QmXT5…n6` ». Il suffit qu'au moins un des nœuds du réseau actuellement disponible possède la ressource pour que la requête soit satisfaite. Par ailleurs, des interfaces sont prévues avec les protocoles web classiques (HTTP, notamment). Il est par exemple possible à partir de n'importe quel navigateur web de récupérer la ressource précédente par l'URL `https://ipfs.io/ipfs/QmXT…n6` : le serveur à l'adresse `ipfs.io` est configuré pour comprendre une telle requête comme signifiant « *connecte-toi à l'IPFS, récupère la ressource `ipfs://QmXT…n6` et envoie-moi le résultat par le protocole HTTP* ».

Le stockage de données sur l'IPFS constitue donc une forme de « *cloud computing* décentralisé ». L'intérêt d'un tel système est que l'indisponibilité d'un seul utilisateur ou d'une seule machine n'implique pas pour autant l'indisponibilité de la ressource : la responsabilité individuelle des hébergeurs est diminuée. Compte tenu du caractère décentralisé, l'IPFS connaît un succès important pour le stockage des contenus « Web 3.0 », notamment les images associées aux NFT.

Toutefois, **le stockage doit toujours être assuré par au moins une machine**, ce qui peut être difficile à assurer sans responsable identifié. En pratique, le plus souvent, les utilisateurs qui ont le plus intérêt à ce qu'une ressource accessible par l'IPFS reste bien disponible payent une entreprise spécialisée dans le stockage de contenus (typiquement, Amazon Web Services – AWS) pour qu'elle conserve la ressource sur une machine constituant un nœud IPFS.

## 2.3. Dans ce contexte, la détention d'un NFT est parfois présentée comme un droit de propriété sur l'actif associé, mais cette qualification est trompeuse

### 2.3.1. Certains promoteurs des NFT identifient la détention du NFT à la propriété d'un actif sous-jacent, confondant le jeton et le bien qu'il représente

En 2022, l'usage des NFT le plus connu du grand public a consisté à les présenter comme des **droits de propriété cessibles sur des œuvres**, notamment d'art graphique. Usuellement, plusieurs NFT correspondant à une œuvre similaire sont émis avec des numéros de série permettant de les distinguer (*cf.* annexe III, en particulier sections 1 à 3).

Au-delà des œuvres, le NFT est également souvent utilisé, notamment dans l'univers du jeu vidéo, pour représenter un objet virtuel dont le joueur serait propriétaire, par exemple une armure ou une carte de jeu. De même que pour une œuvre, le NFT comporte dans ce cas un lien vers une ressource en ligne définissant les propriétés de cet actif, incluant une image supposée le représenter.

De façon plus rare, des NFT ont pu être utilisés pour pointer vers des biens corporels, à l'exemple d'une série émise en janvier 2022 représentant des souvenirs des *Beatles* appartenant à Julian Lennon. Les métadonnées des NFT ne comportent, là aussi, qu'une représentation des objets.

Dans ce contexte, les dictionnaires grand public *Larousse*, *Robert* et *Wiktionnaire* comportent tous les trois des définitions d'un NFT similaires, mais impropres, associés à l'idée de propriété et d'authenticité (*cf.* encadré 8). En d'autres termes, selon cette vision, **le détenteur (tel qu'identifié par la *blockchain*) d'un NFT serait le propriétaire de l'œuvre ou de l'objet auquel renvoie le NFT en lui-même**. Il s'agirait d'un droit de propriété, au sens d'un droit réel (sur une chose, *jus in re*), opposable à tous (*erga omnes*).

Cette vision donne lieu à des confusions entre le NFT, c'est-à-dire l'inscription dans la *blockchain* d'une association entre une URL et l'adresse d'un détenteur d'une part et les données auxquelles il renvoie, d'autre part (*cf.* encadré 8). Une telle confusion est présente par exemple dans l'expression « *œuvres d'art sous la forme de NFT* » : l'œuvre est pourtant distincte du jeton qui lui est associé.

Elle est encouragée par le vocabulaire qu'emploient les promoteurs de cette technologie et par l'ergonomie des logiciels de portefeuille (programmes permettant d'interagir avec la *blockchain* et de passer des transactions). En particulier, ces derniers présentent souvent l'image associée à un NFT comme « contenue » dans son « portefeuille », ce qui renforce l'idée de propriété en la comparant à un objet matériel, alors qu'il s'agit, en réalité, d'un lien internet inscrit sur la *blockchain*, associé à un détenteur identifié par ce logiciel. De même, les plateformes d'échanges de NFT *Rarible* et *OpenSea* se présentent comme des sites de vente aux enchères des biens ou des œuvres que représente le NFT.

**Encadré 8 : Définition d'un NFT dans trois dictionnaires grands publics en ligne**

D'après le *Larousse*, un jeton non fongible est un « *fichier numérique non reproductible et infalsifiable représentant un actif unique, objet virtuel ou physique (œuvre d'art, Tweet, morceau de musique, etc.), qui est répertorié dans une* blockchain *et auquel est associé un certificat digital d'authenticité et de propriété* ».

D'après *Le Robert* en ligne, un NFT est un « *certificat cryptographique associé à un objet numérique (image, vidéo, musique…) dont l'authenticité et la traçabilité sont garanties par la* blockchain ».

Enfin, pour le *Wiktionnaire*, tel que consulté le 21 février 2023, un NFT est un « *titre numérique d'authenticité d'un objet immatériel* », cette définition étant rattachée aux lexiques « *droit de propriété* » et « *informatique* ».

### 2.3.2. En réalité, les NFT représentent plutôt soit des outils purement techniques, soit des titres de droits, qui représentent rarement un droit de propriété

La vision qui précède, selon laquelle la détention d'un NFT pourrait représenter la « propriété » des objets vers lesquels il pointe, est trompeuse dans la majorité des cas. La compréhension fine de ce que peut représenter un NFT suppose donc plusieurs étapes dans l'analyse.

D'une part lieu, il importe de relever que **l'idée même d'une propriété sur des objets numériques, incorporels, copiables à l'infini et sans rivalité d'usage, est contestable d'un point de vue économique**. Par exemple, pour un NFT se voulant une œuvre d'art, l'image sous-jacente est systématiquement publique et peut être dupliquée et projetée à l'infini, qui plus est en toute légalité conformément à l'exception de copie privée (*cf.* section 4 de l'annexe IV).

D'autre part, **il n'existe aucune restriction technique sur ce qui peut être mis en circulation comme jeton**. Toute personne peut très facilement émettre un NFT présenté comme un NFT « sur » n'importe quel objet, réel ou virtuel, sans y attacher de droits. Certains NFT ne sont en effet pas présentés comme un titre sur l'image qui figure dans leur description, mais comme un titre *sur un objet représenté par cette image*. Rien n'empêche par exemple un particulier d'émettre un « NFT sur la robe de mariage de Lady Diana », « NFT sur la ville de Paris », ou encore un « NFT sur le RMS *Titanic* ». De tels NFT sont manifestement sans droits associés, mais ont pourtant une existence propre : d'après la plateforme *OpenSea*, de l'ordre de 80 % des NFT émis en utilisant son outil de *minting* gratuit et public seraient « *des plagiats, des faux ou du spam* »[10]. *A fortiori*, dans le cas (majoritaire) où les métadonnées ne sont pas stockées sur la *blockchain,* mais seulement désignées par une URL, l'intégrité des données n'est pas garantie (*cf.* encadré 9), sauf à stocker *on chain* les données en elles-mêmes ou bien leur *hash* (*cf.* encadré 10).

Ce sont donc davantage les possibilités techniques exactes et les droits juridiques que confère la détention d'un NFT qu'il est pertinent d'analyser afin de les qualifier juridiquement et de pouvoir déterminer le régime applicable. De telles analyses sont réalisées dans la section 1 de l'annexe IV. Les principales lignes directrices de l'analyse sont que :

- les NFT peuvent soit être « nus » (sans aucun droit associé), soit représenter un titre de droit sous-jacent : droit de créance sur une personne le plus souvent, ou éventuellement droit de propriété sur une chose. L'étude des actes contractuels passés en lien avec la vente du jeton (conditions générales de vente, en particulier) permet de distinguer les droits associés, parfois avec difficultés. **Une obligation de toujours énoncer explicitement les droits associés à un NFT mis en vente constituerait un outil souhaitable de protection du consommateur** ;
- le NFT, lorsqu'il a pour sous-jacent un bien (corporel ou incorporel), doit toujours en être distingué. **Il n'y a en principe pas identité entre le jeton et son sous-jacent** : les deux constituent des objets juridiques séparés. Seule la loi et le règlement pourraient décider une telle assimilation ;
- les NFT peuvent être qualifiés de biens, même si la notion de propriété d'un bien incorporel est complexe à appréhender. Des décisions de justice ont été rendues en ce sens dans d'autres États. En revanche, compte tenu de la distinction qui précède, la propriété des jetons n'implique pas la propriété du sous-jacent ;
- les NFT peuvent dans certains cas être transparents ou accessoires à leur sous-jacent. Le fait qu'il existe une distinction entre le NFT et son sous-jacent ne fait pas obstacle, par exemple, à ce que le NFT soit assimilé à son sous-jacent pour un traitement fiscal ;
- en ce qui concerne plus précisément les NFT à caractère « artistique », la qualification d'« œuvre d'art » pour les jetons est fausse. Sauf disposition contractuelle contraire, les NFT se contentant d'un renvoi vers une image numérique sont « nus » et dépourvus de quelque droit que ce soit.

[10] Affirmation présentée dans un *tweet* du 28 janvier 2022 (https://twitter.com/opensea/status/1486843204062236676, consulté le 12 avril 2023).

## Annexe II

### Encadré 9 : Le NFT piégé de Moxie Malinspike

Fin 2021, le créateur de la messagerie Signal, Moxie Malinspike, a piégé des acheteurs de NFT en vendant un jeton représentant une œuvre d'art numérique, mais se « transformant » en une image de l'émoji « caca » une fois acheté.

En effet, le jeton contenait un lien vers une URL sur un serveur qu'il maîtrisait. Le serveur était programmé pour envoyer l'image de l'œuvre d'art lorsque la requête était envoyée depuis les serveurs de Rarible ou OpenSea : ces sites représentaient donc l'image sous la forme attendue lors des ventes aux enchères. En revanche, hors du cas d'une requête de Rarible ou OpenSea, l'image renvoyée était celle de l'émoji « caca » : le NFT apparaissait donc sous cette forme une fois « dans » les « portefeuilles ».

Ce piège avait vocation à mettre en garde les acheteurs de NFT contre la fragilité des droits acquis.

### Encadré 10 : Le stockage de métadonnées *on chain* par Sorare

Sorare est une entreprise éditant un jeu fondé sur l'utilisation de cartes virtuelles représentant des footballeurs. Les cartes sont associées à un NFT, sont destinées à être collectionnées et peuvent être jouées dans le cadre d'un tournoi « SO5 » dont les résultats dépendent des performances réelles des sportifs.

Le programme autonome sur *blockchain* gérant les cartes Sorare comporte, pour chaque NFT en circulation, un lien vers une URL sur un serveur détenu par Sorare (sous la forme `https://-api.sorare.com/api/v1/cards/`*`numérodecarte`*). À cette adresse se trouve un fichier comprenant les métadonnées associées à la carte et à son joueur : le nom du joueur, le numéro de série, le club, *etc.* Le fichier contient aussi une URL pointant vers l'image, format PNG, de la carte. Cette URL est également détenue par *Sorare*, à une adresse de la forme `https://assets.sorare.com/carddata/-`*`numérodecarte.png`*.

Ce faisant, aucun obstacle technique n'empêcherait, en principe, Sorare de modifier unilatéralement les données associées à un NFT. Toutefois, en réalité, les métadonnées stockées en format textuel (rareté de la carte, numéro de série, saison d'émission, nom du joueur, date de naissance, nom du club, ville du club) sont également stockées *on chain* dans le programme autonome. Ce dernier est par ailleurs défini d'une telle façon que Sorare ne peut pas les modifier. Le détenteur a donc la certitude que certaines des données fondamentales de sa carte, qui contribuent à lui donner sa valeur spéculative, ne peuvent être altérées.

Par ailleurs, au-delà de l'aspect de collection, c'est dans les conditions générales d'utilisation de Sorare que doivent être recherchés les droits offerts par la détention d'une carte. En particulier, ces conditions ne comprennent pas d'engagement, pour l'entreprise, à permettre la participation au tournoi pour un joueur détenant cinq cartes.

# ANNEXE III

## Les principaux cas d'usage des jetons à vocation commerciale dans l'économie française

# SOMMAIRE

**La technologie des NFT est utilisée pour représenter des droits cessibles dans un univers virtuel.** Grâce à cet outil, un utilisateur peut créer, au sein d'une chaîne de blocs (*blockchain*), un jeton unique auquel peut être associé un titulaire (*cf.* section 2 de l'annexe II). Un titulaire de jeton peut décider de le transférer à une autre personne, le cas échéant contre une certaine quantité de cryptomonnaie créée sur cette même *blockchain*, l'intégrité de la transaction étant garantie par la *blockchain*. Considérant que le titulaire du jeton est le seul à pouvoir décider de s'en défaire et que le jeton est unique, les promoteurs de cette technologie comparent parfois la détention du jeton à un titre de propriété (pour l'analyse juridique des droits associés aux NFT, *cf.* annexe IV). La valeur du jeton réside dans les droits que lui associe l'émetteur (droit de prendre part à un vote ou de participer à un jeu, par exemple) et dans la crédibilité de l'émetteur pour garantir ce droit au titulaire.

# 1. Les jeux représentent le cas d'usage principal des NFT à fins commerciales

## 1.1. La technologie de la *blockchain* permet de conférer aux joueurs un « droit de propriété » sur des objets numériques échangeables

**Dans le domaine du jeu, les NFT sont principalement utilisés comme des certificats de détention d'objets numériques échangeables présents dans le jeu.** L'éditeur du jeu associe le NFT à un objet virtuel unique. Il certifie le fait que la détention (dans la *blockchain*) du jeton représente la possibilité d'utiliser l'objet représenté (dans le jeu) et que seul le titulaire du jeton a cette possibilité[1]. Le NFT représente par exemple :

- dans les jeux *Sorare* et *Gods Unchained*, une carte virtuelle de jeu numérotée (à tirage limité), que le joueur est le seul à pouvoir utiliser ;
- dans le jeu *Axie Infinity*, un animal virtuel, que le détenteur du jeton est le seul à pouvoir jouer ou faire reproduire ;
- dans le jeu *StepN*, une paire de chaussures virtuelle dont la détention par le joueur modifie sa performance de jeu.

Dans chaque cas, l'éditeur certifie que la détention du NFT représente la « *propriété* » de l'objet dans le monde du jeu, qui confère donc certains pouvoirs ou privilèges ainsi que le droit d'être affiché publiquement comme « *propriétaire* » dudit objet, par exemple sur le profil public du joueur. L'objet représenté par le NFT est échangeable (le changement de titulaire du jeton correspondant à un changement de « *propriétaire* » de l'objet représenté) et peut constituer un objet de collection. La technologie des NFT[2] est donc un moyen de mettre en œuvre l'idée d'une « *propriété* » virtuelle.

[1] Rien n'interdit en revanche à l'éditeur de créer plusieurs objets ayant des propriétés identiques.

[2] D'autres technologies sont envisageables pour aboutir au même effet en utilisant, par exemple, des bases de données servant de registre de propriété.

Les NFT ont pour avantage de faciliter les échanges, puisque cette technologie les rend possibles indépendamment de l'éditeur, *via* des plateformes spécialisées et concurrentes telles que *Binance* ou *OpenSea*. Des standards techniques qui se sont imposés dès l'émergence de ces jetons (ERC 721, *cf.* partie 2 de l'annexe II) facilitent l'interopérabilité des jetons entre les plateformes. L'éditeur doit en revanche maintenir la confiance des joueurs quant aux garanties qu'il continue d'apporter : certification de l'équivalence entre le NFT et l'objet virtuel, possibilités qu'offre la « *propriété* » des objets virtuels dans le jeu ou encore rareté des objets. Du fait du caractère décentralisé des ventes, les jeux à NFT sont rattachés à l'idée de « web décentralisé », parfois aussi qualifié de « Web 3.0 » par ses promoteurs[3].

**Cette notion de « *propriété virtuelle* » est d'un intérêt multiple pour le secteur du jeu.** D'après les représentants du secteur du jeu vidéo (syndicat national des jeux vidéo et syndicat des éditeurs de logiciels de loisirs), elle répond à une forte demande des joueurs de « *posséder* » le fruit de leur investissement, parfois important, à la fois en temps et en argent, dans le jeu. Des démarches des éditeurs de jeux pour faciliter l'interopérabilité entre les jeux pourraient également permettre aux joueurs d'utiliser les objets dont ils sont « *propriétaires* » dans plusieurs jeux distincts, voire de créer de nouveaux objets afin de modifier le jeu (« *modding* »).

**Par ailleurs, la cessibilité des NFT permet au détenteur d'engranger des gains en revendant ses objets sur une plateforme de marché** (gérée par l'éditeur du jeu ou non), parfois avec des plus-values. Cette innovation crée un marché secondaire permettant aux joueurs de revendre leurs objets lorsqu'ils se lassent d'un jeu. Elle présente également le risque d'une utilisation spéculative des jeux en introduisant une espérance de gain lorsque le jeu récompense les joueurs sous la forme d'objets numériques échangeables, que leur valeur soit liée aux performances dans le jeu ou à une valeur de collection[4].

Ainsi, dans *Axie Infinity*, la possession des animaux virtuels autorise à les croiser, sous réserve de détenir une cryptomonnaie propre au jeu (qu'il est possible d'acheter ou de gagner), leur progéniture étant représentée par un nouveau NFT lui-même cessible. S'agissant de *Sorare*, la détention de cartes permet de participer à des tournois dont l'enjeu est le gain de nouvelles cartes-NFT et d'une cryptomonnaie grand public (l'ether). Ces jeux sont donc présentés par leurs éditeurs et identifiés par la presse spécialisée comme un moyen pour le joueur de gagner de l'argent.

---

[3] Les appellations « Web 1.0 » et « Web 2.0 » étant utilisées, de façon consensuelle, pour désigner respectivement les sites internet statiques (une personne maintenant seule une page) et les sites participatifs dont les membres créent le contenu (en particulier mais sans s'y limiter, les réseaux sociaux).

[4] C'est le cas par exemple de certaines cartes ne pouvant pas être jouées dans *Sorare* (celles représentant des footballeurs célèbres mais retraités) ou bien des « *skins* » (habillage de personnages) cessibles dans le jeu *Counter Strike*.

## 1.2. Encore embryonnaires, les jeux à objets numériques échangeables peuvent permettre l'apparition de nouveaux modèles économiques pour les éditeurs de jeux et avoir des retombées sur l'usage des NFT

### 1.2.1. Les objets numériques échangeables font émerger de nouveaux modèles économiques reposant sur une « boucle ouverte »

Le secteur du jeu vidéo a connu, sous l'impulsion d'innovations successives, une diversification tant des supports de jeu (ordinateur, console, téléphone portable, tablettes) que des modèles économiques des éditeurs. De nouveaux modèles économiques sont apparus avec le temps (*cf.* tableau 1), passant d'un modèle dominant où le revenu est tiré de la vente du support unique de jeu à des modèles variés où le revenu peut être tiré de différentes sources non exclusives (achat du jeu, achats *in game*, publicité, abonnement, *etc.*). La multiplication des achats complémentaires à l'acquisition initiale du jeu (bonus, objets, niveaux débloqués, contenus téléchargeables après la sortie du jeu[5], *etc.*) permet aux éditeurs de prolonger la durée de vie d'un jeu en en tirant des revenus sur le long cours, afin d'amortir des coûts de développement de plus en plus élevés.

Si le troc d'objets numériques est ancien dans l'univers du jeu vidéo[6], le fonctionnement des jeux antérieurs au Web 3.0 était caractérisé par une « boucle fermée » : les objets échangés ne pouvaient pas être revendus, ils restaient dans le jeu. Par exemple, dans *Fortnite* ou *FIFA*, il est techniquement possible d'échanger un objet en vendant le compte joueur qui le détient, mais cette possibilité est explicitement interdite par l'accord de licence du jeu et fait encourir au fraudeur le risque de suppression du compte.

L'introduction des objets numériques échangeables, cessibles et monétisables, constitue un nouveau modèle, dans lequel les objets sont désormais en « boucle ouverte » et peuvent être revendus en dehors du jeu. Dès lors, ces jeux peuvent mêler plusieurs motivations : le plaisir de jouer, mais aussi la volonté de gagner de l'argent en remportant des objets numériques revendables. Cette innovation a ainsi fait naître le modèle des « *play to earn* », qui suppose d'avoir la « *propriété* » sur ses objets et de pouvoir les monétiser en dehors du jeu. Dans ce modèle, l'éditeur finance le développement du jeu par l'émission des premiers objets numériques (par exemple, des cartes sous forme de NFT) et tire un revenu régulier de l'émission de nouvelles séries d'objets. Il peut en outre prélever une commission sur l'échange des NFT par les joueurs, même si ces échanges n'ont pas lieu sur une plateforme qu'il gère, si cette règle a été fixée dès la création du NFT.

**Tableau 1 : Exemple de modèles économiques dans le secteur des jeux vidéo**

| Modèle économique | Exemple de jeu |
|---|---|
| *Premium* sur ordinateur personnel ou sur console : l'éditeur vend un support physique (cartouche, CD-rom, *etc.*) contenant l'intégralité du jeu. | Jeux de GameBoy, comme *Pokémon*<br>*SimCity* 1 à 4<br>*Age of Empire* |
| *Game as a service* : jeu en ligne à abonnement. | *World of Warcraft* (jeu à abonnement mensuel, avec possibilité d'acheter des options payantes de façon définitive). |

[5] À l'exemple des nouveaux circuits de *Mario Kart 8 Deluxe*, téléchargeables à partir de 2022 alors que le jeu est initialement sorti en 2017.

[6] La série de jeux vidéo *Pokémon* est fondée sur le principe de l'échange d'animaux virtuels que dirigent les joueurs : de tels échanges sont même nécessaires pour terminer en intégralité le jeu. Apparue en 1996, *Pokémon* constitue en novembre 2021 la quatrième série de jeux vidéo la plus vendue de l'histoire (environ 380 millions d'unités).

| Modèle économique | Exemple de jeu |
|---|---|
| *Free-to-play* : l'accès au jeu est gratuit. L'éditeur peut se financer par la publicité ou par les achats *in game* (bonus, skins, *etc.*), qui peuvent être contenus dans une *lootbox*. Une version payante peut permettre au joueur de ne plus être exposé à la publicité. | *Angry birds*<br>*Candy Crush*<br>*Fortnite* |
| *Freemium* : jeu gratuit, dont une partie ou un mode n'est accessible qu'aux joueurs acquérant la licence complète. | *Clash of Clans* (le mode *premium* offre des droits supplémentaires dans le jeu, permettant une meilleure expérience et une progression plus rapide) |
| Jeux *play to earn* à objets échangeables : le joueur achète à l'éditeur ou sur le marché secondaire un objet numérique échangeable, fait augmenter sa valeur en jouant, et peut le revendre sur le marché secondaire | *Sorare, Axie Infinity, Gods unchained* |

*Source : Mission.*

### 1.2.2. Le développement des jeux est un moteur essentiel du développement de l'écosystème Web 3.0.

Le secteur des jeux Web 3.0 connaît une forte croissance, en dépit du retournement de la conjoncture dans le domaine des cryptoactifs intervenu en 2022. Le développement de nouvelles technologies autour des *blockchains*[7] explique cette résilience et le nombre de jeux actuellement en développement, près de 2 000 d'après l'Autorité nationale des jeux (ANJ). D'après le cabinet de conseil *Bain & Company,* 35 à 40 % des investissements réalisés par des entreprises dans les applications et systèmes terminaux (destinés aux utilisateurs finaux) utilisant des NFT concernent le secteur du jeu vidéo[8]. Selon DappRadar[9], l'investissement dans les jeux Web3 a atteint, à l'échelle mondiale, 7,6 Md$ en 2022 contre 3,7 Md$ en 2021, soit une multiplication par deux en un an, et 190 M$ en 2020.

**Les jeux deviennent ainsi le principal cas d'usage des technologies Web 3.0. Selon DappRadar[10], les activités de jeu représentent 48,5 % des portefeuilles uniques actifs chaque jour** (*daily unique active wallets, dUAW)* sur les *blockchains* en janvier 2023. Le solde se répartit entre les autres usages, parmi lesquels la finance décentralisée (DeFi) qui comptabilise 21 % des *wallets* uniques actifs.

Ce secteur joue un rôle d'autant plus essentiel qu'il constitue un laboratoire d'innovation quant à la technologie NFT en elle-même, susceptible d'avoir des retombées sur les autres cas d'usage (*cf. infra* : consommation dans les métavers, secteur artistique, identité numérique, *etc.*)[11]. En conséquence, **les jeux vidéo constituent aujourd'hui un secteur clef dans la perspective d'un développement de la technologie NFT**.

---

[7] Notamment l'émergence des technologies de « *layer* 2 » telles qu'*Immutable X*. Celles-ci visent à simplifier l'utilisation des jetons et de la technologie *blockchain* par les développeurs puis par les joueurs et à réduire les coûts de transaction (*cf.* section 4 de l'annexe I).

[8] Bain & Company, *Technology Report 2022: Tech Companies Eat Disruption for Breakfast*, figure 3f, p. 23.

[9] *Blockchain Games Report*, *2022 Overview*, janvier 2023.

[10] *Blockchain Games Report*, n° 12, mars 2023.

[11] Par exemple, l'entreprise *Ubisoft* a indiqué à la mission travailler avec la *startup* française *Aleph.im*, spécialisée dans le développement d'infrastructures de stockage et de calcul décentralisées, afin de réduire le rôle des intermédiaires centralisés critiques (*cf.* section 4 de l'annexe I). Cette problématique est commune à l'ensemble des cas d'usage du Web 3.0 : les investissements réalisés au titre du cas d'usage jeu vidéo pourraient donc bénéficier à l'écosystème dans son ensemble.

Le secteur est très évolutif. Les principaux acteurs peuvent connaître une chute aussi fulgurante que l'ascension qui l'a précédée, comme cela a été le cas pour le jeu *Axie Infinity*. D'après DappRadar[12], les trois jeux Web 3.0 les plus utilisés en 2022 étaient *Splinterlands*, qui a rassemblé 235 000 portefeuilles uniques actifs par jour en moyenne (mais uniquement 158 000 fin 2022), puis *Alien Worlds*, qui a attiré 200 000 joueurs par jour en moyenne (et 225 000 fin 2022) et enfin, *Axie Infinity*, avec en moyenne 76 000 joueurs par jour. En mars 2023[13], le classement des cinq jeux les plus populaires a déjà connu des évolutions : *Alien Worlds* est devenu leader incontesté (238 000 joueurs), *Splinterlands* poursuit sa baisse (78 000) et est rattrapé par *Farmers World* (78 000), tandis que *Planet IX* (54 000) et *Upland* (27 000) complètent le tableau.

**Encadré 1 : *Axie Infinity***

*Axie Infinity* est un jeu de combat dans un monde fantastique où chaque joueur doit vaincre son adversaire grâce à son équipe d'*Axies*, de petites créatures ayant des traits individuels (santé, moral, habileté, vitesse) et associées à des NFT. Pour commencer à jouer, le joueur doit acquérir trois *Axies* (qui sont payants). Le joueur joue des cartes, qui représentent les pouvoirs de chaque *Axie*, consommant une certaine quantité d'énergie et infligeant des dommages à l'adversaire. Le joueur peut jouer seul selon un mode aventure ou contre d'autres joueurs connectés (mode arène). En cas de victoire, le joueur remporte des SLP (*smooth love potion*), un jeton de cryptomonnaie spécifique à ce jeu qui permet au joueur d'élever de nouveaux *Axies*. Un troisième type de jetons, l'*Axie Infinity Shard* (AXS), permet aux joueurs de participer à la gouvernance du jeu.

*Axie Infinity*, disponible sur ordinateur et sur mobile, a remporté le plus grand succès des jeux NFT. Développé par le studio vietnamien *SkyMavis*, utilisant la *blockchain Ethereum*, il a revendiqué jusqu'à 2,7 millions de joueurs en janvier 2022. L'excès de création de SLP a néanmoins fait chuter la valeur du jeton. Le jeu a également pâti d'un piratage de grande ampleur en mars 2022, occasionnant une perte de jetons équivalente à 615 M$, puis de la faillite de FTX. La société a rebondi en lançant une nouvelle version du jeu, *Axie Origin*, en août 2022, dans laquelle les SLP ne sont plus accessibles en mode aventure et peuvent être utilisés pour acquérir de nouveaux objets de jeu, afin de rééquilibrer le marché des SLP. Cette modification n'a cependant pas engagé de nouvelle dynamique pour le cours du jeton de gouvernance du jeu AXS, passé de 70 € en janvier 2022 à 6,5 € en janvier 2023.

Plusieurs types de jeux peuvent être distingués, sans que la liste suivante épuise tous les modèles de jeux :

- les jeux de rôles, de combats, les plus proches des jeux vidéo traditionnels, développant souvent un univers fantastique, comme *Gods Unchained* ;
- les jeux dits de « *move to earn* », fondés sur les défis sportifs pour les utilisateurs, dont *StepN* est le meilleur exemple ;
- les « tamagotchi », fondés sur le soin porté à un animal ou à une créature de compagnie. C'est par exemple le cas de *Genopets* ou de *Dogami* ;
- les jeux de « *fantasy* » sportive, c'est-à-dire fondés sur les résultats de compétitions sportives réelles, dont *Sorare* illustre la réussite ;
- les jeux liés à un métavers, comme *Sandbox*, ou centrés sur des stratégies foncières (*Planet IX*, par exemple).

Il est à noter que les jeux vidéo traditionnels peuvent également intégrer des éléments liés à la *blockchain*, comme des objets de jeu associés à des NFT, sans pour autant basculer dans un modèle totalement Web 3.0 et sans que les jeux deviennent des « *play to earn* ». Cet apport peut notamment être lié aux *lootboxes*, des « coffres à butin aléatoire » qui procurent au joueur, contre paiement, une récompense aléatoire, qui, si elle est associée à un NFT, pourrait être revendue sur un marché secondaire.

[12] *Blockchain Games Report*, 2022 Overview, janvier 2023.

[13] Classement en temps réel de *DappRadar* consulté le 21 mars 2023.

Si le secteur français du jeu Web 3.0 n'est pas au premier rang mondial, puisqu'il ne compte aucun des jeux les plus utilisés (*cf. supra*), il n'en reste pas moins dynamique, porté par des acteurs de niveau international (comme *Sorare*, dans le monde des « *play to earn* » sportifs (*cf.* encadré 2) et par des projets nombreux (*Oval3* et *Metafight* dans la fantaisie sportive, *Immortal Games* dans les échecs – *cf.* encadré 3 – ou encore *Dogami*, un tamagotchi). Les atouts de la France dans le secteur des jeux vidéo, avec notamment la présence du leader Ubisoft, constituent également un levier de développement potentiel pour les jeux Web 3.0.

**Encadré 2 : Un leader français : *Sorare***

*Sorare* est un jeu de cartes représentant des sportifs de haut niveau dans plusieurs sports (football, basketball, baseball), grâce aux accords d'exclusivité signés par Sorare avec les sportifs et les ligues. Les joueurs composent des équipes grâce aux cartes en leur possession et s'inscrivent à des tournois qui ont lieu régulièrement (deux fois par semaine pour le football). Les cartes acquièrent un score plus ou moins élevé en fonction de différents paramètres : bonus lié à l'expérience acquise par la carte, désignation par le joueur comme capitaine, bonus lié au fait que la carte ait été émise au cours de la saison et surtout, performances réelles du sportif. La somme des scores des cartes donne le score de l'équipe, le joueur qui a enrôlé l'équipe au score le plus élevé remporte le tournoi.

Il existe deux types de cartes : des cartes payantes, associées à des NFT, achetées sur le marché primaire (lors de l'émission par Sorare, avec enchères) ou sur le marché secondaire, ainsi que des cartes gratuites incessibles, reçues aléatoirement lors de l'inscription. En fonction de la rareté des cartes détenues, le joueur peut avoir accès à certains types de tournois, plus ou moins sélectifs et associés à des récompenses plus ou moins élevées. Les récompenses prennent la forme de cartes NFT distribuées gratuitement, d'expériences réelles (billets de match, rencontres avec des sportifs, *etc.*) et de versements dans la cryptomonnaie éther. Depuis mars 2023, les joueurs peuvent également gagner des « coins », une monnaie de jeu interne à Sorare, qui permet d'acquérir des bonus pour ses cartes.

Les cartes permettent de participer aux tournois, mais ont également une valeur d'objet de collection.

La société Sorare a été fondée en 2018 et connaît depuis sa création une forte croissance, son chiffre d'affaires passant de 8 M€ en 2020 à 325 M€ en 2021. Elle comptait, en 2022, environ 120 salariés, dont la moitié en France. Elle a levé, en 2021, 730 M$ au cours de deux levées de fonds.

**Encadré 3 : Un projet français : *Immortal Games***

*Immortal games* est un jeu d'échecs à base de NFT, lancé en 2021 par des Français. Le jeu utilise la *blockchain Ethereum* et son *layer 2 Immutable X* et a levé 15,5 M$ en 2022. Chaque joueur peut intégrer à ses pièces de jeu jusqu'à quatre pièces particulières, appelées des Immortels. Ces Immortels sont associés à un NFT et peuvent être échangés en dehors du jeu. Ils peuvent être de quatre niveaux de rareté (appelés niveaux de « pureté ») et sont associés à des quêtes (par exemple : « le roi ne doit pas bouger »), qui, si elles sont accomplies, rapportent des points. Les joueurs qui gagnent des parties remportent aussi des points, ce qui détermine leur classement hebdomadaire au sein de la communauté de joueur. Les vainqueurs du classement reçoivent en récompenses des NFT, des éthers et des jetons du jeu, les $CMT (« CheckMate Tokens »), utilisables dans le jeu pour améliorer les Immortels, par exemple.

### 1.2.3. Le développement des jeux Web 3.0 soulève un problème juridique majeur

Dans la mesure où les jeux Web 3.0 remplissent les quatre critères (*cf.* encadré 4) qui définissent, en droit français, un jeu d'argent et de hasard, ceux-ci devraient être interdits en vertu du principe de prohibition de ces jeux qui prévaut en France (article L. 320-1 du code de sécurité intérieure, CSI). En effet, les jeux Web 3.0 ne rentrent dans aucune des exceptions à cette prohibition prévues à l'article L. 320-6 du CSI.

L'application stricte de cette analyse juridique conduirait donc à empêcher tout développement du jeu dans le secteur du Web 3.0 en France, par assimilation du « *gaming* » au « *gambling* ».

**Encadré 4 : La définition des jeux d'argent en droit français**

Pour délimiter le périmètre de la prohibition prévue par l'article L. 320-1 du CSI, ce même article énonce quatre critères cumulatifs : « *Sont réputés jeux d'argent et de hasard et interdits comme tels toutes opérations* ***offertes au public****, sous quelque dénomination que ce soit, pour faire naître* ***l'espérance d'un gain*** *qui serait* ***dû, même partiellement, au hasard*** *et pour lesquelles un* ***sacrifice financier*** *est exigé de la part des participants* ».

Les jeux Web 3.0 remplissent ces critères :

- étant proposés en ligne, ils constituent par nature une offre publique ;
- le résultat du jeu est au moins partiellement dû au hasard (le fait que l'habileté du joueur joue un rôle non négligeable n'entre pas en compte puisque la loi prévoit que l'interdiction recouvre « *les jeux dont le fonctionnement repose sur le savoir-faire des joueurs »)* ;
- le sacrifice financier est caractérisé dès que l'accès au jeu est conditionné à l'achat d'un objet de jeu[14] (la plupart du temps, un NFT), dans la mesure où sa définition en droit revient à la présence simple d'une dépense (et non d'une mise ou d'une perte) ;
- l'espérance d'un gain est matérialisée puisqu'il s'agit du principe même de ces jeux, qui promettent à leurs joueurs des récompenses (la nature de ces récompenses important peu dans leur qualification de gain, dès lors qu'elles ont une valeur patrimoniale).

Les *lootboxes*, présentes dans les jeux vidéo, remplissent les trois premiers critères. L'Autorité de régulation des jeux en ligne (ARJEL), devenue Autorité nationale des jeux (ANJ), a estimé par une prise de position de 2018 que le quatrième critère n'était pas rempli tant que les récompenses octroyées n'étaient pas monétisables, ce qui permet à la majorité des *lootboxes* de ne pas être considérées comme des jeux d'argent et de hasard.

*Source : Mission, code de la sécurité intérieure.*

Le développement des jeux Web 3.0 suppose donc une évolution du cadre réglementaire. Les enjeux d'une telle évolution sont présentés dans le rapport n° 2022-M-062-02 de l'Inspection générale des finances.

## 2. Les NFT connaissent de nombreux usages dans le secteur de l'art et de la culture, relevant le plus souvent de l'ostentation ou de l'achat de produits dérivés et, plus rarement, de la gestion de droits

### 2.1. L'usage des NFT dans le domaine artistique est en grande partie porté par l'assimilation des jetons à des œuvres d'art

#### 2.1.1. Les promoteurs des NFT à usage artistique assimilent ces jetons à des œuvres ou à des « jumeaux numériques » d'œuvres

L'un des principaux cas d'usage des NFT consiste à présenter le titulaire du jeton comme étant le détenteur de l'œuvre d'art qu'est le fichier sous-jacent, le plus souvent une image. C'est en particulier dans ce contexte que les NFT ont été connus du grand public à partir de 2020 et que l'« art NFT » a connu une bulle spéculative jusqu'en 2022, culminant avec la vente d'un NFT sur l'œuvre *Everydays : the First 5000 Days* de Mike Winkelmann (Beeple), adjugée par Christie's pour 69,3 M$ le 11 mars 2021.

[14] C'est autour de ce critère qu'a porté le dialogue entre la société Sorare et l'ANJ, à l'automne 2022. L'ANJ a demandé à Sorare, afin d'éviter l'interdiction, de se mettre en conformité en prévoyant un canal de jeu gratuit qui permettrait au critère du sacrifice financier de ne pas être rempli.

La qualification juridique exacte de ce que pourrait être un « NFT artistique », en particulier l'analyse des droits que confère ou que peut conférer un tel NFT au regard du droit de la propriété littéraire et artistique et du droit civil *stricto sensu*, sont analysés en section 3 de l'annexe IV[15]. Il ressort de cette analyse qu'un « NFT artistique » ne peut aucunement être considéré comme une œuvre ni, plus généralement, comme une forme, même dégradée, de propriété sur une œuvre ou son support. Néanmoins, cette assimilation du NFT à une œuvre, à un support d'œuvre ou à une notion indéfinie de « double numérique » d'œuvre reste à la source de ce cas d'usage.

Parmi ces œuvres, doivent être signalées de nombreuses œuvres « collectibles », c'est-à-dire diffusées par collection. Les *Bored Ape Yacht Club* forment ainsi une collection de 10 000 images de singes comportant diverses variantes, émises par la société *Yuga Labs* : chaque image est numérotée et significativement différente des autres (les singes ont chacun des *traits caractéristiques*). Pour certaines collections en revanche, les NFT ne comportent qu'un numéro de série différent, mais portent sur des images identiques ou quasiment identiques.

**Le postulat des collectionneurs de ces œuvres réside dans l'idée que le NFT pointant vers l'œuvre serait intrinsèquement désirable, parce qu'unique.** Certes, l'œuvre sous-jacente est librement copiable, mais le détenteur du NFT pourrait apporter la preuve qu'il a acquis l'œuvre de manière légitime et que celle-ci a bien pour origine l'artiste, le jeton étant techniquement unique et non falsifiable. En outre, il est vrai que toute personne peut techniquement émettre un nouveau NFT contrefait pointant sur la même image, mais comme l'émetteur est identifiable, le NFT contrefait n'aurait aucune valeur, à la différence de l'original, et le contrefacteur serait détecté. Enfin, si un artiste faisait le choix d'émettre de nouveaux NFT sur une même œuvre, ce comportement serait repéré par la communauté d'utilisateurs des *blockchains*, l'artiste perdrait en respectabilité et sa cote baisserait.

Ces arguments justifient, aux yeux des promoteurs de l'« art NFT », l'intérêt économique de la détention du jeton, qui est effectivement un bien rival, authentique et non falsifiable. Le fait que ce jeton soit associé, d'une quelconque manière, à une œuvre d'art, entre cependant peu en considération dans ce raisonnement. Ainsi, des jetons associés à des fichiers ne constituant aucunement des œuvres de l'esprit ont été vendus à des prix extrêmement élevés selon des modalités identiques à des œuvres de « crypto-art ». C'est le cas par exemple d'une capture d'écran du premier tweet, cédée pour 2,9 M$ en septembre 2021 par Christie's[16] et d'un fichier contenant entre autre le code source de quelques-uns des premiers logiciels utilisés pour créer le *Web* en 1990, vendu par Sotheby's pour 5,4 M$[17]. La frontière est ainsi complexe à tracer entre les NFT à caractère artistique et les NFT « biens de consommation » (*cf.* section 3).

**Par ailleurs, les ventes de NFT à caractère artistique ne se limitent pas à des œuvres de « crypto-art natif », c'est-à-dire aux œuvres numériques associées à des NFT dès leur divulgation.** La « tokénisation », c'est-à-dire le fait d'émettre un jeton pointant vers une reproduction numérique d'une œuvre précédemment créée, constitue également un phénomène important dans le secteur de l'art et de la culture.

Cette « tokénisation », quand elle est réalisée à des fins artistiques, peut en fait correspondre à deux cas d'usage :

---

[15] Voir également, en ce sens : Jean Martin et Pauline Hot, *Rapport de la mission sur les jetons non fongibles : sécuriser le cadre juridique pour libérer les usages*, rapport présenté à la séance plénière du conseil supérieur de la propriété littéraire et artistique du 12 juillet 2022.

[16] Jamie Crawley, « *Jack Dorsey's First Tweet Sells for $2.9M* », *Coin Desk*, 22 mars 2021 (https://www.coindesk.com/markets/2021/03/22/jack-dorseys-first-tweet-sells-for-29m/, consulté le 24 mars 2023).

[17] « *Tim Berners-Lee sells web source code NFT for $5.4m* », *BBC News*, 30 juin 2021 (https://www.bbc.com/news/technology-57666335, consulté le 27 mars 2023).

- la **finalité artistique en elle-même de l'acte de tokénisation**. La démarche intellectuelle consistant à émettre, par exemple, un NFT sur une reproduction numérique d'un tableau comme *La Joconde* pourrait ainsi constituer une performance artistique et donc une œuvre originale, de la même façon que la présentation par Marcel Duchamp d'un urinoir comme œuvre d'art sous le titre *Fontaine* avait constitué une création artistique en 1917. Toutefois, une telle démarche, qui était novatrice la première fois qu'elle a été mise en œuvre, ne présente aujourd'hui probablement plus l'originalité nécessaire à la reconnaissance de la qualité d'œuvre de l'esprit ;
- la **création d'un « jumeau numérique »**. Dans ce cas, le NFT pointe vers une représentation numérique d'une œuvre matérielle, le plus souvent une version numérisée d'un tableau réel. Pour les promoteurs d'une telle démarche, le NFT serait un bien meuble incorporel de même substance que l'œuvre originale. Par exemple, une œuvre célèbre détenue par un musée pourrait être tokénisée soit pour être vendue (logique d'ostentation, comme un poster, ou logique de souvenir, comme une carte postale), soit pour être « prêtée » à un autre musée qui pourrait ainsi l'afficher de façon « authentique ». Le « jumeau numérique » pourrait quant à lui faire l'objet d'un démembrement de propriété ou d'un achat en indivision.

### 2.1.2. L'usage des NFT « œuvres d'art » repose en premier lieu sur des plateformes d'échange et d'ostentation

Comme pour l'ensemble de l'écosystème NFT, leur usage dans le secteur de l'art est porté par les **plateformes d'échange.** Ce sont ces plateformes qui, les premières, ont pu rendre les NFT à caractère artistique liquides et contribuer à leur donner une valeur marchande. La plupart de ces plateformes ne sont cependant pas orientées sur les NFT à caractère artistique et permettent l'échange de jetons non fongibles de toutes natures. Historiquement, la principale plateforme mondiale d'échange de NFT est la plateforme américaine *OpenSea* qui concentrait 89 % des transactions en janvier 2022[18]. La place dominante d'*OpenSea* est remise en cause par la concurrence de la plateforme *Blur*, qui connaît une ascension très rapide depuis fin 2022. Les NFT échangés sur les plateformes peuvent être indifféremment « natifs » (œuvre originale) ou « non-natifs » (tokénisation d'une œuvre préexistante).

**Les sites internet, réseaux sociaux et mondes virtuels permettant d'afficher la détention d'un NFT jouent également un rôle essentiel dans le modèle économique de ces jetons.** Compte tenu de la valeur principalement ostentatoire des NFT « œuvres d'art », leur rôle est central pour que le produit soit désirable. Les plateformes d'échange jouent ce rôle en premier lieu, puisqu'elles affichent à tout moment le nom du titulaire du NFT. Plusieurs outils et sites permettent par ailleurs d'afficher les NFT détenus : par exemple, les réseaux sociaux *Twitter* et *Instagram* autorisent leurs utilisateurs à afficher (notamment en image de profil) les images pointées par des NFT qu'ils détiennent, dans un cadre de forme spéciale, qui atteste de leur « propriété » légitime. La plateforme de messagerie instantanée *Discord* permet de réserver aux détenteurs de certains NFT l'accès à une discussion de groupe. À l'avenir, des logiciels de métavers pourraient conditionner la « possession » d'une œuvre dans l'univers numérique à la détention d'un NFT correspondant (*cf.* section 2.2.3.2).

[18] Source : Dune Analytics, chiffre tiré du rapport « *Full-year review 2022* » de Binance Research.

### 2.1.3. La conception et la diffusion d'« art natif NFT » est ensuite portée par un écosystème de « crypto-artistes » et de « galeries NFT »

Les « crypto-artistes » sont des créateurs choisissant de diffuser leurs œuvres d'art sous un format numérique et de les adosser à un NFT ; l'art est alors qualifié de « natif ». La création des œuvre formant des collections implique souvent le recours à de l'art génératif.

Outre une exposition de leurs œuvres en ligne, notamment sur les plateformes d'échange, les « crypto-artistes » peuvent recourir à des « galeries NFT » comme intermédiaires. Ces « galeries NFT » entendent jouer, vis-à-vis du « crypto-art », un rôle similaire à celui des galeries traditionnelles vis-à-vis des œuvres d'art physique.

Certaines de ces galeries ont une existence physique et exposent dans leurs locaux les œuvres d'art numérique en les affichant sur des écrans vidéo. La NFT Factory à Paris et la Vitruvius NFT Gallery à Montpellier entrent par exemple dans cette catégorie. De nombreux sites jouent par ailleurs un rôle de galerie numérique, exposant numériquement les œuvres pour lesquelles ils proposent l'acquisition du jeton.

L'un des rôles des galeries ou, plus généralement, des « curateurs », peut également être de mieux identifier les droits associés à la vente de NFT « natifs ». L'entreprise Exposure Arts, agissant sous la marque Rhapsody Curated, propose ainsi l'exposition en ligne d'œuvres de photographes et la vente des œuvres associées à des NFT. Elle développe des contrats de licence associés à la vente du NFT permettant de transférer des droits limités aux acheteurs.

### 2.1.4. Les musées et collectionneurs privés peuvent émettre des NFT « jumeaux numériques » d'œuvres qu'ils détiennent, mais peu de projets ont émergé en France à ce sujet en raison notamment des risques d'image

Certaines institutions culturelles ont pris le parti d'émettre des « jumeaux numériques » d'œuvres, c'est-à-dire des NFT « authentiques » sur des œuvres physiques qu'elles possèdent (le plus souvent des tableaux). Le « jumeau » a vocation soit à être vendu à un collectionneur, qui peut ainsi se présenter comme son « propriétaire légitime », soit à être prêté ou transmis à un autre musée qui peut ainsi exposer « légitimement » l'œuvre numérique. L'émission de NFT « jumeaux numériques » sur des œuvres autres que picturales a été envisagée ou tentée, mais ne connaît qu'un succès limité. En effet, l'utilisation ostentatoire des NFT repose essentiellement sur la possibilité d'afficher des images (comme image de profil sur un réseau social ou sur un « mur » public par exemple) et se prête mieux à des œuvres picturales ou, exceptionnellement, vidéographique, qu'à des œuvres musicales, architecturales ou encore à des performances.

Environ une dizaine de musées étrangers à dimension mondiale ont ainsi expérimenté la « tokénisation » d'œuvres qu'ils détiennent. C'est le cas de la galerie des Offices, à Florence, qui a vendu un avatar numérique du *Tondo Doni* de Michel-Ange en mai 2021 pour 240 000 €. Le musée de l'Ermitage (Saint-Pétersbourg) a quant à lui collecté, dans le cadre d'un partenariat avec *Binance* NFT, 440 000 $ en septembre 2021 en vendant des « jumeaux numériques » d'œuvres de Léonard de Vinci, van Gogh, Monet, Kandinsky et Giorgione. Ce cas d'usage est envisagé pour permettre un développement de ressources propres pour les institutions culturelles et présente l'intérêt de n'entraîner aucune perte : l'institution reste propriétaire de son œuvre, dont la copie circule déjà librement sur Internet.

La frontière entre ce cas d'usage et celui de l'émission de produits dérivés d'œuvres (*cf.* 2.2) est cependant poreuse. Ainsi, le musée du Belvédère (Vienne) a proposé à la vente, en février 2022, 10 000 NFT représentant chacun un fragment de l'image du *Baiser* de Gustav Klimt, découpée selon une grille de 100 × 100, chacun au prix de 1 850 €. De façon proche, l'entreprise française *LaCollection* a contracté avec le *British Museum* pour l'émission de « jumeaux numériques » d'œuvres de l'artiste japonais Hokusaï destinées à la vente : chaque estampe a fait l'objet d'une émission de 11 117 jetons classés par niveau de rareté (de « commune », 10 000 exemplaires, à « ultra-rare », deux exemplaires). Ces NFT sont alternativement présentés dans la communication du musée comme des « jumeaux numériques » ou comme des « cartes postales numériques » sur les œuvres.

**Ce cas d'usage connaît cependant un ralentissement, notamment du fait du risque d'image que représentent la vente et la privatisation d'objets présentés comme des « jumeaux numériques » de trésors nationaux**. Par ailleurs, malgré le dynamisme du marché des NFT entre 2020 et 2022, les bénéfices financiers pour les institutions sont limités : la vente par la galerie des Offices du « jumeau numérique » du *Tondo Doni* n'a rapporté à l'institution que 70 000 €, une fois déduits les coûts engagés pour l'opération. S'en est suivie une polémique, en Italie, sur la pertinence de telles opérations, en ce qu'elles donnaient l'impression que des trésors nationaux étaient cédés à des particuliers pour des sommes jugées dérisoires. Plusieurs institutions se sont refusé à communiquer sur les bénéfices réalisés lors de leurs opérations de vente de « jumeaux numériques ». **Le gouvernement italien a en conséquence enjoint, en juillet 2022, à ses opérateurs de mettre fin à la pratique de vente de « jumeaux numériques ».**

**À la connaissance de la mission, aucun musée français n'a pour l'instant publiquement expérimenté la « tokénisation » d'œuvres qu'il détient.** Les risques d'image, la faiblesse des ressources propres espérées et le retournement du marché intervenu à l'automne 2022 sont les raisons les plus souvent citées par les acteurs rencontrés par la mission.

Au-delà de la vente de « jumeaux numériques » à des fins mercantiles, plusieurs institutions envisagent le NFT comme un moyen de proposer de nouvelles formes de médiation culturelle, pouvant associer selon les projets l'usage de la vidéo, des *smartphones*, d'internet, de la réalité virtuelle ou augmentée. Toutefois, au printemps 2023, peu de projets concrets ont encore émergé en la matière : une difficulté récurrente consiste à identifier en quoi le jeton cessible pourrait ajouter un intérêt aux technologies susmentionnées.

Enfin, l'entreprise française *LaCollection* a contracté avec le *Museum of Fine Arts* de Boston pour la création de « jumeaux numériques » de pastels impressionnistes fragiles et rarement exposés, destinés à être présentés au musée des impressionnismes (Giverny), c'est-à-dire affichés sur des écrans numériques. Cette dernière démarche est toutefois surprenante, puisque l'existence du NFT n'est en rien nécessaire pour que le musée de Giverny puisse afficher les œuvres sur écran numérique.

### 2.1.5. Les musées, qu'ils soient publics ou privés, sont susceptibles de faire l'acquisition de NFT d'art « natif », en tant que commanditaires, acheteurs ou légataires, sans que cela appelle de cadre spécifique

Ils peuvent tout d'abord se porter acquéreur d'œuvres « natives ». C'est ce qu'ont fait, en France, le musée Granet d'Aix-en-Provence en janvier 2023 et le centre Georges-Pompidou à Paris en février 2023 — il s'agit, à la date de rédaction du présent rapport, des deux seuls musées publics français ayant acquis des œuvres d'« art natif » NFT.

S'agissant du musée Granet, l'acquisition s'est faite dans le cadre d'un appel à projets « *Sphère code cylindre : NFT et art numérique* ». Le musée a contracté avec des artistes contemporains pour la création d'œuvres et l'émission, sur huit d'entre elles, de deux NFT : l'un remis au musée et destiné à être conservé et l'autre remis à l'artiste et susceptible d'être commercialisé. Les œuvres sous-jacentes aux NFT ne sont pas uniquement des fichiers picturaux. Par exemple, l'une des œuvres, produites par Gauthier Le Rouzic, consiste en une série de sculptures obtenues à partir d'une statuette perse numérisée puis imprimée en 3D quinze fois successives, afin d'illustrer la perte de données : les quinze impressions sont exposées au musée, tandis que les NFT pointent vers un fichier numérique comportant les quinze scans 3D prêts à être réimprimés. À la connaissance de la mission, en mars 2023, les acquisitions n'avaient pas encore été évaluées par la commission scientifique régionale des musées de France prévue par les articles L. 451-1 et R. 451-2 du code du patrimoine.

S'agissant du centre Georges-Pompidou, l'acquisition a porté sur dix-huit œuvres d'« art natif » préexistantes. Les œuvres ont été obtenues par achat, don ou legs. **Il est à noter que le musée est passé par des contrats d'acquisition traditionnels (les transactions en NFT ne faisant pas office, en eux-mêmes, de contrats), fixant un prix en euros, et n'a pas manipulé de cryptomonnaies.** Le choix du musée a été d'acquérir une collection d'œuvres présentant un intérêt particulier au titre de l'histoire de l'art : soit qu'il s'agisse d'œuvres emblématiques du « crypto-art » (à l'exemple du *Crypto Punk #110*, de la célèbre collection des « cryptopunks »), soit qu'elles présentent des spécificités dans leur conception (par exemple, des œuvres d'art génératif dont le code source figure sur la *blockchain*), soit qu'elles aient pour objet, de façon réflexive, le crypto-art en lui-même. Les œuvres ont vocation à être présentées à compter d'avril 2023 dans le cadre d'une exposition abordant, de façon plus générale, la numérisation de l'art.

#### *2.1.5.1. L'existence d'un NFT associé à une œuvre d'art numérique est indifférente à la politique d'acquisition des œuvres*

Le fait qu'une œuvre d'art soit diffusée par son auteur avec un NFT de cession de droits n'est pas de nature à modifier la politique d'acquisition. Un musée, en particulier, ne cherche pas, par l'achat d'un NFT, à acquérir le jeton en lui-même, mais un droit d'exploitation de l'œuvre sous-jacente.

Cette acquisition est réalisée dans les mêmes conditions que pour toute autre œuvre numérique. En particulier, l'exposition d'une œuvre nécessite l'acquisition du droit patrimonial non-exclusif correspondant auprès de l'auteur et donc son accord écrit. Le ministère de la culture, en 2019[19], relevait que cette condition était rarement remplie, mais cette problématique n'est pas spécifique aux NFT.

La circonstance qu'il existe un jeton non fongible en circulation dont le titulaire bénéficie d'une concession de droits sur l'œuvre est sans conséquence sur cette analyse (*cf.* section 4 de l'annexe IV). Ce n'est que dans le cas où la concession de droits est accordée à titre exclusif au détenteur du NFT que la représentation de l'œuvre par le musée suppose obligatoirement l'acquisition du jeton. Dans les autres cas, **l'acquisition du jeton ne constitue, pour le musée, qu'un accessoire à l'acquisition des droits de représentation de l'œuvre** (*cf.* section 1 de l'annexe IV)**, ainsi qu'un enjeu d'image**.

[19] Ministère de la culture, communiqué de presse *La rémunération du droit de présentation publique*, 18 décembre 2019 (https://www.culture.gouv.fr/Thematiques/Arts-plastiques/Actualites/La-remuneration-du-droit-de-presentation-publique, consulté le 23 mars 2023).

L'opportunité de l'entrée en collection d'une œuvre (ou de droits sur une œuvre lorsque celle-ci est numérique) s'apprécie, pour une œuvre associée à un NFT, dans des circonstances identiques à toute autre œuvre d'art. Elle dépend en particulier du projet scientifique du musée souhaitant réaliser l'acquisition et, pour les collections des musées de France, suppose le suivi d'une procédure prévue à l'article L. 451-1 du code du patrimoine et destinée à garantir l'intérêt public de l'opération. À titre d'exemple, l'acquisition, par le centre Georges-Pompidou d'œuvres d'art numériques associées à des NFT en février 2023 est motivée par l'intérêt que présentent les œuvres pour l'histoire de l'art contemporain et donc par la stratégie scientifique propre à l'établissement.

**La mission recommande donc que les éventuelles futures acquisitions d'œuvres d'art associées à des NFT par des institutions publiques soient traitées de façon similaire à toute autre acquisition d'œuvres numériques. Pour toute acquisition publique d'une œuvre d'art numérique associée ou non à un NFT, les institutions devraient veiller, par un contrat écrit avec l'auteur ou ses ayants-droit, à ce que l'acquéreur dispose des droits de représentation publique.**

#### *2.1.5.2. La conservation des NFT représente essentiellement un enjeu d'image et non de droits*

En ce qui concerne la conservation, deux problématiques doivent être distinguées :

- d'une part, la conservation du fichier numérique représentant l'œuvre destinée à être exposée. Cette problématique se pose, le plus souvent[20], que l'œuvre soit associée à un NFT ou non. Elle est maîtrisée par les musées d'art contemporain ;
- d'autre part, la conservation de la clef privée nécessaire à la maîtrise du NFT, qui constitue une problématique nouvelle.

**Juridiquement, dès lors que les droits de représentation de l'œuvre numérique ont été cédés à un établissement, un éventuel NFT associé ne comporte plus d'enjeu.** L'œuvre — formellement, les droits de représentation sur l'œuvre numérique — n'a en effet pas vocation à quitter les collections du musée. En effet lorsque l'établissement est classé musée de France, ses collections sont imprescriptibles et inaliénables (art. L. 451-3 et L. 451-5 du code du patrimoine).

En outre, dans la mesure où l'acquisition des droits de représentation suppose un écrit (art. L. 131-2 du code de la propriété intellectuelle), la détention des droits par le musée est assurée par un titre autre que le NFT. La perte ou le vol du NTF ne saurait donc être assimilé, dans ses conséquences, à la perte ou au vol d'une œuvre d'art originale. Sa valeur, enfin, est annihilée une fois l'œuvre ou les droits de représentation sur celle-ci entrés au patrimoine national. En réalité, le titre de droits dans lequel réside la valeur de l'acquisition et dont la conservation doit être garantie par le musée n'est pas le NFT, mais le contrat de cession des droits de représentation.

Les enjeux relatifs à la conservation des clefs ne doivent donc pas être, en droit, surestimés. En particulier, il n'apparaît pas que les règles de la comptabilité publique imposent des modalités particulières de maniement et de conservation des NFT. Tant la détention des clefs par le musée en propre (par exemple sur papier ou sur un disque conservé physiquement dans le coffre de l'agent comptable) ou par un prestataire sont envisageables.

[20] Une exception réside dans les cas où les contenus numériques destinés à être représentés ne sont rendus techniquement accessibles qu'au titulaire du NFT. En ce cas, la conservation numérique de l'œuvre suppose la conservation sous-jacente de la clef privée correspondant à l'adresse du détenteur du NFT.

Toutefois, au-delà des enjeux juridiques, la conservation des NFT pourrait avoir des conséquences en matière d'image, surtout tant que le grand public confond la détention du NFT à la détention de l'œuvre en elle-même — ce à quoi la mission recommande de remédier en évitant que les institutions publiques adoptent une communication ambiguë sur ce point. Il relève donc des choix de chaque établissement d'adopter une solution de conservation en fonction de ses capacités techniques et de sa stratégie de marque. **Le service du numérique du ministère de la culture pourrait utilement accompagner les établissements en émettant, notamment, des lignes directrices concernant les solutions techniques recommandées**.

## 2.2. Les NFT sont envisagés par de nombreux acteurs du monde de la culture comme une façon de maîtriser et de monétiser leur image de marque et leur patrimoine culturel

L'utilisation des « jumeaux numériques » connaît, dans le secteur des arts picturaux, une certaine porosité avec trois autres cas d'usage : l'émission de produits dérivés, le mécénat et la gestion de droits. Ces cas d'usage sont également présents, le plus souvent sans l'idée de « jumeaux numériques » sous-jacente, s'agissant des autres domaines de l'art et de la culture.

### 2.2.1. La vente de produits dérivés constitue le principal cas d'usage transversal au monde de la culture

#### *2.2.1.1. Ce cas d'usage est répandu dans l'ensemble des domaines artistiques : arts graphiques, arts du spectacle, monuments, musique ou encore bande dessinée*

**Le principe général des produits dérivés NFT réside dans l'émission de jetons associés à la propriété intellectuelle d'une institution.** Par exemple, pour un musée, le produit dérivé peut, de façon simple, correspondre à une « carte postale » d'une œuvre. Celle-ci peut alors être affichée par l'utilisateur, toujours de façon ostentatoire. La détention du NFT peut, dans certains cas, donner accès à des contenus interactifs complémentaires, par exemple, des animations autour de l'image apparaissant sur le téléphone du détenteur s'il l'ouvre avec une application qui le permet. Souvent, est également envisagé l'accès à une « communauté » : les détenteurs du NFT peuvent par exemple voir leur nom publié au sein d'une liste de soutiens, accéder à des espaces de discussion réservés ou obtenir l'accès à des événements privatifs. Ces services rapprochent alors l'achat du NFT d'une forme de mécénat (*cf.* 2.2.2).

S'agissant des musées, des expérimentations en la matière existent, mais elles sont peu nombreuses en France. La réunion des musées nationaux, par l'entremise du Grand Palais immersif[21], a par exemple proposé la vente de « souvenirs numériques NFT » de l'exposition immersive *Venise Révélée* : le NFT porte sur des séquences vidéo et des plans 3D de la ville de Venise à la Renaissance. Ces produits dérivés sont édités par *LaCollection*. La mission n'a en revanche pas eu connaissance d'autres expérimentations par des musées français.

Dans le secteur de la bande dessinée, *LaCollection*, toujours, a contracté avec les éditions Dupuis pour émettre des NFT constituant des produits dérivés de bandes dessinées.

[21] Filiale de l'établissement public *réunion des musées nationaux et du Grand Palais des Champs-Élysées* (Rmn-GP, ÉPIC sous tutelle du ministère de la culture chargé de mutualiser certains services pour les musées de France et d'exploiter certains établissements), de la Caisse des dépôts et consignations (opérant sous la marque Banque des Territoires) et de Vinci Immobilier.

S'agissant des arts du spectacle, l'opéra de Paris a émis en mars 2023 une collection de NFT intitulée *Émergence : ballet algorithmique*, associée à sa marque et conçue par le collectif d'artistes *Obvious*. À chaque jeton est associée une vidéo et une musique conçues par art génératif et évoquant les mouvements d'un danseur. Surtout, les jetons donnent accès, après tirage au sort, à un ensemble de biens et services plus ou moins rares, y compris des places pour des spectacles[22]. La maîtrise d'œuvre technique et juridique est assurée par la société *Polyconseil*.

Dans le secteur du patrimoine immeuble, l'entreprise *EverRose* prévoit de lancer, au premier semestre 2023, des NFT portant sur des monuments, en association avec les organismes qui les exploitent et détiennent les droits de marque associés. Pour chaque monument, une série d'images (photographies ou dessins), dont certaines comportent des fonctionnalités « augmentées » (affichage 3D, animations, *etc.*) seront émises en un nombre limité d'exemplaires. L'entreprise a notamment contracté, à cette fin, avec le Centre des monuments nationaux et la Société d'exploitation de la tour Eiffel.

Dans le domaine de la musique, la startup française *Pianity* exploite une plateforme de *streaming* pour des œuvres d'artistes avec lesquels elle contracte. Les utilisateurs peuvent acquérir des NFT, en tirage limité, pointant vers les fichiers audio. La détention du NFT n'est présentée ni comme la possession des droits sur l'œuvre (qui restent détenus par l'artiste), ni comme une condition pour jouer le titre (la plateforme de *streaming* est accessible publiquement). Elle représente donc avant tout un produit dérivé ostentatoire, permettant d'afficher son intérêt pour l'œuvre. Par ailleurs, la revente des NFT est grevée d'un droit de suite bénéficiant à la plateforme (20 %) et à l'artiste (80 %).

#### *2.2.1.2. Le développement de ce cas d'usage repose surtout sur la standardisation technique que permettent les* blockchains*, mais est difficilement dissociable de la fourniture de biens et services physiques accompagnant les NFT*

La liste précédente ne correspond qu'à un petit nombre d'expérimentations parmi celles qui sont en cours, menées par les seuls acteurs rencontrés par la mission.

Deux points communs apparaissent toutefois de façon transversale à ces cas d'usage.

Il s'agit, d'une part, de **l'importance des « utilités » associées aux NFT**. Les NFT sont rarement vendus comme de simples jetons pouvant être affichés. Ils donnent le plus souvent accès à des services annexes : loterie promotionnelle permettant d'emporter divers lots (privatisation de monuments pour les cartes d'*EverRose*, visites privées et places pour les spectacles de l'opéra de Paris, catalogue de l'exposition pour les NFT souvenirs de *Venise révélée*), accès à des espaces d'échange privés ou parfois délivrance d'un bien physique lié au NFT (envoi d'un disque vinyle de la musique pour certains des NFT de *Pianity*, envoi d'un tirage papier pour certaines œuvres des éditions Dupuis). Il est le plus souvent difficile de distinguer, parmi la valeur vénale du NFT, une part correspondant à l'intérêt intrinsèque du NFT comme bien de consommation ostentatoire et une part correspondant aux services auxquels il donne accès.

D'autre part, **la plupart de ces produits dérivés exploitent la standardisation technique qui s'impose *de facto* dans l'univers Web 3.0**. L'émission est simplifiée par le fait que l'affichage des fichiers numériques associés aux NFT est interopérable, que l'achat peut se faire avec n'importe quel logiciel de portefeuille, que les jetons sont échangeables sur un grand nombre de plateformes, ce qui leur donne de la liquidité. Cette standardisation permet par exemple pour les émetteurs :

[22] Ces places de spectacles, à la différence des jetons, sont incessibles après le tirage au sort.

- une exploitation de données personnelles des acheteurs. Le détenteur d'un NFT et ses transactions étant publics, l'auteur des produits dérivés peut utiliser ceux-ci pour connaître ses clients et le cas échéant cibler ses démarches commerciales — ce qui représente des enjeux significatifs en termes de protection de la vie privée, *cf.* section 4 de l'annexe V ;
- une forme de maîtrise de l'image de marque, liée notamment à la mise en valeur par les réseaux sociaux des contenus associés à un NFT « officiel ». Un musée peut par exemple inciter ses utilisateurs à partager les « cartes postales souvenir » (payantes), avec des photographies et des messages standardisés validés par son service de communication, plutôt que des photographies prises individuellement, parfois de mauvaise qualité.

En outre, les acteurs du secteur réalisent en règle général un **pari selon lequel la valeur des NFT pourrait augmenter si, dans un environnement mieux maîtrisé, leur détention pouvait conférer des droits** : soit au sens juridique (droits de propriété intellectuelle reconnus au détenteur d'un NFT), soit dans un sens technique (accès de certaines fonctionnalités au détenteur d'un NFT uniquement, grâce à une fermeture des environnements techniques et une maîtrise plus importante des copies d'œuvres par les fournisseurs de logiciels et de matériel).

### 2.2.2. À la frontière de la vente de produits dérivés, l'achat de NFT est parfois associé à des actions de mécénat

**Les émissions de NFT peuvent servir à des opérations de mécénat.** Plutôt que la simple vente d'une « carte postale » ou d'un « jumeau numérique », le NFT est conçu comme un produit montrant la participation de l'acheteur à une opération précise, par exemple la restauration d'une œuvre. La détention du NFT permet d'afficher publiquement sa participation. Le NFT permet ensuite de rendre cessible l'effet d'image associé à la participation financière.

Il est difficile de tracer une frontière nette entre ce cas d'usage et l'émission de produits dérivés ou de « jumeaux numériques ». Par exemple, les NFT sur des titres musicaux commercialisés par *Pianity* empruntent des trois natures : le jeton pointe vers la musique et peut donc être présenté comme un « double numérique », il constitue avec sa jaquette un produit dérivé de l'œuvre, mais l'une des utilités de l'achat est aussi de pouvoir soutenir et afficher son soutien à un artiste. Un tel achat peut être rapproché de l'achat d'un disque vinyle d'une œuvre musicale par un consommateur de musique qui possède un abonnement à une plateforme de *streaming* et peut donc déjà l'écouter de façon illimitée.

Les institutions culturelles rencontrées par la mission ont fait part de plusieurs projets de mécénat à des stades encore précoces, sous le sceau de la confidentialité. Une analyse toutefois prédominante est que le NFT ne constitue qu'un élément marginal d'une telle opération : la collecte de fonds, pour avoir une chance de réussir, doit avant tout partir d'un projet d'acquisition ou de restauration bien élaboré et susceptible d'intéresser les mécènes, le NFT ne constituant qu'un instrument technique destiné à faciliter l'ostentation et susciter l'intérêt.

### 2.2.3. La possibilité que les NFT permettent une meilleure maîtrise des droits sur les œuvres du patrimoine national reste incertaine, tant dans sa faisabilité que dans son opportunité

Un constat consensuel parmi les acteurs du monde de la culture rencontrés par la mission est que l'utilisation des technologies numériques, en facilitant la copie de contenus, fait obstacle à la maîtrise par les auteurs, les éditeurs et les institutions culturelles de leur propriété intellectuelle et engendre des manques à gagner. Ce constat est notamment fondé en ce qui concerne la contrefaçon sur internet d'œuvres couvertes par le droit d'auteur. La possibilité que les NFT puissent représenter un titre de droit sur l'exploitation de ces œuvres est étudiée en section 4 de l'annexe IV.

Le constat est cependant davantage controversé en ce qui concerne l'exploitation des biens culturels immatériels lorsqu'elle n'est plus protégée par le droit d'auteur. Conformément aux articles L. 123-1 *sq.* du code de la propriété intellectuelle, le monopole sur l'exploitation des œuvres qui est garanti à l'auteur puis à ses ayants-droits expire, en principe, 70 ans après la mort de l'auteur. Par ailleurs, l'exploitation, même à des fins commerciales, de l'image d'un bien relevant du domaine public a été jugée par le Conseil d'État dans le contentieux opposant les brasseries Kronenbourg au domaine national de Chambord comme ne constituant pas une occupation privative et ne pouvant donner lieu à redevance à ce titre — sauf dans le cas où la prise d'image implique une utilisation privative du domaine public[23].

En introduisant, par la loi n° 2016-925 du 7 juillet 2016 relative à la liberté de création, à l'architecture et au patrimoine, l'article L. 621-42 dans le code du patrimoine, le législateur a entendu soumettre à autorisation préalable et à redevance l'utilisation à des fins commerciales de l'image des immeubles qui constituent les domaines nationaux, sur tous supports, exception faite des exploitations à finalité culturelle, artistique, pédagogique, d'enseignement, de recherche, d'information ou d'illustration de l'actualité. Il ressort des travaux préparatoires de la loi que l'objet de cette disposition est de créer des droits d'exclusivité sur l'exploitation des biens culturels publics afin de créer une source de revenus financiers supplémentaires pour leurs gestionnaires, que ceux-ci doivent alors gérer.

Cependant, cette disposition spécifique ne concerne que l'image desdits domaines, à l'exclusion du reste du patrimoine national. Ainsi, par exemple, l'émission d'un NFT sur *La Joconde* ne peut être soumise à autorisation préalable de l'établissement public du musée du Louvre — sauf si le NFT utilise l'image de marque de l'établissement, couverte par la propriété industrielle.

**Dans ce contexte, l'utilisation des NFT à des fins de maîtrise d'image est envisagée par l'écosystème, mais son opportunité ne fait pas l'objet d'un constat partagé.** En réalité, cette préoccupation comprend deux composantes bien distinctes : l'évitement d'un manque à gagner dans l'émission des NFT en eux-mêmes et la restriction technique des possibilités de copies illicites.

Dans les deux cas, la mission constate que **les opérateurs sont principalement dans une approche « essayer et apprendre » (*test and learn*), mais pressés par la crainte de voir une source de recettes propres importante leur échapper**, gardant en mémoire le contentieux ayant opposé l'établissement public du domaine national de Chambord aux brasseries Kronenbourg à ce sujet entre 2010 et 2018.

---

[23] Conseil d'État, assemblée, 13 avril 2018, n° 397.047, *Établissement public du domaine national de Chambord*, considérant 6. Dans cette affaire, la société Les Brasseries Kronenbourg avait réalisé une publicité intitulée *1664 : Le goût à la française* et exploitant l'image du château de Chambord. L'établissement public du domaine national de Chambord avait défendu que cette exploitation commerciale de l'image du domaine public revenait à une occupation privative de celui-ci, soumise à redevance, mais ses prétentions n'avaient pas été accueillies par le Conseil d'État. Une intervention du législateur a donc été nécessaire pour permettre à l'établissement public de monétiser l'image du domaine public dont il est propriétaire.

#### *2.2.3.1. Certains opérateurs culturels envisagent l'utilisation de NFT afin de précéder les diffusions « pirates »*

Les acteurs rencontrés partagent entre eux l'opinion selon laquelle **la tokénisation de biens culturels lors du marché haussier de 2020 à 2022 aurait constitué un manque à gagner pour les opérateurs culturels.** Même en mars 2023, alors que le marché des NFT a connu une forte baisse, des NFT présentés comme « *Mona Lisa Original* » sont régulièrement vendus pour des prix de l'ordre du millier d'euros[24]. L'adoption d'une stratégie NFT par ces institutions viserait donc à précéder les tokénisations « pirates » de tokénisations « authentiques », réalisées par les institutions détentrices des œuvres du patrimoine national.

Toutefois, l'existence d'un manque à gagner reste difficile à prouver. L'engouement pour la tokénisation d'œuvres célèbres est survenu alors même qu'aucun droit ne leur est associé. Il est incertain que l'existence de copies « officielles » aurait suffi à assécher le marché des copies « pirates », tant l'achat de ces jetons relève de logiques irrationnelles.

**Outre les NFT, les institutions rencontrées envisagent d'établir leur présence dans les principaux métavers grand public** : il s'agirait, dans la même logique, d'éviter la création de répliques « pirates » de musées ou des domaines nationaux. La détention de NFT pourrait alors être rendue nécessaire pour certifier l'authenticité de la reproduction du musée ou du domaine dans le métavers (*cf.* 2.2.3.2).

L'opportunité de ce choix n'est cependant pas consensuelle parmi les acteurs du monde de la culture rencontrés. La création d'un musée dans un métavers représente d'importants coûts de développement et fait peser des risques d'image compte tenu de la difficulté qui réside dans la réalisation de graphismes satisfaisants. Enfin, **l'idée qu'un musée devrait lutter contre la création de répliques virtuelles n'est elle-même pas consensuelle** : la logique d'ouverture des données publiques pourrait au contraire conduire à tolérer, voire à inciter la diffusion la plus large possible des œuvres relevant du patrimoine national. Enfin, la lutte contre les reproductions « pirates » peut passer par d'autres outils : si elles utilisent une image de marque protégée et contreviennent donc aux droits de l'établissement, celui-ci peut déposer un recours, sans avoir pour autant à créer son espace « officiel » dans le métavers concerné. Si au contraire la reproduction ne contrevient à aucun droit, l'opportunité de lutter contre ce phénomène est contestable.

#### *2.2.3.2. Des procédés techniques futurs pourraient associer le NFT à des droits exclusifs d'utilisation d'une image*

Un nombre important d'acteurs rencontrés envisagent un scénario dans lequel, à l'avenir, **la détention d'un NFT pourrait être indissociable de la possibilité d'exploiter certains contenus culturels**. Certains environnements techniques (métavers, écrans d'affichage bridés…) pourraient contrôler l'utilisation d'images et ne l'autoriser que pour le détenteur d'un NFT associé. Ainsi, par exemple :

- la projection d'une photographie sur un cadre numérique bridé supposerait de détenir un NFT associé ;
- seul le propriétaire d'un NFT associé à un tableau pourrait le détenir dans un métavers ;
- l'éditeur de ce même métavers pourrait interdire la reproduction de bâtiments publics, sauf à une personne détenant un NFT « de » ce bâtiment ;
- un NFT pourrait représenter des droits de marque exploitables dans ce métavers.

[24] Voir notamment sur *OpenSea*, la collection *Mona Lisa Original* de *ElmonX* : https://opensea.io/fr/collection/elmonxmonalisaoriginal?search[sortAscending]=false&search[sortBy]=LAST_SALE_DATE. Entre le 26 février 2023 et le 27 mars 2023, les ventes de ces NFT représentent un volume d'environ 77 éthers, soit plus de 100 000 €.

Cette idée constitue une autre motivation à explorer, tester et apprendre les technologies des NFT, selon les acteurs rencontrés. Elle comporte toutefois des limites fortes dans la mesure où :

- ce cas d'usage suppose de réaliser des contrôles automatiques des contenus multimédias diffusés (sur les cadres, dans les métavers, *etc.*) afin de pouvoir censurer les œuvres sur lesquelles l'utilisateur ne détient pas les droits représentés par un NFT. Cependant, une telle détection automatique de contenus soumis à droit d'auteur pose de sérieuses difficultés techniques et donne encore aujourd'hui lieu à de nombreux faux-positifs ;
- tout un chacun peut émettre un NFT sur une image de son choix. Le contrôle de l'authenticité des NFT émis sur une image couverte par des droits supposerait donc un certain niveau de centralisation pour vérifier que l'émetteur d'un NFT sur une image détient bien les droits y associés, en contradiction avec les promesses du « Web 3.0 » ;
- la viabilité économique du modèle est incertaine. Les acheteurs de biens et services numériques auraient en effet davantage intérêt à choisir un modèle non-bridé pour les matériels et services qui existent déjà. Ce n'est que sur les produits nouveaux que le bridage pourrait être envisagé comme la solution technique par défaut.

**L'opportunité même d'une telle évolution est par ailleurs hautement contestable**, dans la mesure où elle induirait des obstacles à la libre diffusion des œuvres qui ne sont plus couvertes par des droits d'auteur motivée uniquement par la recherche de revenus financiers supplémentaires pour des personnes publiques. Ce faisant, elle irait à contre-courant du choix de politique publique porté par le ministère de la culture consistant à encourager la libre-diffusion des œuvres du patrimoine national, qu'illustrait par exemple la campagne *Tous photographes* de 2014.

## 2.3. Les NFT peuvent enfin être utilisés dans le milieu de l'art et de la culture pour des finalités techniques ou de gestion de droits

En marge des principaux cas d'usage décrits en section 2.1 et 2.2, la mission a identifié quelques cas d'usages marginaux pour lesquels les NFT sont utilisés à des fins techniques ou de gestion de droit dans le domaine des arts et de la culture.

Ainsi, s'agissant des ventes aux enchères, la maison londonienne *Christie's* a développé une solution fondée sur le recours à des NFT pour représenter les œuvres et les enchères réalisées sur celles-ci. L'objectif principal, selon les promoteurs du projet, est d'assurer après-coup une transparence sur la circulation des œuvres.

**En matière de gestion de droits, des réflexions sont engagées notamment dans le secteur de la musique et du cinéma.** Dans chaque cas, l'objectif est d'utiliser le caractère interopérable des *blockchains* et l'automatisation permise par les programmes autonomes (« *smart contracts* ») pour représenter, par des jetons adéquats, les droits et obligations des personnes ayant participé à la création d'une œuvre et les flux financiers complexes qui peuvent en résulter. Par exemple, un détenteur de jeton représentant un droit voisin au droit d'auteur et l'acquéreur de jeton servant à financer la production d'un film pourraient percevoir, automatiquement, une part des bénéfices issus de l'exploitation du film. Les finalités principales sont de faciliter et d'accélérer les flux financiers en automatisant le calcul des redevances d'exploitation de contenus soumis aux droits d'auteur et droits voisins et de créer de la liquidité en facilitant la revente de créances. De tels travaux sont notamment menés, dans le cinéma, par l'entreprise française *Cascade8*.

Ces cas d'usage relèvent cependant davantage de la finance décentralisée que de l'utilisation commerciale grand public des actifs numériques. Ils n'atteindraient leur potentiel maximal qu'en cas d'automatisation des flux financiers, directement sur la *blockchain*. Ce cas suppose que les flux soient réalisés en cryptoactifs (lesquels pourraient être des *stablecoins*, afin d'accroître leur acceptabilité) et que le programme autonome puisse servir de contrat régissant les droits. Or, ces deux hypothèses ne sont pas satisfaites. Les NFT sont donc actuellement utilisés uniquement pour le calcul des droits et les flux financiers sont eux, opérés en dehors de la *blockchain*, en monnaie *fiat*. Par ailleurs, l'utilisation de jetons pour représenter la détention des droits moraux sur une œuvre, incessibles, est également envisagée et s'apparente davantage au cas d'usage de l'identité numérique décentralisée.

**Enfin, l'utilisation des NFT pour gérer la billetterie d'événements culturels ou sportifs constitue un cas d'usage bien identifié**. Il présente pour les organisateurs l'intérêt de contrôler le marché secondaire et de pouvoir automatiser la perception de flux financiers sur la revente et pour les spectateurs de pouvoir céder leurs billets sur le marché secondaire de façon sécurisée, sans risque de duplication frauduleuse du billet revendu. Des projets sont portés en la matière, tant par des entreprises de billetterie classiques (*TicketMaster*) que par des startups spécialisées (*Billy*, *Tesschain*, *Tailor NFT*). En l'absence de barrière à l'entrée, ce secteur de marché est fortement concurrentiel : les innovations résident principalement dans le fait d'associer aux tickets des contenus ou des « souvenirs ».

## 3. Les NFT sont utilisés dans le secteur de la consommation, soit en tant qu'objets de consommation virtuels, soit en tant qu'objets numériques associés à des biens ou à des projets réels

### 3.1. Grâce à leur non fongibilité, les NFT peuvent être utilisés dans les mondes virtuels comme des biens de consommation

**Les NFT ayant pour propriété d'être non fongibles et cessibles, ils reproduisent dans le monde numérique la notion de propriété en permettant de reconnaître à un détenteur unique des droits**. Ces droits sont limités puisque l'image vers laquelle les NFT pointent dans la plupart des cas reste librement accessible sur des sites de stockage, souvent décentralisés. Néanmoins, l'émission du NFT permet de désigner un « *propriétaire* » légitime — sa légitimité reposant uniquement sur le fait qu'il l'a payé — et de le distinguer des autres utilisateurs qui auraient téléchargé l'image sans pour autant être « propriétaires » de ces droits.

**Cette réplication de la « propriété » dans le monde numérique permet de créer de la rareté là où elle était difficile à imaginer, puisque les fichiers numériques sont reproductibles à l'infini**. Cette « propriété », qui a d'abord permis de faire naître sur les *blockchains* des « monnaies » numériques, comme le bitcoin (sans elle, une monnaie numérique aurait pu être créée sans limite par tout un chacun et aurait donc été inopérante), permet aussi, *via* les NFT, de donner une valeur marchande à un objet numérique en garantissant à son acquéreur qu'il en sera le seul détenteur légitime.

**Les NFT peuvent donc devenir des biens de consommation comparables aux biens réels, à condition que la jouissance de leur « propriété » soit considérée comme source d'utilité pour les consommateurs.** La combinaison des métavers et des NFT est, à ce titre, fondamentale. Les objets numériques désignés par les NFT sont, en effet, d'autant plus « utiles » qu'ils peuvent être utilisés dans un monde virtuel où leur possession est valorisée par les consommateurs. Si un éditeur de métavers s'engage à ne permettre d'arborer un objet (notamment, un accessoire, bijou ou vêtement) qu'aux utilisateurs détenteurs du NFT correspondant[25], alors le NFT devient gage de différenciation, comme la propriété de l'objet réel équivalent (l'accessoire, le bijou ou le vêtement) l'est dans le monde réel.

La logique de consommation ostentatoire peut donc, grâce aux NFT, être importée dans les mondes virtuels des métavers, à deux différences près :

- les objets acquis dans le monde virtuel n'apportent pas à leur acquéreur l'utilité pratique que leurs équivalents réels proposent, en plus de leur valeur ostentatoire (un sac de luxe permet de transporter des affaires personnelles, un NFT de sac de luxe, non) ;
- la jouissance du bien acquis et les possibilités qu'offre sa détention sont conditionnées au fonctionnement du métavers et donc aux règles établies par son éditeur. Le métavers peut ainsi cesser d'exister si son éditeur ne le maintient plus tandis qu'un changement dans les programmes permettant de l'explorer peuvent suffire à faire disparaître ou à dénaturer les objets virtuels que le joueur détient.

Les NFT peuvent donc représenter des objets de consommation similaires aux objets « classiques », mais utilisés par les consommateurs pour leur avatar numérique. Cette possibilité ouvre des perspectives de débouchés aux industries produisant des biens susceptibles de faire l'objet d'un tel désir ostentatoire, au premier rang desquelles le secteur du luxe. C'est pourquoi certaines marques ont d'ores et déjà lancé des collections de NFT représentant des produits à porter dans le monde virtuel. Lorsque l'objet est une image, le cas d'usage se rapproche des NFT artistiques (*cf.* 2.1), qui peuvent néanmoins être associés à une logique de consommation ostentatoire. Par exemple, la marque d'horlogerie Tag Heuer, propriété du groupe LVMH, a développé en 2022 une série de montres « *Tag Heuer connected* » permettant d'afficher en fond un NFT grâce à une connexion entre la montre et le portefeuille de cryptoactifs, accompagnée d'une preuve visuelle de propriété : en cas de propriété de NFT détectée grâce au portefeuille, l'image associée apparaît dans un hexagone avec un nuage de particules gravitant autour de l'image.

**L'intérêt des marques de mode pour le monde virtuel a été inauguré par leur pénétration du marché des jeux vidéo**. Avant l'émergence du Web 3.0, plusieurs maisons ont collaboré avec des jeux grand public pour toucher de nouveaux types de clientèles. Dès 2019, Louis Vuitton, leader du luxe mondial, collaborait avec le jeu *League of Legends* à l'occasion du championnat du monde se déroulant à Paris. Plusieurs tenues (« *skins* ») sont dessinées par la marque pour les personnages du jeu. En 2021, la maison Balenciaga faisait de même avec le jeu *Fortnite*, jeu au succès mondial réunissant d'après le site Statista 350 millions de joueurs. La même année, Gucci, autre maison du groupe français Kering, a lancé une première collection virtuelle dans le métavers Roblox : la marque a présenté dans Roblox son exposition *Gucci Archetypes*, aussi présente dans le monde réel, à Florence, et avait vendu à cette occasion des objets numériques. Un exemplaire numérique du sac « *Dionysos avec abeille* » avait attiré l'attention en se revendant à environ 4 115 $ quelques jours plus tard, soit plus que le prix de son équivalent réel, s'élevant à 3 400 $.

[25] Ce qui constitue une condition non négligeable qui limite l'intérêt des NFT-biens de consommation pris isolément.

**Dans chacun de ces cas, les objets n'étaient pas liés à des NFT et ne pouvaient donc pas quitter l'univers du jeu dans lesquels ils étaient conçus**. Le développement des NFT et des métavers pourrait donner une nouvelle dimension à ce mode de consommation numérique en promettant une interopérabilité entre univers numériques : un sac de luxe pourrait ainsi être acheté en tant que NFT et être utilisé à la fois dans un métavers social et un jeu vidéo de combats, par exemple.

Cette promesse n'est pas encore tenue et l'interopérabilité n'est pas acquise. Certaines initiatives émergent pour connecter les différents métavers et garantir cette interopérabilité, nécessaire au développement du marché. Ainsi, la marque d'habillement américaine Tommy Hilfiger a ouvert, en mars 2023, une boutique dans le métavers Decentraland qui permet de connecter les utilisateurs à quatre autres métavers (Roblox, Spatial, DressX et Ready Player Me). Dans l'attente de la structuration du marché et de la standardisation des technologies, le Web 3.0 continue de représenter une opportunité de développement pour l'industrie de la mode et du luxe, mais les entreprises rencontrées par la mission ont toutes indiqué appréhender ce nouveau segment de manière exploratoire.

**D'un côté, la consommation dans le monde virtuel permet à ces marques de toucher de nouveaux clients, qui n'auraient pas les moyens d'acheter leurs produits réels, de cultiver leur image de marque en développant la créativité et en renforçant le sentiment d'appartenance, ainsi que de répliquer la rareté de leurs produits dans un nouveau monde, tout en bénéficiant financièrement des reventes[26].** La combinaison des NFT avec le métavers peut permettre aux marques de proposer à leurs clients des expériences nouvelles, dans un univers virtuel, qui peut comporter une dimension de jeu (« gamification »), une dimension sociale (nombreux salons de discussion associés aux NFT, en particulier sur le réseau social *Discord*) ou simplement un acte d'achat dans une réalité augmentée qui peut prendre des formes encore plus créatives que les boutiques réelles.

**De l'autre, la consommation dans le monde virtuel ne permet pas d'associer les produits aux notions de savoir-faire et de qualité, qui sont souvent au cœur de l'image de marque de ces maisons et se limite actuellement à des communautés réduites de technophiles, qui ne peuvent pour l'instant pas constituer de réels relais de croissance des ventes.** L'utilisation de NFT suppose d'avoir les outils pour interagir avec une *blockchain* (« portefeuille », cryptomonnaies), ce qui constitue une barrière à l'entrée et provoque une expérience client généralement peu fluide. Par ailleurs, elle pose un vrai défi de détermination du juste prix : une marque de luxe a-t-elle intérêt à vendre des NFT à des prix accessibles pour élargir sa clientèle, au risque de brouiller son positionnement, ou d'afficher des prix comparables à ceux de ses produits réels, au risque qu'ils soient injustifiés au vu de l'immatérialité du produit ?

Le lancement de la collection de NFT *911* par le constructeur d'automobiles Porsche a, par exemple, été sévèrement jugé par la communauté des utilisateurs du Web 3.0. Lancée en janvier 2023, la collection, dotée initialement de 7 500 exemplaires représentant des Porsche 911, a finalement été arrêtée alors que seul un quart des NFT avaient été vendus. Les internautes ont notamment critiqué le prix de vente des NFT, 0,9 éther soit environ 1 350 €, pour des avantages jugés trop flous, dans une période de retournement de marché pour les NFT et de perte de valeur.

[26] Les « *smart contracts* » à l'origine des NFT peuvent prévoir que toute revente du NFT engendrera le versement d'une commission à l'émetteur initial, en l'occurrence la marque. Le marché d'occasion des NFT est donc plus facilement traçable et valorisable financièrement pour les marques que le marché d'occasion réel.

**Ces différentes raisons expliquent les approches hybrides des marques, qui utilisent l'innovation de la *blockchain* et des NFT selon des formats variés**, mêlant objet de consommation numérique, dimension artistique, appartenance à une communauté, voire accès à une expérience réelle. Ainsi, Gucci a développé plusieurs initiatives liées au Web 3.0, notamment Gucci Vault Land, un espace dans le métavers The Sandbox et plusieurs collections de NFT, comme SuperGucci, en partenariat avec la startup Superplastic, en février 2022. Dans le cas de cette collection, le NFT, représentant un personnage de Superplastic aux couleurs de la marque, est accompagné d'un objet réel, une sculpture en porcelaine. En 2022, Balenciaga a émis 10 000 NFT représentant des dessins du fondateur, Cristobal Balenciaga, dans une collection appelée *To the Moon*, où chaque NFT était associé à des récompenses (cartes cadeaux, tickets de concert, *etc.*).

La proximité naturelle entre la logique ostentatoire propre aux objets de luxe et celle qui préside à l'acquisition de NFT place le secteur du luxe comme premier utilisateur potentiel du cas d'usage de la vente de NFT en tant que biens de consommation. Preuve de cette accointance, une première « *Metaverse fashion week* » a eu lieu dans le métavers Decentraland du 24 au 27 mars 2022, dupliquant les événements d'une « *fashion week* » réelle : défilés, conférences, soirées, *etc.* Cet événement a été renouvelé en 2023, du 28 au 31 mars. De ce fait, la France, siège des plus grands groupes de luxe au monde (LVMH, Kering, Hermès, Chanel, *etc.*), possède un avantage comparatif en la matière, qui pourrait constituer un atout si elle voulait favoriser le développement des NFT.

## 3.2. Les NFT peuvent représenter un outil de marketing offrant de nouveaux modes d'accès à la clientèle

### 3.2.1. Les NFT peuvent constituer des « passeports numériques » pour des produits réels

Quand ils ne sont pas vendus en tant que biens de consommation virtuels, les NFT peuvent être utilisés comme accessoires numériques, émis à titre gratuit la plupart du temps, associés à l'acquisition d'un bien de consommation réel. À ce titre, un NFT peut représenter un « passeport numérique » lié à un objet et remplir plusieurs rôles.

**Le NFT peut constituer une preuve d'achat numérique qui contient des informations sur le produit (composition, caractéristiques techniques, guide d'entretien etc.), éventuellement d'identification individuelle (numéro de série, modèle etc.), et qui peut être utilisée dans la relation entre le client et la marque, par exemple pour faire valoir des droits (entretien, garantie)**. Dans cette même logique, le NFT peut contenir des informations en matière de traçabilité du produit, à des fins de responsabilité sociale de l'entreprise vendeuse. Utilisés à cette fin, les NFT pourraient constituer le support du « passeport numérique produit » prévu par un règlement européen en cours de négociation.

**Encadré 5 : Le « passeport numérique produit » européen**

L'éco-conception vise à limiter l'impact sur l'environnement d'un produit tout au long de son cycle de vie (production, distribution, utilisation, fin de vie). Outre les modifications de mode de production et de distribution, l'éco-conception passe par la promotion de l'économie circulaire, qui consiste à réutiliser des produits en fin de vie afin de limiter à la fois la pollution et la production de produits nouveaux.

Au sein de l'Union européenne, la directive 2009/125/CE a posé des exigences en matière d'étiquetage énergétique pour certains groupes de produits électroniques (éclairage, ordinateurs, électroménager, *etc.*). L'information du consommateur fait partie des outils mobilisés pour orienter les comportements afin de permettre à l'Union européenne de respecter ses objectifs environnementaux.

La Commission européenne a soumis, le 30 mars 2022, une proposition de règlement[27] abrogeant la directive 2009/125/CE et élargissant le périmètre des exigences en matière d'écoconception. Ce projet, en cours de négociation, prévoit l'obligation d'associer à chaque produit mis sur le marché un passeport numérique (article 8). Les informations présentes dans le passeport et les autres modalités de mise en œuvre doivent être précisées dans un acte délégué.

Ce passeport numérique doit permettre de fournir au consommateur des informations sur la traçabilité des composants, sur la durabilité du produit et sur son impact environnemental. Il devrait également faciliter la réparation et le recyclage par une bonne information.

L'obligation du passeport numérique devrait progressivement entrer en vigueur, par groupe de produits (textile, batteries, matériel électronique, *etc.*). Le calendrier d'entrée en vigueur doit encore être déterminé.

*Source : Mission, site internet du ministère de la transition écologique, site internet de la Commission européenne.*

Cette preuve d'achat, qui équivaut à considérer le NFT comme un titre de propriété (reconnu uniquement par la marque vendeuse), peut aussi être utilisé par le client vis-à-vis d'un autre particulier, en cas de revente sur un marché secondaire. La détention du NFT officiel, émis par la marque et associé à l'objet, permet à l'acquéreur de s'assurer que l'objet n'a pas été volé. En revanche, le NFT ne peut pas servir de garantie d'authenticité puisque rien n'assure à l'acquéreur que l'objet qu'il a sous les yeux est bien l'objet initialement associé au NFT par la marque, sauf à ce que l'objet en question soit marqué d'un identifiant le rattachant au NFT, comme un numéro de série ou un QR code.

Ce cas d'usage est au fondement du lancement, en avril 2021, du consortium Aura Blockchain. Créé par LVMH, Prada et Cartier, ce consortium vise à développer une solution technologique basée sur la blockchain *Quorum* à destination des groupes de luxe permettant de diffuser à grande échelle les certificats numériques d'authenticité et de traçabilité. Ce service de passeport numérique est également proposé par la startup française Arianee, fondée en 2018, qui enrichit cette fonction par l'intégration d'une messagerie facilitant le lien entre la marque et le propriétaire du produit.

Lorsqu'un tel passeport numérique existe et est utilisé par les propriétaires de l'objet en cas de revente, le NFT ne bénéficie pas qu'aux clients mais permet à la marque de :

- percevoir une commission sur la revente (lorsque celle-ci a lieu *on chain* et à condition que les consommateurs aient été prévenus lors de l'acquisition), chose qui lui est impossible en l'absence de NFT car les flux financiers réels sont en dehors de son champ de contrôle ;
- conserver un lien avec le nouveau propriétaire de l'objet. En effet, en cas de revente sur un marché secondaire dépourvu de NFT, la marque ne sait pas qui détient l'objet, une fois revendu, et ne peut joindre que le premier acquéreur. Avec le NFT, le nouveau propriétaire a accès aux services liés (canal *Discord* dédié, promotions conditionnées à la détention d'un NFT, *etc.*) et développe un lien avec la marque qu'il ne lui aurait pas été possible d'avoir sans NFT.

[27] Proposition de règlement du Parlement européen et du Conseil établissant un cadre pour la fixation d'exigences en matière d'écoconception applicables aux produits durables et abrogeant la directive 2009/125/CE, 30 mars 2022, n° COM/2022/142 final
(https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:52022PC0142, consulté le 15 mai 2023).

**Encadré 6 : Les NFT appliqués à la logistique**

L'utilité du recours aux NFT en matière de traçabilité peut également justifier leur une utilisation pour sécuriser les chaînes logistiques au sein des processus de production. Dans ce cas d'usage, les NFT ne sont ni vendus, ni proposés aux clients, mais servent, au sein d'une entreprise ou au sein d'un réseau réunissant une entreprise et ses fournisseurs, à établir la responsabilité des prestataires de livraison afin de limiter les pertes financières liées au mauvais suivi des livraisons.

Ainsi, la startup française Ownest propose une solution associant à tout objet en transit (palette, carton ou autre) un NFT. La chaîne logistique comprend un certain nombre de sites (usines, entrepôt, centre de tri, boutique, *etc.*), en vue des différentes étapes du processus productif. Le produit semi-fini est transféré d'un site à un autre par des prestataires. L'utilisation de la technologie *blockchain* permet d'associer à chaque acteur un portefeuille et d'inscrire sur la *blockchain* la bonne réception de l'objet en transférant le NFT d'un portefeuille à un autre. Chaque acteur est responsabilisé : il n'accepte le NFT que s'il correspond au bien livré. Tant qu'il ne l'a pas lui-même livré à un autre acteur, le détenteur du NFT est considéré comme responsable du bien. La solution d'Ownest permet ainsi de retracer la chaîne de responsables plutôt que de retracer la localisation des biens. Cette solution utilise la capacité d'horodatage de la *blockchain,* mais l'identification du détenteur du NFT suppose, elle, l'existence d'une base de données fiable regroupant tous les acteurs de la chaîne logistique et gérée par le client.

### 3.2.2. Les NFT constituent un nouvel outil de marketing, utile pour fédérer des communautés de clients

**Le NFT peut servir d'instrument de marketing pour développer un nouveau type de relation entre la marque et le client**. La détention d'un NFT permet en effet de fédérer des communautés fondées sur un sentiment d'appartenance et d'utiliser ces communautés comme levier de fidélisation à la marque ou de recrutement de nouveaux clients. L'outil Web 3.0 constitue, en lui-même, un atout marketing pour les marques qui souhaitent toucher des profils de consommateurs ciblés (jeunes, technophiles), que les méthodes de marketing traditionnelles ne parviennent pas à mobiliser. Au-delà de la communauté de « crypto-fans », les marques peuvent utiliser les NFT pour mobiliser des clients en leur proposant des services nouveaux (expériences dans un métavers, accès aux événements exclusifs, *etc.*). L'émission des NFT ne se faisant généralement pas à titre onéreux dans ces cas d'usage, le NFT devient un pur outil technologique et n'a pas besoin de revêtir les aspects ostentatoires ou artistiques des NFT représentant des biens de consommation virtuels.

Ainsi, Decathlon a développé un projet NFT liant un produit réel à un NFT gratuit qui permet au client de bénéficier d'une expérience client enrichie et dépassant la simple visite en magasin. Actuellement limité à deux produits (une paire de chaussures de sport et un maillot de VTT), ce projet permet au client de récupérer le NFT en scannant un QR code situé sur le produit et d'accéder grâce au NFT à un espace virtuel, à du contenu relatif au produit et à des loteries pour gagner des récompenses. Dans cette même logique marketing, Carrefour développe actuellement un projet de partenariat avec la plateforme d'échange Binance pour cibler des clients identifiés par Carrefour comme présentant un profil de joueur de jeux vidéo (supposés plus intéressés par les NFT que la moyenne) et leur proposer de lier leur carte de fidélité Carrefour à la *blockchain* de Binance, voire de réaliser des offres croisées. Dans ce cas, le recours aux NFT est mutuellement bénéfique : la publicité liée au projet concourt à la notoriété de chaque acteur au sein de la base de clientèle du partenaire.

La marque de cosmétiques Yves Saint Laurent Beauté, propriété du groupe L'Oréal, a lancé un projet de NFT gratuits, en juin 2022, donnant accès à une image en trois dimensions d'un bloc doré (qui ne correspond pas à un produit vendu par la marque). Ce NFT, à mi-chemin entre le NFT artistique et l'outil marketing, visait à mobiliser une communauté de « fans » de la marque, en leur donnant accès à des événements exclusifs. Les NFT sont bien utilisés, dans ce cas, comme un mode d'interaction avec les clients et non comme certificat d'un produit réel, lequel n'est d'ailleurs pas, en ce qui concerne des cosmétiques, revendable.

Les NFT utilisés comme signe d'appartenance à une communauté de clients ne sont pas toujours gratuits et sont parfois vendus par les marques. Ainsi, la marque Lacoste a bâti une expérience Web 3.0 appelée *Under water* en vendant 11 212 NFT à ses clients en juin 2022. Ces NFT donnent accès à un serveur *Discord*, lieu d'animation de la communauté. Ces NFT sont conçus pour être dynamiques, c'est-à-dire évolutifs, en fonction de l'implication du détenteur au sein de la communauté *Discord*. Plus que de percevoir de nouvelles recettes commerciales, le but du projet est donc d'accroître l'engagement des clients attachés à la marque, par exemple en leur donnant la possibilité de contribuer à la création de collections spéciales.

Le projet de Carrefour est à la croisée de l'utilisation des NFT comme outil de recrutement de clients et comme outil de fidélisation. **Les NFT sont parfois présentés comme le futur support des programmes de fidélité, à la suite, notamment, du lancement du programme de fidélité de Starbucks** (*cf.* encadré 7). Les NFT pourraient ainsi faire office de carte de fidélité numérique et remplacer les cartes physiques. Ils pourraient donner accès à des espaces réservés aux clients, voire différenciés selon le statut du client (argent, or, platine, *etc.*).

**Encadré 7 : Le programme Odyssée de Starbucks**

Annoncé en septembre 2022 et lancé en décembre 2022, le programme « Odyssée » de Starbucks est un nouveau format de communauté de clients, qui vient compléter le programme de fidélité classique (Starbucks Rewards) et qui interagit avec lui. Conçu pour offrir une expérience client fluide, permettant une diffusion au grand public et non seulement aux habitués du Web 3.0, le programme prévoit une identification *via* l'application Starbucks et les mêmes identifiants que le programme de fidélité, qui donnerait accès à un espace personnel où le client peut sélectionner des « voyages ». Ces quêtes, liées à l'histoire de l'entreprise et au monde du café, lui permettent de gagner des NFT édités sur le *layer 2 Polygon*, appelés « timbres ». Certaines de ces quêtes nécessitent de réaliser des achats en boutique, d'où le lien avec le programme de fidélité classique. D'autres NFT, rares, seront disponibles à l'achat et pourront être revendus entre clients. En collectionnant les NFT, les clients obtiennent des points, qui leur permettent ensuite d'avoir accès à des récompenses réservées aux clients Odyssée, au-delà des cafés gratuits déjà accessibles par le système de fidélité classique (voyages, visites d'exploitation, *etc.*).

**La valeur ajoutée du recours à la *blockchain* et aux NFT dans ce cas d'usage est néanmoins contestable**, dans la mesure où la décentralisation est illusoire puisque la confiance envers la marque reste nécessaire. L'avantage d'une *blockchain* par rapport à une base de données gérée par la marque, qui détient de toute façon un tel fichier clients, est peu clair. La numérisation d'une carte de fidélité, pour l'aspect purement pratique, peut passer par un code barre ou un QR code et ne requiert pas d'utiliser la *blockchain*. Par ailleurs, la cessibilité permise par le NFT semble inutile pour une carte de fidélité, dont le but est justement de récompenser la loyauté d'un client donné à une marque et non pas de pouvoir être cédée entre clients.

### 3.3. Dans une optique proche du mécénat, les entreprises peuvent recourir aux NFT pour financer des projets extra-financiers

**Le NFT peut être utilisé comme preuve de soutien à un projet philanthropique, mené ou financé par une marque, dans une logique proche de celle du mécénat prévalant dans le monde de l'art** (*cf.* 2.2.2). Le NFT est alors « vendu », bien qu'il ne représente aucun objet utilisable, et les recettes sont reversées au projet. Cette logique permet de créer une communauté autour du projet, qui peut par la suite être mobilisée par la marque dans un but davantage tourné vers la consommation.

Les maisons du groupe LVMH, peu engagées dans la vente de NFT comme objets de consommation, ont développé plusieurs initiatives suivant ce modèle. Ainsi, la maison Guerlain a émis en 2021 une collection de 1828 « *cryptobees* », des NFT représentant des abeilles sous un format artistique, au profit de la Vallée de la Millière, dans les Yvelines : ce projet, monté par Yann Arthus-Bertrand, vise à « réensauvager » un territoire de 28 hectares afin d'y accroître la biodiversité. La maison de cosmétiques Givenchy a également vendu, en juin 2022, une collection de NFT artistiques conçues par le collectif Rewind, représentant des portraits animés. Les recettes de cette vente organisée à l'occasion du « mois des fiertés », ont été reversées à l'association Le MAG Jeunes, association française de soutien aux jeunes LGBT. Cette action permet ainsi à la maison à la fois de s'initier au Web 3.0 tout en mettant en exergue des valeurs qu'elle associe à son image de marque[28].

Le soutien de projets dépasse les frontières du secteur du luxe, le groupe français de grande distribution Carrefour ayant aussi émis en 2022 deux collections de « NF Bees », des NFT représentant des abeilles, afin de reverser les recettes à un projet mené par la Fondation de France pour la protection des abeilles. D'une valeur comprise entre 15 et 750 €, proportionnelle à leur niveau de rareté et aux avantages associés (pot de miel reçu, « skin » pour son avatar sur The Sandbox, *etc.*), les NFT visaient à tester l'appétence de la clientèle de Carrefour pour cette technologie, y compris lorsqu'elle n'est pas associée aux produits de luxe.

* * *

Les cas d'usage des NFT recensés par la mission dans le domaine de la consommation sont divers. Les NFT peuvent à la fois constituer des biens de consommation virtuels, des certificats de propriété, des programmes de fidélité numériques ou des outils de marketing. En fonction du cas d'usage, la valeur ajoutée du recours à la *blockchain* et aux NFT est variable. **La promesse fondamentale des *blockchains* de créer de la confiance *ex nihilo* est infondée dans ces cas d'usage car ils reposent tous sur la confiance accordée à un tiers** (marque qui émet le certificat, métavers qui reconnaît le NFT, *etc*.). **En matière de biens de consommation, l'intérêt des NFT réside dans la cessibilité qu'ils octroient aux objets, mais est conditionné par l'interopérabilité des métavers**. En son absence, les métavers fonctionnent comme des jeux vidéo en vase clos, qui n'ont pas besoin de *blockchain* pour proposer des achats « *in game* ». **En matière de marketing, les entreprises rencontrées par la mission ont indiqué que le recours aux NFT était justifié par un souci de diversification de la clientèle et par un enjeu d'image (le Web 3.0 étant associé à la modernité, à la jeunesse, aux nouvelles technologies), mais pas par une nécessité technique**.

[28] Le site internet de Givenchy indique ainsi : « *Des photographies inédites, que le collectif a retravaillées numériquement aux couleurs du Rainbow Flag, exprimant ainsi l'engagement de Givenchy pour une beauté plus diverse, plus inclusive… En un mot, plus universelle.* »

## 4. Les jetons peuvent servir de solution technique aux services d'identité numérique

Les *blockchains* peuvent être utilisées pour faciliter l'échange de données sensibles, en particulier de données d'identité ou de données personnelles, tout en maîtrisant leur diffusion. Dans ce cas d'usage, c'est principalement la fonctionnalité de registre public interopérable qui est utilisé : la *blockchain* enregistre publiquement l'information selon laquelle une certaine personne possède une donnée qu'elle peut révéler *off chain* si la demande lui est faite. Le fait que les utilisateurs de la *blockchain* disposent préalablement d'un couple de clefs (publique et privée) permettant de les identifier et de chiffrer des informations facilite la mise en œuvre des échanges nécessaires à ce cas d'usage.

### 4.1. L'identité numérique consiste à numériser certaines données personnelles dans des buts de vérification et de maîtrise des données

Ainsi, un utilisateur peut avoir besoin de partager certaines données personnelles auprès d'organismes tiers (identité, âge, adresse, niveau de ressources, *etc.*) afin de valider une condition qui donne accès à un droit ou à une ressource (par exemple, attester d'un diplôme pour avoir accès à un emploi ou attester de sa majorité pour avoir accès à un contenu réservé aux majeurs). La vérification de ces données passe, en général, par des procédés peu sécurisés comme la transmission de fichiers numériques (attestations sous forme de fichiers PDF, scans de documents officiels, *etc.*) non signés ni certifiés. Le cas d'usage des *blockchains* et des jetons lié à l'identité numérique vise à renforcer la sécurité de ces procédés, tant du point de vue de la véracité des données transmises que du contrôle de leur confidentialité.

Les outils du Web 3.0 sont utilisés afin d'établir une identité numérique décentralisée. Trois modèles d'identité numérique sont possibles :

- l'identité numérique centralisée : dans ce cas, les données relatives à tous les utilisateurs sont détenues par un opérateur unique, qui gère une base de données centrale. Les « comptes utilisateurs », associés à un identifiant et un mot de passe utilisables uniquement pour l'accès à un espace donné, représentent des cas d'identité numérique centralisée. L'espace client numérique d'un client de banque est un exemple concret : il revient à chaque banque de sécuriser sa base de données afin d'éviter toute usurpation d'identité et toute manipulation frauduleuse des comptes en banque ;
- l'identité numérique fédérée : dans ce cas, les données relatives aux utilisateurs sont détenues par un opérateur donné (appelé « fournisseur d'identité » ou « *identity provider* »), mais servent à accéder à des services gérés par des opérateurs différents. Il en va ainsi par exemple de l'identifiant Gmail, qui peut permettre à un utilisateur Gmail de se connecter à d'autres sites internet requérant l'ouverture d'un compte (par reconnaissance du compte Gmail) ou, dans la sphère publique, de l'identifiant France Connect, qui permet, grâce à un seul identifiant, d'accéder à plusieurs services publics en ligne (impôts des particuliers, allocations familiales, immatriculation des véhicules, demandes de documents d'état civil, *etc.*) ;
- l'identité numérique décentralisée (en anglais, « *decentralised ID* ») : dans ce cas, chaque utilisateur détient ses données personnelles et accède directement aux différents services en transmettant les informations nécessaires au prestataire concerné. **Ce cas suppose que les prestataires reconnaissent les informations transmises par l'utilisateur comme vraies, d'où l'importance de mécanismes permettant d'assurer leur authenticité.**

Par opposition aux identités numériques centralisées et fédérées, qui supposent la détention des données personnelles par un tiers, l'identité décentralisée entend rendre l'utilisateur « maître de ses données » (une idée traduite par l'expression anglaise « *self sovereign identity* »). **Comme l'utilisateur n'est pas un organisme reconnu comme digne de confiance, la vérification de ses informations doit passer par un certificateur extérieur.** L'identité décentralisée constitue une réponse à l'enjeu de la maîtrise des données mais ne supprime pas la question de la confiance (contrairement à la philosophie ayant présidé à la conception de la *blockchain Bitcoin*) puisqu'elle suppose de faire confiance, si ce n'est à l'utilisateur, au moins à l'émetteur des données (*cf. infra*).

La mise en place de l'identité numérique décentralisée implique donc plusieurs acteurs :

- l'utilisateur, concerné par les données ;
- l'émetteur des données concernées, appelées « *verifiable credentials* » (VC), garant de leur véracité originelle. Les VC nécessitent souvent, en amont de leur émission, l'authentification de leur origine, qui peut prendre la forme d'un document physique (carte d'identité, titre de propriété, *etc.*). Les *credentials* physiques ont eux-mêmes été émis par un émetteur fondamental (l'État pour les informations d'état civil, une université pour un diplôme, un fournisseur d'énergie pour un justificatif de domicile, *etc.*) ;
- un vérificateur, qui fournit un service de vérification de l'authenticité de la donnée, pour donner accès à un service (dans les faits, l'utilisateur ne fait pas la différence entre le vérificateur et le service, qui sont intégrés).

Plusieurs choix techniques sont possibles pour la mise en œuvre d'une solution d'identité décentralisée. Une possibilité implique l'utilisation d'une *blockchain*. Avec cette solution, l'utilisateur peut utiliser un logiciel de « portefeuille » lui permettant de passer des ordres de transaction sur une *blockchain* donnée (un *wallet*, *cf.* section 2.1 de l'annexe I), qui stockera *off chain* (c'est-à-dire dans un emplacement autre que la *blockchain*), ses *verified credentials*. Il peut ensuite inscrire sur la *blockchain* l'information selon laquelle il détient la donnée personnelle, sans toutefois la révéler. Cette inscription peut, pour des raisons d'interopérabilité, prendre la forme d'un jeton ni fongible, ni cessible, appelé « *soulbound tokens* » (SBT)[29]. Ces jetons n'ont pas de valeur marchande et diffèrent donc des NFT utilisés dans les autres cas d'usage développés plus haut.

Lorsque l'utilisateur souhaite avoir accès à un service, il communique son identifiant, ce qui permet au vérificateur (en observant sur la *blockchain* les SBT détenus par l'utilisateur) de savoir qu'il détient une donnée lui permettant d'obtenir l'autorisation. Si cette vérification réussit, alors, le vérificateur donne à l'utilisateur le droit d'accéder au service. Le vérificateur peut ensuite conserver en mémoire l'information selon laquelle l'utilisateur a le droit d'accéder au service (indéfiniment ou pour une durée limitée, selon les situations) et lui donner à nouveau l'accès ultérieurement sur le fondement de son identifiant sans avoir à reprendre connaissance de ces données.

[29] Les *wallets* contenant les SBT sont appelés des « *souls* », « âmes » en français. Chaque utilisateur peut détenir plusieurs *souls*, s'il souhaite par exemple compartimenter ses données personnelles (professionnelles, médicales, familiales, *etc.*).

Ces procédures de vérification permettent de choisir quelles informations sont rendues visibles pour le vérificateur afin de ne pas divulguer plus d'informations que nécessaires. Par ailleurs, des techniques de « connaissance zéro » (« *zero knowledge proof* ») peuvent être utilisées pour vérifier le respect d'une condition sans divulguer l'information vérifiée. Par exemple, un utilisateur peut dans certaines situations prouver qu'il est majeur sans pour autant divulguer sa date de naissance ou qu'il dispose d'un niveau de revenu supérieur à un seuil donné sans pour autant révéler son salaire exact. À défaut de telles techniques, le vérificateur s'engage à ne pas conserver les données personnelles auxquelles il a accédé pour la vérification. En outre, le logiciel de portefeuille, qui comporte les fonctions cryptographiques permettant d'accéder à la *blockchain*, peut utiliser celles-ci pour sécuriser les transferts de données *off chain* nécessaires à la vérification.

## 4.2. Le développement de l'identité numérique décentralisée est porté par l'enjeu croissant de la numérisation de l'économie et de la maîtrise des données personnelles

Le déploiement de technologies d'identité numérique, qu'elles reposent sur des *blockchains* ou non, pourrait avoir plusieurs avantages pour les utilisateurs particuliers comme pour les services ayant recours à un vérificateur.

Pour les particuliers, l'identité décentralisée permet, outre le fait de limiter la diffusion des données personnelles à de trop nombreuses entités centralisées, de disposer d'un identifiant unique qui pourrait être utilisable pour avoir accès à de nombreux services et ainsi, éviter la création de multiples comptes clients et d'autant de mots de passe. La souveraineté de l'utilisateur sur ses données pourrait être étendue à leur éventuelle marchandisation : l'utilisateur pourrait décider de partager telles ou telles données contre rémunération des sites intéressés par leur exploitation.

Pour les prestataires de service, l'intégration des technologies d'identité décentralisée permet de limiter les cas de fraude en contrôlant le respect des conditions d'accès par des méthodes cryptographiques. La sécurisation de documents sensibles et néanmoins facilement contrefaits (ordonnances, diplômes, justificatif de domicile, *etc.*) peut constituer un enjeu majeur pour les prestataires, y compris dans la sphère publique (pour l'octroi d'une prestation sociale, par exemple).

Les avantages de ce cas d'usage ont incité les instances européennes à le favoriser *via* l'émergence de règles communautaires. La Commission européenne a publié le 9 mars 2021 une communication intitulée *Une boussole numérique pour 2030 : l'Europe balise la décennie numérique*, qui fixe l'objectif de mettre en place un cadre qui, d'ici à 2030, devrait avoir conduit au déploiement à grande échelle d'une identité de confiance contrôlée par l'utilisateur, permettant à chaque citoyen d'avoir la maîtrise de ses propres interactions et de sa présence en ligne.

Le 3 juin 2021, la Commission européenne a soumis une proposition de règlement[30] modifiant le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (ci-après le « règlement eIDAS »).

[30] Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, 3 juin 2021, n° COM/2021/281 final (https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=COM:2021:281:FIN, consulté le 15 mai 2023).

La Commission part du constat que « *le marché se caractérise par l'émergence d'un nouvel environnement dans lequel l'accent est mis non plus sur la fourniture et l'utilisation d'identités numériques monolithiques, mais sur la fourniture et l'utilisation d'attributs spécifiques en lien avec ces identités* », qu'il « *ressort de l'évaluation du règlement eIDAS que, dans sa version actuelle, cet instrument n'est pas en mesure de répondre à ces nouvelles demandes du marché* » et que « *les solutions d'identité qui ne relèvent pas du champ d'application du règlement eIDAS, telles que celles proposées par les fournisseurs de médias sociaux et les établissements financiers, suscitent des inquiétudes quant au respect de la vie privée et à la protection des données* », que « *le cadre eIDAS actuel n'englobe pas la fourniture d'attributs électroniques, tels que les certificats médicaux ou les qualifications professionnelles, ce qui rend difficile de garantir la reconnaissance juridique paneuropéenne de tels justificatifs sous forme électronique* » et que « *le règlement eIDAS ne permet pas aux utilisateurs de limiter le partage des données d'identité à ce qui est strictement nécessaire à la fourniture d'un service* ».

La proposition de la Commisison prévoit « *une architecture technique et un cadre de référence communs ainsi que des normes communes devant être élaborés en collaboration avec les États membres* ». Cette initiative est « neutre technologiquement ». Elle ne prescrit pas l'utilisation des technologies issues du Web 3.0 mais ses objectifs et les cas d'usages qu'elle vise à encourager sont compatibles avec l'utilisation des technologies *blockchain*.

## 4.3. Ce cas d'usage n'est pas central en matière d'économie des jetons

L'identité numérique constitue en tant que telle un enjeu important pour l'économie, du fait du rôle croissant des échanges numériques, mais les mécanismes liés à l'identité numérique n'impliquent pas nécessairement l'utilisation des *blockchains* et des jetons. Les capacités de vérification associées à l'identité numérique supposent la mise en œuvre de techniques cryptographiques, en particulier de signature électronique (*cf.* section 1.3 de l'annexe I), qui sont utilisées sur les *blockchains* mais qui peuvent tout à fait mises en œuvre indépendamment de celles-ci.

Ainsi, les principaux projets « Web 3.0 » relatifs à l'identité numérique dont la mission a eu connaissance utilisent les *blockchains* de façon incidente. La société française Archipels, qui développe un système de vérification de documents, se repose sur une *blockchain* permissionnée de consortium (*cf.* encadré 6 de l'annexe I), comme un moyen de distribuer entre quelques acteurs de confiance les données d'identité qui doivent être conservées et d'accroître la confiance des utilisateurs. La startup Synaps, qui propose un protocole d'identité décentralisée appelé Anima, s'appuie quant à elle sur des *wallets* connus (Metamask et Ledger) car les utilisateurs du secteur Web 3.0 les utilisent déjà et ont, de ce fait, un couple de clefs permettant de les identifier et de réaliser des opérations cryptographiques ; en revanche, les solutions qu'elle fournit ne supposent pas de réaliser des inscriptions sur une *blockchain*.

Ce cas d'usage est encore embryonnaire et le modèle économique n'est pas aisé à déterminer dans la mesure où le coût du service peut être supporté par l'utilisateur particulier ou par le prestataire du service à accès conditionné. L'interopérabilité des solutions constitue un enjeu crucial pour ce cas d'usage car la solution présente un intérêt d'autant plus important pour l'utilisateur qu'elle peut lui ouvrir l'accès à un nombre élevé de services sans avoir à créer de nouveaux comptes. Un puissant effet de réseau devrait donc être à l'œuvre dans ce secteur : la solution qui parviendra à s'imposer auprès de grands clients (banques, administrations, services en ligne grand public, *etc.*) risque d'imposer sa domination si une démarche de standardisation s'imposant à tous n'aboutit pas.

# ANNEXE IV

# Problématiques liées à la détermination des droits associés aux jetons

**Annexe IV**

# SYNTHÈSE

La présente annexe porte sur la compréhension de la nature juridique des jetons à vocation commerciale.

Les jetons à vocation commerciale, qui sont l'objet de la mission, ont pour spécificité d'avoir un sous-jacent : ils sont conçus pour conférer des « possibilités » (terme volontairement non juridique) à leur détenteur. Souvent, cette « possibilité » sous-jacente est un *droit* personnel : le détenteur peut exiger d'un tiers (généralement l'émetteur) qu'il exécute une obligation à son égard ; plus rarement, il peut se revendiquer propriétaire légitime d'un bien. **Le jeton et son sous-jacent, lorsqu'il existe, sont alors deux biens qui doivent être distingués.** Cependant, pour l'application de nombreuses branches du droit (fiscalité et consommation, par exemple), le premier ne sera que l'accessoire du second.

En revanche, **une difficulté substantielle réside souvent dans l'identification du sous-jacent et plus spécifiquement dans la connaissance par l'acheteur d'un jeton des droits exacts qu'il acquiert**. Le sous-jacent est parfois défini dans le code source d'un logiciel, parfois dans les conditions générales de vente de l'émetteur, il est souvent implicite et plus rarement défini dans un contrat joint au jeton. En outre, il est rare qu'un contrat prévoie explicitement que la vente du jeton équivaut à une cession de droits. Il suit, d'une part, une insécurité juridique générale dans les relations entre émetteurs et acheteurs de jetons et, d'autre part, une difficulté à respecter pleinement les obligations de transparence et loyauté lorsque la vente des jetons relève du droit de la consommation. **La mission formule ainsi une proposition principale pour améliorer la transparence, consistant à imposer que toute émission de jetons destinés à la consommation s'accompagne de conditions contractuelles écrites, annexées au jeton, qui exposeraient les droits associés au jeton.**

Une fois ces droits définis, ils doivent encore pouvoir être invoqués devant le juge civil en cas de contentieux. Or, une source d'interrogations réside dans la valeur probatoire des *blockchains* : les écritures d'un tel registre peuvent-elles constituer des preuves au sens du droit civil ? Selon la fédération française des professionnels de la *blockchain* (FFPB), cette possibilité ne serait pas assurée, d'où suivrait une insécurité juridique. La mission partage l'analyse selon laquelle les dispositions du Code civil relatives aux signatures électroniques ne reconnaissent pas pleinement la valeur de certaines inscriptions sur des *blockchains*, mais relève que cette situation est circonscrite et peut être résolue à droit constant par le recours à des prestataires de services de confiance. Surtout, **elle estime qu'une modification *ad hoc* du droit visant à reconnaître aux signatures utilisées sur les *blockchains* une présomption de fiabilité serait techniquement injustifiée et constituerait une incohérence majeure dans le droit.** Elle recommande plutôt aux pouvoirs publics, dans l'hypothèse où ceux-ci souhaiteraient sécuriser la valeur juridique des transactions inscrites sur une *blockchain* sans recourir à un tiers de confiance, d'engager des réflexions pour actualiser les dispositions du code civil relatives aux signatures électroniques, qui datent de plus de vingt ans et maintiennent une différence de traitement avec les signatures manuscrites.

La logique de transparence sur les droits associés aux jetons *via* l'annexion de conditions contractuelles est toutefois plus difficile à mettre en œuvre pour les NFT présentés comme des œuvres d'art. La mission rappelle, comme l'avait déjà démontré un rapport remis au conseil supérieur de la propriété littéraire et artistique (CSPLA) en juillet 2022, qu'**un NFT ne peut jamais constituer une œuvre d'art, un support d'œuvre, un « jumeau numérique d'œuvre », ni un certificat d'authenticité d'œuvre**. Les NFT « artistiques » sont en réalité le plus souvent « nus », sans droits associés, et n'ont qu'une valeur ostentatoire. Il importe donc que la communication des acteurs publics à ce sujet soit empreinte de transparence, de prudence et n'alimente pas de confusions auprès du grand public.

Les NFT ne sont pas des œuvres d'art et peuvent tout au plus constituer des titres de droits sur l'œuvre vers laquelle ils pointent, une partie des droits d'auteur (les droits patrimoniaux) étant cessibles en droit français. L'association entre des droits d'auteur et un NFT permettraient de rendre ces droits plus facilement échangeables. La cession de droits d'auteur est néanmoins strictement encadrée par le code de la propriété intellectuelle et nécessite l'accord de l'auteur, ce qui limite les possibilités de revente d'un NFT. **La mission étudie donc la façon dont des contrats de licence pourraient permettre au détenteur du NFT de disposer du droit, économiquement rival, d'exploiter l'œuvre**.

# SOMMAIRE

L'annexe II expose les principes techniques du fonctionnement des actifs numériques, en particulier les jetons échangeables et les NFT. Ainsi, **ce que l'on appelle *jeton* dans le contexte des actifs numériques est en réalité simplement l'inscription d'un solde dans le registre que constitue une *blockchain*** : soit par l'enregistrement des transferts successifs qui permet de calculer un solde, soit par l'écriture directement dans la mémoire d'un programme autonome sur *blockchain* du solde des porteurs, modifié à chaque transaction. Lorsque le jeton est non fongible, le solde est nécessairement zéro ou un : le programme enregistre donc uniquement un couple de données (identifiant du jeton, adresse du titulaire du jeton) et peut comporter quelques métadonnées associées au jeton.

**La finalité principale des jetons est de représenter des « droits », entendus dans un sens non juridique comme la *possibilité pour le porteur du jeton de faire ou d'obtenir quelque chose***.

Ces « droits » sont parfois conçus dans un sens purement technique : par exemple, la détention d'un bitcoin ne donne aucun autre « droit » que d'écrire sur la *blockchain* une transaction permettant de le transférer à quelqu'un d'autre ; les concepteurs de *Bitcoin* n'ont pas cherché à définir quels droits et obligations (au sens juridique) pouvaient conférer ces jetons à leur porteur. Certains jetons de protocole représentent des possibilités techniques vis-à-vis d'organisations dépourvues de la personnalité juridique : par exemple, dans le protocole de preuve d'enjeu d'*Ethereum*, la détention d'éthers confère le droit de participer à la validation des transactions, mais ce n'est un droit opposable à aucune personne physique ou morale identifiable.

Dans d'autres situations au contraire, il est clair que les jetons représentent une obligation de l'émetteur vis-à-vis du porteur : c'est par exemple le cas d'un NFT auquel est associé le droit, pour le porteur, de recevoir un disque vinyle. Certains NFT sont parfois même présentés comme un titre de droit sur une chose, par exemple la propriété d'une œuvre d'art — cette possibilité est discutée en section 3. Enfin, les jetons peuvent avoir un caractère mixte, conférant à la fois des droits juridiques (par exemple, une créance) et des possibilités techniques (par exemple, possibilité d'utiliser un objet dans un jeu vidéo).

Or, l'utilité économique conférée aux jetons et leur valeur dépendent en grande partie des droits et obligations qu'ils représentent — bien qu'une partie de leur désirabilité puisse parfois provenir des caractéristiques du jeton en lui-même plutôt que de son sous-jacent, par exemple son émetteur[1]. Leur traitement juridique et fiscal est susceptible de dépendre de ces droits. Ce faisant, **l'identification de la nature juridique des jetons et des droits associés constitue un préalable essentiel à toute étude.**

À cette fin :

- la section 1 a trait à la qualification juridique de ce qu'est un jeton et notamment à la distinction entre le jeton et son sous-jacent ;
- la section 2 porte sur les difficultés liées à l'identification des droits sous-jacents aux jetons ;
- la section 3 se concentre sur les difficultés probatoires et de validité qui pourraient survenir dans l'utilisation des *blockchains* comme supports d'actes juridiques ;
- la section 4 analyse la situation spécifique des NFT présentés par leurs promoteurs comme des « œuvres d'art », qui est la plus complexe compte tenu des règles d'ordre public du droit de la propriété intellectuelle.

[1] C'est le cas en particulier s'agissant de NFT « sur » des œuvres d'art, dont il est démontré en section 4 qu'ils ne représentent en général aucun droit, mais qui peuvent acquérir une valeur spéculative considérable.

Le fil directeur de l'analyse qui y est livrée est que **la sécurité juridique des utilisateurs de jetons n'est pas assurée lorsque les utilisateurs entendent utiliser des inscriptions sur une *blockchain* comme titres de droits, car les données inscrites sur cette dernière sont en règle générale insuffisantes**.

## 1. Les jetons ne doivent en principe pas être confondus avec leur sous-jacent, même s'ils peuvent être traités de façon transparente pour l'application de certaines règles de droit

Une première problématique consiste à déterminer ce qu'est la **nature juridique** du jeton en lui-même : s'agit-il d'une chose ? D'un titre de créance ? D'un titre de propriété ? D'un objet juridique nouveau et inclassable ? Le jeton peut-il, en fonction de son utilisation, être une œuvre d'art, un titre financier ou encore un contrat ? Ces interrogations ne sont pas uniquement des débats doctrinaux théoriques, puisque la qualification juridique des jetons est essentielle à la détermination des règles qui s'appliquent à eux.

Sur ce point, une analyse complète est présentée par la professeure Nathalie Martial-Braz dans une étude de droit des biens parue dans la *Revue de droit bancaire et financier* en juillet 2022[2]. La mission synthétise ci-après quelques enseignements de cette étude.

Ainsi que l'explique la professeure Nathalie Martial-Braz, les jetons, parce qu'ils ont une *valeur* et qu'ils sont *appropriables*, remplissent la définition d'un bien. **Les jetons à proprement parler doivent être distingués de leur éventuel sous-jacent, quelle qu'en soit la nature, celui-ci constituant un bien distinct.** Ainsi, si un jeton représente une place de concert, deux biens doivent être distingués : le jeton à proprement parler, qui est un bien meuble incorporel consistant en une écriture sur une *blockchain*, et le droit personnel sous-jacent, à savoir le droit opposable à l'organisateur d'accéder à la place de concert, qui est également un bien meuble incorporel. En revanche, si le jeton est « nu », c'est-à-dire sans droit associé, alors il existe un seul bien, constitué du jeton en lui-même. À noter toutefois que cette analyse est doctrinale : la mission n'a pas connaissance d'une décision de justice qui en apporterait confirmation.

Certes, la nature exacte du droit de propriété sur le jeton et l'idée d'appropriation d'un tel bien sont complexes à appréhender : le droit de propriété, tel qu'il a été conçu à la rédaction du Code civil en 1804, envisageait une propriété de bien corporels (d'où la *summa divisio* entre biens meubles et immeubles) et l'idée même de propriété d'un bien incorporel consistant en une inscription dans un registre numérique est difficile à concevoir. Néanmoins, le droit civil français permet en son principe d'accueillir la notion de propriété sur un tel bien : une décision du tribunal de commerce de Nanterre a par exemple reconnu aux bitcoins la qualité de biens meubles[3].

**Il existe donc bien, toujours selon cette étude, un authentique droit de propriété sur le NFT.** Ce droit doit ensuite s'articuler avec le bien sous-jacent.

Le plus souvent, cette articulation est une relation entre principal et accessoire : le jeton n'est qu'un accessoire des droits qu'il représente, lesquels droits ont vocation à y être incorporés. Cette situation est comparable à celle d'un véhicule cédé avec son certificat d'immatriculation : le certificat est un bien distinct du véhicule, qui permet de justifier sa propriété en cas de contestation, mais il n'en est que l'accessoire.

---

[2] Nathalie Martial-Braz, « Les NFT aux prises avec le droit des biens : essai d'une qualification – étude par Nathalie Martial-Braz », *Revue de droit bancaire et financier*, n° 4, juillet 2022, dossier 31.

[3] T. com. Nanterre, 6e chambre, 26 février 2020, n° 2018F00466, *SDE Bitspread Ltd c. SAS Paymium* (*Gazette du Palais*, 9 juin 2020, n° 379z0, p. 6).

Cependant, cette situation n'est pas systématique : si, par exemple, le NFT représente contractuellement un titre de propriété sur un bien corporel, alors le bien corporel et le titre de propriété pourraient être vendus indépendamment l'un de l'autre, rompant de fait la relation de principal à accessoire. Par exemple, si cette activité était possible, un certificat d'immatriculation ayant quelques propriétés remarquables (nom du titulaire, particularité du numéro d'immatriculation) pourrait devenir un objet de collection susceptible d'être dissocié du véhicule sur lequel il porte et d'être vendu seul après avoir été barré. Lorsque le NFT est « nu », il n'est plus l'accessoire d'aucun principal.

**Ce n'est que si la loi le prévoyait explicitement que le jeton pourrait devenir, en droit, indissociable de son sous-jacent.** Une telle situation est similaire à celle des titres financiers, même antérieurement à l'apparition des *blockchains* : la partie législative du code monétaire et financier rend le titre (document au porteur ou inscription dans un registre physique ou numérique) indissociable du droit personnel qu'il représente. Le propriétaire d'un titre obligataire n'est pas propriétaire *à la fois* du titre et de la créance qu'il représente, mais d'un bien unique.

L'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 a ouvert la possibilité d'utiliser une *blockchain* comme registre d'inscription de certains titres financiers : lorsque le titre est techniquement représenté par un jeton, alors le jeton est bien rendu, par la loi, indissociable du droit qu'il représente vis-à-vis de l'entité émettrice. Les décrets d'application prévoient que cette possibilité soit ouverte en particulier aux bons de caisse, qui sont qualifiés, lorsque le registre utilisé est une *blockchain*, de « minibons ». Néanmoins, à la connaissance de la mission, il n'existe pas d'autre cas de figure dans lequel le législateur a créé une assimilation entre un cryptoactif et son sous-jacent.

**Par ailleurs, sans que cela entre en contradiction avec l'analyse précédente, certaines branches du droit peuvent être amenées à traiter le NFT comme transparent vis-à-vis de son sous-jacent.** C'est par exemple le cas en matière fiscale, pour l'application du régime relatif à la taxe sur la valeur ajoutée (TVA) : « *la prestation constituée d'un seul service au plan économique ne doit pas être artificiellement décomposée pour ne pas altérer la fonctionnalité du système de la TVA*[4] », si bien qu'il appartient au juge du fond de déterminer dans quelle situation les opérations de vente d'un jeton et des droits sous-jacents doivent être décomposées ou assimilées et, dans le cas où elles sont assimilées, quel est l'objet principal : la vente du jeton ou celle de son sous-jacent (*cf.* annexe VI pour les enjeux fiscaux liés aux NFT). De même, pour l'application du droit de la consommation, l'accessoire suit le principal, si bien qu'une vente de jetons représentant le droit à une prestation de services sera régie par les règles applicables à la vente de cette prestation de services. Il appartient à la loi ou au règlement de prévoir explicitement les cas où le jeton doit être considéré comme l'accessoire d'un sous-jacent principal et les cas où ils doivent être assimilés.

[4] Cour de justice des communautés européennes, 25 février 1999, *Card Protection Plan Ltd (CPP)*, n° C-349/96, cons. 29.

# 2. Augmenter la sécurité juridique des situations nées de l'achat de jetons et accroître la protection des consommateurs suppose un effort de transparence contractuelle de la part des émetteurs de jetons

## 2.1. Dans la grande majorité des cas d'usage, les droits sous-jacents aux jetons sont mal définis, ce qui est source d'insécurité juridique pour les parties

### 2.1.1. Les droits associés au jeton peuvent être exécutés sur la *blockchain* qui les accueille ou en dehors de celle-ci

**Une distinction doit être réalisée entre les jetons conférant des droits *on chain* et ceux qui confèrent des droits *off chain*** (*cf.* section 1.3.2 de l'annexe II). Les droits et obligations que représente un jeton sont parfois exécutés, en tout ou partie, sur la *blockchain*, c'est-à-dire *on chain*, par la mise en œuvre d'un programme autonome qui constitue alors une modalité d'exécution du contrat. C'est le cas pour un jeton dont la détention représente des droits financiers : le programme peut réaliser un versement automatique aux porteurs et c'est alors le code du programme qui prévoit la façon dont les droits seront mis en œuvre. Néanmoins, le plus souvent, l'exécution des droits intervient *off chain* : soit dans le monde réel (par exemple, par expédition d'une marchandise, qui doit être réalisée par le débiteur de l'obligation), soit dans un système informatique distinct de la *blockchain* (par exemple, pour l'accès à un service numérique). Certains jetons peuvent par ailleurs avoir une nature mixte (droits *on chain* et *off chain* associés à un même jeton).

C'est lorsque le droit sous-jacent est inscrit *on chain*, c'est-à-dire lorsqu'il peut être mis en œuvre par l'exécution d'un programme autonome sur *blockchain*, qu'il est le plus simple à identifier. En effet, la lecture du code source du programme, lorsque celui-ci est disponible et n'a pas été rendu volontairement inintelligible, peut permettre d'identifier ces droits et obligations. Il existe un débat doctrinal quant au fait de savoir dans quelles conditions le code source du programme autonome peut alors constituer un instrument contractuel valable[5]. Néanmoins, dans une telle situation, le lien entre les jetons et le programme autonome mettant en œuvre les droits apparaît à la consultation de la *blockchain*, si bien que la nature exacte des droits et obligations *on chain* prévues par le « *smart contract* » peut être identifiée par toute personne capable de comprendre le code source.

**La situation est plus complexe lorsque le sous-jacent est *off chain*. En effet, dans cette situation, il importe en premier lieu d'identifier le siège des droits et obligations. Or, la mission a constaté que celui-ci était rarement clairement identifiable pour les jetons mis en vente.**

### 2.1.2. Plusieurs actes sont susceptibles de constituer le siège des droits associés au jeton à son émission

Il existe, en premier lieu, de nombreux jetons « nus » pour lesquels aucun droit ou obligation n'est sous-jacent ; dans ce cas, il n'y a pas de siège de droits et obligations à identifier. C'est le cas, en particulier, de la plupart des NFT « artistiques » échangés sur des plateformes spécialisées telles qu'*OpenSea* ou *Rarible* : pour ceux-ci, la promesse d'un « droit de propriété » sur l'œuvre d'art représentée est le plus souvent chimérique (*cf.* section 4).

---

[5] Ce débat rejoint en grande partie celui sur la valeur probatoire des *blockchains*, exposé en section 3 : il est en effet indispensable que l'obligation résidant dans le contrat soit valide et que son existence puisse être prouvée, ce qui suppose donc dans certains cas que le *smart contract* soit qualifié d'écrit.

En deuxième lieu, pour certains jetons, le siège des obligations peut être trouvé dans des instruments contractuels. Il peut en particulier figurer dans les conditions générales d'utilisation ou de vente du site de l'émetteur ou du vendeur. **Alternativement, les conditions peuvent parfois figurer dans un document « joint » au jeton** : par exemple, le code source du programme automatique de gestion du jeton peut comporter en mémoire un renvoi vers le document contractuel et éventuellement un *hash* (*cf.* section 1.2 de l'annexe I) assurant l'intégrité de ce document.

Enfin, en troisième et dernier lieu, des engagements contractuels peuvent exister sans pour autant avoir de siège sous la forme d'un document écrit ou numérique. En effet, selon le principe du consensualisme, la validité des contrats n'est *en principe* soumise à aucune condition de forme — de telles conditions existent néanmoins pour certains types de contrats, *cf.* section 3.

**Une situation particulièrement complexe est ainsi celle où les possibilités techniques offertes par la détention du jeton ne correspondent pas à des droits écrits au sens juridique.** Tel est le cas, par exemple, du jeu en ligne organisé par l'entreprise *Sorare* : la détention de cinq NFT permet techniquement de participer à certains tournois du jeu et ouvre la possibilité de gagner de nouveaux jetons, mais les conditions générales de vente du site ne formalisent pas un tel droit pour le détenteur du NFT, tandis que la possibilité de participation au jeu ou les modalités du jeu peuvent évoluer sur décision unilatérale de l'organisateur. Peut alors se poser la question de l'existence de droits vis-à-vis de l'entreprise *Sorare* (droit à participer au jeu et à gagner des récompenses en cas de victoire) pour le détenteur du NFT[6] dans la mesure où il n'existe pas de contrat écrit permettant de formaliser de droits. La loi et le règlement, en particulier le droit de la consommation, peuvent toutefois dans certains cas permettre de déduire des pratiques commerciales de l'émetteur l'existence de droits pour le consommateur.

### 2.1.3. La cession des droits sous-jacents lors de la cession du jeton est le plus souvent implicite

Les analyses précédentes portaient sur la détermination des droits associés à l'émission primaire de jetons. Une question similaire se pose lorsque le jeton est revendu sur le marché secondaire.

En principe, si le jeton représente un titre de droits, la revente du jeton représente une cession de créance détenue sur l'émetteur au sens de l'article 1321 du Code civil[7]. Or, un tel transfert de créance est le plus souvent implicite et déduit du transfert du jeton. Le fait qu'un acheteur sur le marché secondaire détienne des droits vis-à-vis de l'émetteur se déduit donc d'un ensemble de contrats : le contrat d'émission, dont l'identification est source des difficultés énoncées en 2.1.2, puis une succession de contrats de cession de créance associés à la vente du jeton dont certains sont parfois implicites.

En outre, en application de l'article 1324 du Code civil, la cession n'est en principe opposable à l'émetteur que si elle lui a été notifiée : un contrat pourrait prévoir que l'inscription dans la *blockchain* de la cession de jetons vaut notification, mais cette pratique ne peut être postulée sans contrat.

---

[6] Ce n'est cependant pas pour autant que le NFT devrait être regardé comme « nu ». En effet, il pourrait être associé à une concession de droits de marque, puisque les NFT sont associés à des images exploitant des marques déposées (image des footballeurs, noms de championnats, *etc.*).

[7] En principe, conformément à l'article 1323 du Code civil, la cession doit être, à peine de nullité, constatée par écrit. La possibilité que cette condition soit respectée lorsque la cession est réalisée *via* une *blockchain* est étudiée en section 3 *infra*.

**Ainsi, l'incorporation de la créance dans le jeton ne peut, en principe et dans le silence de la loi, être présumée, mais suppose une succession de déductions implicites. Il importe qu'une documentation contractuelle adéquate prévoie explicitement que les droits associés au jeton soient détenus par le porteur et opposables à l'émetteur, quelle qu'ait été la chaîne de cessions de droits.**

### 2.1.4. Cette situation est source d'insécurité juridique pour les parties

**La situation décrite constitue une source d'insécurité juridique.** La détermination des droits associés à un jeton en cas de contentieux peut être rendue complexe.

L'insécurité est maximale dans le cas où les droits associés au jeton reposent sur des engagements non écrits et devant être déduits de l'intention des parties. Cependant, même dans le cas où des écrits existent, l'association des droits au jeton est source de difficultés.

En effet, dans le cas où ce sont des conditions générales — c'est-à-dire un contrat unilatéral — qui définissent les droits associés au jeton, l'acheteur n'en a pas nécessairement connaissance :

- sur le marché primaire, lorsque l'achat est réalisé *via* une plateforme, les conditions générales de vente de l'émetteur peuvent figurer sur le site de ce dernier et non pas sur celui de la plateforme ;
- lorsque la revente du jeton a lieu sur le marché secondaire, l'acheteur n'interagit en principe pas avec l'émetteur et n'a donc pas connaissance des conditions générales.

Enfin, dans le cas où l'exécution du contrat est définie par le code source d'un programme autonome sur *blockchain*, même si le code est lié au jeton et reste identifiable, il n'est pas garanti que l'acheteur (primaire ou secondaire) soit en mesure de le comprendre et donc de consentir de façon libre et éclairée.

**Seul le cas où les droits et obligations ont leur siège dans un contrat écrit « joint » au jeton apporte un niveau de sécurité juridique élevé pour les parties (émetteur, acheteur primaire, éventuels acheteurs secondaires), car le contrat « suit » dans ce cas le jeton, quel que soit son détenteur.**

## 2.2. Le code de la consommation ne prévoit qu'une protection limitée des acheteurs de jetons

**Le droit de la consommation protège, dans certaines situations, le consommateur contre la situation d'insécurité juridique précédemment décrite.** Cependant, en l'état actuel du droit, la protection offerte aux consommateurs reste limitée.

**Le plus souvent, le jeton est l'accessoire de son sous-jacent, qui peut être la livraison d'un bien ou d'une prestation de services (*cf.* section 1), et relève expressément du code de la consommation**. Cette applicabilité du code rend en particulier obligatoire une présentation « *claire et compréhensible* » des contrats de vente (art. L. 211-1 du code de la consommation).

En principe, pour les contrats conclus par voie électronique, l'article L. 221-5 du code de la consommation prévoit que le professionnel a l'obligation de fournir au consommateur l'information des « *caractéristiques essentielles du bien, du service, du service numérique ou du contenu numérique* », ce « *de manière lisible et compréhensible* ». Or, lorsque le jeton est un titre de droit, la nature exacte de ces droits constitue une caractéristique essentielle du produit acheté. Lorsque les jetons sont associés à un sous-jacent dont ils sont dès lors l'accessoire, c'est la qualité de bien (ou de service) de ce sous-jacent qui emporte l'obligation de respecter le code de la consommation. L'information concernant les caractéristiques essentielles du bien et du jeton devraient donc être systématiquement fournie lors de la vente du jeton. La mission constate que cette obligation n'est, dans les faits, pas toujours respectée.

Lorsque les jetons sont dépourvus de sous-jacent (on parle de NFT « nus »), ils ne peuvent pas être considérés comme des biens accessoires et doivent obéir aux obligations relatives aux jetons. L'émission de jetons est assimilée à un service financier par les articles L. 111-3 et L. 222-1 du code de la consommation. Les services financiers sont exclus du périmètre d'application de l'article L. 221-5 par l'article L. 221-2. Néanmoins, l'article L. 222-5 dispose qu'« *en temps utile et avant qu'il ne soit lié par un contrat, le consommateur reçoit des informations dont la liste est fixée par décret en Conseil d'État et portant sur : […] 2° Les informations relatives aux produits, instruments et services financiers proposés* ». Ces informations sont précisées par l'article R. 222-1.

**Néanmoins, plusieurs limites réduisent la portée de la protection apportée par le code de la consommation.**

**En premier lieu, par principe, le code de la consommation ne couvre que les transactions entre un professionnel et un consommateur, que la vente soit primaire ou secondaire** (dans le cas d'un revendeur professionnel)[8]. Les ventes de particulier à particulier sur le marché secondaire ne sont donc pas couvertes : seules les règles générales du droit civil s'appliquent et celles-ci ne prévoient pas d'obligation d'information *a priori*. Ces ventes sont pourtant particulièrement sensibles du point de vue de la protection du consommateur, puisque l'acheteur sur le marché secondaire n'est pas nécessairement informé des conditions générales de vente définissant les droits liés au jeton. En outre, les droits associés aux jetons peuvent être altérés entre deux ventes du produit (par exemple, s'agissant de jetons utilitaires, par la consommation des droits liés aux jetons[9]).

**En second lieu, il n'existe pas, en règle générale, d'obligation de conservation du contrat sur un support durable**. Une telle obligation a en effet été supprimée dans le cas général pour les contrats de vente en ligne par la loi n° 2014-344 du 17 mars 2014 relative à la consommation. Si cette suppression s'explique en ce qu'elle était susceptible d'entraver le développement des échanges sur internet — le simple affichage à l'écran des conditions générales ne constituant pas une « conservation sur un support durable » —, elle conduit à une dégradation significative du niveau d'information des consommateurs s'agissant des jetons, qui sont des titres de droits transférables, puisque **rien n'oblige le revendeur à conserver puis transmettre avec le bien les conditions générales de vente de l'émetteur primaire lors des reventes sur le marché secondaire**. L'article L. 213-1, qui prévoit une obligation pour le professionnel de conserver durant dix ans le contrat lorsque la vente porte sur un montant supérieur à 120 €, ne permet pas de remédier à cette difficulté.

[8] Ce modèle économique est, début 2023, peu répandu : l'intermédiation des ventes est davantage le fait de plateformes opérant sur un marché biface. Toutefois, l'émergence de « brocanteurs NFT », achetant pour leur compte des objets jetons puis les revendant après en avoir été propriétaire, est envisageable.

[9] À l'exemple d'un jeton permettant à son détenteur de recevoir un bien une unique fois, cédé sur le marché secondaire après que le bien a été délivré par l'émetteur.

**En conséquence, il apparaît souhaitable de prévoir une modification du droit positif pour améliorer l'information des consommateurs lorsqu'ils réalisent un achat de jetons représentant des titres de droits transférables.**

## 2.3. Ces difficultés peuvent être résolues par une obligation de précision systématique des droits associés au jeton dans un document contractuel joint à celui-ci

**La rédaction d'un contrat prévoyant les droits que détient le détenteur du jeton à un instant donné sur l'émetteur constitue, compte tenu de ce qui précède, le moyen le plus adapté pour accroître la sécurité juridique de l'ensemble des parties. Il permet également de maximiser le niveau de protection des acquéreurs, que ce soit sur le marché primaire ou sur le marché secondaire.** Il garantit en effet que l'acheteur dispose, en toute situation, de la possibilité de prendre connaissance immédiatement des droits et obligations que l'émetteur du jeton y attache et permet d'apporter la preuve des obligations en cas de contentieux.

Certes, cette solution ne signifie pas la suppression de toute possibilité contentieuse quant aux droits et obligations liés au jeton. En effet, il ne saurait être exclu que les dispositions du contrat joint comportent des dispositions contraire à l'ordre public, qui seraient annulées en cas de contentieux[10]. L'insertion d'un tel écrit ne permet pas non plus de traiter complètement la situation dans laquelle l'émetteur n'inscrit, volontairement, pas l'ensemble des droits conférés par le jeton dans cet écrit et où en conséquence la personne prétendant détenir une obligation non écrite à l'égard de l'émetteur devra saisir le juge pour la faire reconnaître. Elle constitue cependant une façon d'améliorer la transparence de l'information et de prévenir le contentieux.

Dans le but de maximiser la sécurité juridique, les émetteurs peuvent par ailleurs gagner à faire figurer dans le contrat joint au jeton une mention de la législation applicable et du tribunal compétent pour le règlement des litiges. Il est en outre souhaitable qu'ils fassent figurer dans la *blockchain* un *hash* du document comportant les conditions contractuelles, ce qui permet de prouver son immuabilité — quitte à prévoir les conditions dans lesquelles les conditions contractuelles peuvent être mises à jour[11]. Par ailleurs, dans le cas où certains droits associés au jeton sont consomptibles (par exemple, le droit d'accéder à un spectacle), il est préférable que le niveau de consommation des droits figure explicitement sur la *blockchain*[12]. Enfin, quand bien même il pourrait être envisagé que le code source d'un programme autonome constitue un contrat valide et recevable comme preuve, les émetteurs pourraient toujours doubler le code source d'un écrit joint au jeton pour formaliser les droits et obligations *on chain* associés, afin là aussi de réduire le risque contentieux.

---

[10] *Cf.* par exemple la section 4 de la présente annexe, sur la difficulté de créer un tel contrat dans le cas où un NFT a vocation à représenter des droits sur une œuvre d'art.

[11] Une telle prévision peut par exemple prendre la forme suivante : insérer dans le contrat joint un article prévoyant les conditions de modification du contrat et introduire dans le code source du programme autonome sur *blockchain* gérant les jetons une fonction permettant de façon visible de remplacer le document contractuel par un nouveau document (soit sur décision unilatérale de l'émetteur, soit sur accord de l'émetteur et du porteur).

[12] Ainsi, si un jeton représente le droit de recevoir un bien une unique fois, il pourrait être inscrit dans la mémoire du programme autonome si le droit a été ou non consommé. Le contrat joint au jeton pourrait mentionner explicitement l'engagement pris par l'émetteur à inscrire dans la *blockchain* le fait que le droit a été consommé.

**En conséquence, la mission recommande aux pouvoirs publics de poursuivre une politique visant à ce que les jetons destinés à être vendus à des consommateurs incluent systématiquement un document contractuel en « pièce jointe ».** Une telle recommandation pourrait passer, cumulativement ou alternativement, par :

- une obligation pour les émetteurs de jetons destinés à être vendus à des consommateurs d'inclure un tel document contractuel en pièce-jointe ;
- une interdiction pour les plateformes d'échanges (incluant les plateformes de pair à pair, *cf.* section 2.2.2 de l'annexe V) d'admettre à la négociation des jetons qui ne comporteraient pas de tels documents contractuels en pièce-jointe. Une telle interdiction ne serait rendue applicable qu'aux jetons émis postérieurement à l'entrée en vigueur de la disposition.

Le document devrait enfin prévoir explicitement, lorsque des droits sont associés au jeton, que le transfert de celui-ci sur une *blockchain* vaut cession de créance et notification de l'émetteur.

Les jetons à vocation commerciale feraient donc l'objet de règles spécifiques, plus strictes et plus protectrices du consommateur que le droit commun, puisque la forme du document présentant les caractéristiques essentielles du bien et la façon dont il est présenté au consommateur seraient imposées. Cette proposition suppose, en droit interne, une modification du code de la consommation. Cependant, pour qu'elle puisse être pleinement effective et pour éviter qu'elle ne constitue une entrave à la circulation des jetons sur le marché unique, il serait préférable qu'elle soit établie au moins au niveau européen. Une telle disposition pourrait être introduite lors de la révision du règlement MiCA (*cf.* annexe V).

**<u>Proposition n° 1</u> : Rendre obligatoire l'association à tout jeton à vocation commerciale émis ou/et échangé dans l'Union européenne d'un document contractuel définissant les droits et obligations incorporés comme sous-jacent et détenus par tout porteur du jeton.**

Il est à noter, enfin, que cette proposition, bien que comportant des points communs avec la disposition du règlement MiCA relative aux livres blancs, en est distincte dans son esprit comme dans son champ d'application. Le règlement MiCA prévoit en effet que les émetteurs de certains cryptoactifs ont l'obligation de notifier un livre blanc (« *white paper* ») précisant en particulier les droits et obligations associés à la détention d'un jeton[13]. Néanmoins, ce livre blanc n'est pas le siège des droits et obligations. En outre, le formalisme du livre blanc s'inspire des obligations de prospectus applicables aux émissions de titres financiers, plutôt qu'aux principes de transparence et d'information qui fondent le droit de la consommation : il vise en particulier à informer l'investisseur sur les risques associés à l'acquisition des jetons. Enfin, le champ d'application de cette obligation ne couvre que les jetons fongibles et émis en grande série : l'intention des colégislateurs européens n'était pas, par cette obligation, de traiter les jetons destinés à la consommation, mais ceux destinés à être utilisés comme substituts à une monnaie ou comme support d'investissement (les jetons non fongibles étant exclus du champ d'application du règlement MiCA, *cf.* section 2 de l'annexe V).

Au contraire, la proposition de la mission devrait être rédigée de façon à cibler les jetons destinés à la consommation, ce qui inclut en particulier les jetons non fongibles ou émis en petite série ainsi que les jetons utilitaires.

[13] *Cf.* articles 4, 5 et 6 du titre II du règlement.

## 3. Les règles du droit civil relatives aux écrits électroniques pourraient constituer un obstacle à l'utilisation des *blockchains*, mais celui-ci peut être surmonté à droit constant

Une fois assurée l'existence d'une documentation contractuelle définissant sans ambiguïté les droits et obligations associés à un jeton, **il importe que les contrats respectent les conditions de forme exigées par le Code civil et que les droits puissent être établis devant le juge civil**.

Or, selon la Fédération française des professionnels de la *blockchain* (FFPB), des incertitudes en matière de droit de la preuve seraient source d'insécurité juridique et feraient obstacle à une large adoption des *blockchains*. En particulier, il existerait un risque que l'autorité judiciaire refuse de prendre en compte des inscriptions figurant dans le registre public qu'est la *blockchain* : écriture d'une transaction dans la monnaie de la chaîne, écriture de création d'un programme autonome sur *blockchain*, écriture d'exécution d'une fonction de ce programme, *etc.* (*cf.* encadré 1). La FFPB présente la preuve sur *blockchain* comme « *insusceptible de remplir aujourd'hui les exigences du droit français* ». Il suivrait « *un décalage entre la réalité technique et la reconnaissance juridique* »[14] lorsque la *blockchain* est utilisée à des fins d'horodatage d'informations.

Cette problématique a été abordée par un groupe de travail juridique de France Stratégie en 2018[15]. Elle a fait l'objet d'une réponse du secrétaire d'État chargé du numérique à une question écrite du député Daniel Fasquelle en 2019[16]. Elle est également traitée de façon approfondie, pour répondre à la question de la valeur juridique des « *smart contracts* », dans le manuscrit de thèse de doctorat de M^me^ Claire Leveneur intitulée *Les smart contracts : étude de droit des contrats à l'aune de la blockchain* (2022)[17].

**Encadré 1 : Différentes natures d'inscriptions sur des *blockchains***

Les inscriptions sur les *blockchains* peuvent représenter plusieurs types d'informations.

Il peut s'agir, en premier lieu, de données de transactions dans la cryptomonnaie de la chaîne. Une telle transaction est inscrite par une succession de données élémentaires : adresse de l'expéditeur, du destinataire, montant transféré, signature électronique de l'expéditeur autorisant la transaction.

En second lieu, les données peuvent représenter un programme autonome (*smart contract*, *cf.* annexe II). En général, les données inscrites sur la *blockchain* ne sont pas le code source du programme lui-même, mais une version dite *compilée* de celui-ci, directement interprétable par les ordinateurs mais inintelligible pour un humain.

En troisième lieu, des transactions peuvent donner l'ordre d'exécuter des fonctions des programmes autonomes. L'inscription correspondante inclut alors tous les paramètres passés à la fonction et le sens à donner à cette inscription dépend du contexte. Par exemple, une inscription peut correspondre à un ordre d'exécuter la fonction d'un *smart contract* ERC 721 (*cf.* annexe II) permettant le transfert d'un jeton. Il est nécessaire, pour donner du sens à cette inscription, de connaître les fonctionnalités du *smart contract* concerné et donc de disposer de son code source.

---

[14] FFPB, *Blockchain et preuve : pour une reconnaissance de la valeur probatoire de la blockchain en droit français*, mars 2023.

[15] France Stratégie, *Les enjeux des blockchains : rapport du groupe de travail présidé par Joëlle Toledano*, juin 2018, fiche « preuve et signature numérique », p. 99 à 109 (https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-rapport-blockchain-21-juin-2018.pdf, consulté le 4 mai 2023).

[16] Réponse du 10 décembre 2019 à la question n° 22103 de M. Daniel Fasquelle, député du Pas-de-Calais, au secrétaire d'État chargé du numérique (JOAN p. 10774, https://questions.assemblee-nationale.fr/q15/15-22103QE.htm, consulté le 6 avril 2023).

[17] Claire Leveneur, *les smart contracts : étude de droit des contrats à l'aune de la blockchain*, thèse de doctorat de droit soutenue le 2 décembre 2022 (https://www.theses.fr/2022ASSA0063, consulté le 6 avril 2023). Voir en particulier section « *la preuve du contrat informatisable* », n° 468 à 498.

Enfin, il est possible d'ajouter des inscriptions libres sur une *blockchain*, par exemple dans une case *ad hoc* de la mémoire d'un *smart contract*. De telles inscriptions peuvent alors être du texte clair (par exemple la phrase « *Le 4 mai 2023, je déclare renoncer à toute prétention dans le litige m'opposant à Untel* »), la représentation binaire d'un document quelconque (par exemple, d'un document PDF) ou encore le *hash* de ce document (*cf.* section 1.2 de l'annexe I). En règle générale, le coût financier de l'espace mémoire sur la *blockchain* conduit à éviter d'inscrire des documents trop lourds et à privilégier l'écriture d'un *hash*, qui prend une place réduite et suffit à démontrer l'existence du document concerné à une date donnée.

## 3.1. Plusieurs problématiques relatives à la reconnaissance juridique des écrits sur *blockchain* doivent être distinguées

En réalité, la question de la valeur juridique des inscriptions sur les *blockchains* se pose dans plusieurs situations qui doivent être distinguées :

- le cas où ces inscriptions seraient utilisées pour prouver des *faits juridiques*, par exemple le fait qu'une personne ait eu connaissance d'une information à une certaine date, qui pourrait être déduit du fait qu'elle a inscrit cette information sur une *blockchain* à cette date ;
- le cas où ces inscriptions seraient utilisées pour prouver l'existence d'actes juridiques, en particulier d'obligations (conditions dites *ad probationem*), par exemple l'existence d'un engagement de l'émetteur de jetons vis-à-vis de la personne qui les achète ;
- le fait de savoir si ces inscriptions respectent les conditions de formes requises pour la validité de certains *actes juridiques* (conditions dites *ad validitatem*), notamment pour les contrats qui pourraient être passés *via* une *blockchain*.

Ces difficultés sont traitées sous l'hypothèse qu'il existe effectivement un acte valide et bien identifié qui établisse les droits et obligations afférents à la détention des jetons (*cf.* section 2).

Or, les règles fixées par la loi, en particulier par le Code civil, diffèrent pour les trois situations.

**Tout d'abord, en ce qui concerne les faits juridiques, la preuve est libre hors des cas où la loi en dispose autrement** (art. 1358 du Code civil)**.**

**Ensuite, en ce qui concerne la preuve des obligations juridiques, l'écrit est en principe obligatoire, conformément à l'article 1359 du Code civil.** La preuve écrite s'entend comme la preuve par un écrit *parfait* et donc signé (*cf.* encadré 2). Par ailleurs l'article 1361 prévoit qu'il peut en principe être suppléé à l'écrit par un autre moyen de preuve parfaite (aveu judiciaire ou serment décisoire) ou bien par un commencement de preuve par écrit sous réserve qu'il soit corroboré par un autre moyen de preuve.

Deux catégories d'exception à ce principe doivent être citées :

- d'une part, la loi prévoit des situations dans lesquelles prévaut la liberté de preuve. Il s'agit notamment des cas dans lesquels l'obligation dont on cherche à prouver l'existence a une valeur inférieure à 1 500 € ou est celle d'un commerçant. Les preuves imparfaites peuvent alors suffire à prouver l'obligation ;

- d'autre part, dans certaines situations, l'écrit est obligatoire, sans que les autres moyens de preuve (en particulier le commencement de preuve par écrit) puissent y suppléer. Par exemple, l'article L. 131-2 du code de la propriété intellectuelle (CPI) requiert que les contrats prévoyant la cession de droits d'auteurs soient constatés par écrit. La jurisprudence de la Cour de cassation[18] interprète cette exigence de l'écrit comme une condition probatoire et non comme une condition de validité : ainsi, un contrat non écrit ne sera pas nul, mais la partie qui s'en prévaut ne sera pas en mesure d'en apporter la preuve devant le juge si la réalité du contrat est contestée (*cf. 4.2.1.2)*.

**Sur la validité des contrats, enfin, le principe est celui du consensualisme** (art. 1172 du Code civil) ; autrement dit, la validité des contrats n'est soumise à aucune condition de forme et le contrat peut être formé par oral (cas d'une vente à la criée) ou par une action mécanique (cas d'un distributeur automatique). Par exception, certains contrats, dits solennels, requièrent l'observation des formes déterminées par la loi à peine de nullité, sauf possible régularisation. L'utilisation de l'écrit fait généralement partie de ces conditions de forme. Par exemple, l'article 1322 du Code civil requiert que les cessions de créance soient constatées par écrit.

**Tableau 1 : Synthèse des régimes de preuve et de validité étudiés par la mission**

| Situation | | Régime de preuve |
|---|---|---|
| Prouver des faits juridiques | Cas général | Preuve libre |
| Prouver l'existence d'actes juridiques | Cas général | Preuve parfaite (écrit, aveu judiciaire, serment décisoire, copie fiable) ou, à défaut, commencement de preuve par écrit corroboré par un autre moyen de preuve |
| | *Cas particulier des obligations d'un montant de moins de 1 500 € ou d'un commerçant* | Preuve libre |
| | *Cession de droits de propriété intellectuelle* | Écrit parfait requis |
| Constituer des actes juridiques valides | Cas général | Consensualisme : pas de conditions de forme |
| | *Cas particulier des cessions de créances* | Écrit parfait requis |

*Source : Code civil (articles 1172, 1322, 1358 et 1359) et code de la propriété intellectuelle (article L. 131-2).*

**Encadré 2 : Principaux modes de preuve définis par le Code civil**

Le Code civil définit, en son article 1365, l'écrit comme « *une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quel que soit leur support* ». Sa perfection, c'est-à-dire son opposabilité au juge, suppose par ailleurs qu'il soit signé : la signature identifie l'auteur et manifeste son consentement aux obligations qui découlent de l'acte (art. 1367).

Outre l'écrit, la loi prévoit d'autres modes de preuve : certaines sont dites parfaites (aveu judiciaire, serment décisoire, copie fiable) et sont opposables au juge en toute situation ; les autres, dites imparfaites, peuvent être écartées par le juge. Le commencement de preuve par écrit est « *l'écrit qui, émanant de celui qui conteste un acte, rend vraisemblable ce qui est allégué* » (art. 1362). Un document non signé peut ainsi constituer un commencement de preuve par écrit s'il émane de la personne à laquelle l'acte est opposé. La mention d'un écrit sur un registre public vaut également commencement de preuve par écrit (art. 1362).

[18] Cour de cassation, première chambre civile, 12 avril 1976 (Bull. civ. I, n° 123). Voir en particulier *Code de la propriété intellectuelle*, éd. Dalloz, 2023, commentaires sous l'art. L. 131-2.

## 3.2. La valeur des inscriptions sur une *blockchain* n'est pas source de difficultés dans les cas où la loi n'exige pas de conditions de forme car les technologies utilisées sont éprouvées

Dans les situations où la preuve est libre et la passation des contrats dispensée de toute forme, la valeur juridique des inscriptions sur une *blockchain* n'est source d'aucune difficulté. C'est le cas par exemple :

- d'un contrat de vente pour un montant de moins de 1 500 €, qui peut, de façon licite, être formé par la réalisation d'une inscription sur une *blockchain* (consensualisme), laquelle peut être librement être produite devant le juge (liberté de la preuve) en cas de litige ;
- d'une inscription par laquelle une personne, à une date donnée, a fait figurer une déclaration écrite dans une *blockchain*, par exemple le *hash* d'un document qui preuve son existence.

La liberté de la preuve n'exclut cependant pas que celle-ci puisse être contestée, auquel cas il appartient au juge d'apprécier la force probante des inscriptions. À cette fin, il lui incombe en particulier d'apprécier le sens qu'il peut leur donner, de s'assurer qu'elles n'ont pas été falsifiées et de vérifier qui en est l'auteur. Ces contraintes sont étudiées dans les sections 3.2.1 à 3.2.3 *infra*.

Par ailleurs, sous ces mêmes réserves d'intégrité, d'intelligibilité et d'imputabilité, les inscriptions figurant sur une *blockchain* constituent au moins un commencement de preuve par écrit. Ainsi, même pour une obligation supérieure à 1 500 €, elles constituent une preuve recevable devant le juge et sont en principe suffisantes si elles sont corroborées par un autre élément.

**La situation des preuves par *blockchain*, lorsque la loi les rend admissibles, est comparable à celle de l'ensemble des documents électroniques.** En effet, la production devant le juge civil d'un courrier électronique, d'un document PDF ou d'une page web pose les mêmes enjeux d'intégrité, d'intelligibilité et d'intégrité que la production d'une inscription par *blockchain*. Or, la mission relève que le droit positif n'a pas fait obstacle au développement du commerce électronique ni à la résolution des litiges impliquant des échanges en ligne.

En conséquence, une fois déterminés le sens, l'auteur et l'intégrité des inscriptions, **ce n'est que lorsque la loi rend l'écrit obligatoire, que ce soit *ad probationem* ou *ad validitatem* que leur valeur juridique peut être source de difficultés**.

### 3.2.1. L'exigence d'intelligibilité des inscriptions ne parait pas constituer un obstacle au développement des cryptoactifs

**La première difficulté réside dans l'intelligibilité des écrits.** Les inscriptions figurant sur une *blockchain* sont en effet de simples suites de *bits* (*cf.* annexe I), qu'il est difficile d'interpréter.

M[me] Leveneur expose que « *l'intelligibilité doit être comprise comme la possibilité de retrouver une signification* »[19], ce qui n'exclut pas que l'écrit soit difficilement compréhensible.

La possibilité qu'une inscription soit reconnue comme intelligible dépendra donc du type d'inscription dont il est question (*cf.* encadré 1, p. 10). Dans deux cas, l'intelligibilité des inscriptions ne devrait jamais être source de difficultés :

- pour les inscriptions *en clair*. Ce cas de figure est en effet identique à celui de toute autre écriture ou de tout autre document électronique ;

[19] Leveneur, 2022, *op. cit.*, n° 474.

- pour les inscriptions représentant des transactions. En effet, les protocoles définissant les *blockchains* précisent explicitement quelle signification doit être donnée à la suite de *bits* qui les constituent. Il existe en conséquence divers outils permettant d'explorer et de visualiser sous une forme aisément compréhensible les opérations inscrites dans une *blockchain*. Cette situation n'est pas propre aux *blockchains* : l'interprétation de n'importe quelle donnée informatique, stockée sous forme binaire, suppose de connaître les spécifications permettant de les lire (*cf.* partie 1.1 de l'annexe I). Ce n'est qu'en cas de contestation du sens à donner aux inscriptions binaires qu'un recours à l'expertise pourrait être rendu nécessaire.

**Dans la situation où l'inscription consiste en la création, l'exécution ou la lecture de la mémoire d'un programme autonome sur *blockchain* (« *smart contract* »), l'intelligibilité dépendra de la disponibilité du code source.** En effet, la *blockchain* ne contient pas nécessairement le code source intelligible (écrit en code informatique par un programmeur) du programme pouvant être compris par un développeur spécialisé[20]. Même quand ce code source est divulgué, il peut l'être sous une forme qui le rend volontairement inintelligible.

Dans une telle situation, l'écriture sur la *blockchain* pourrait ne pas constituer, à elle seule, une écriture intelligible pouvant être présentée au juge. Cela dit, cette situation est souhaitable, puisqu'elle évite de fonder des faits et actes juridiques sur des données qui ne peuvent pas être comprises. Elle ne constitue en outre pas un obstacle au développement de la preuve sur *blockchain*, puisqu'il suffit aux personnes souhaitant l'utiliser de diffuser les codes sources intelligibles des programmes. Lorsque ce code source est divulgué, l'intelligibilité de l'écrit apparaît acquise.

**Un autre problème peut apparaître dans la situation où ne figure pas sur la *blockchain* un document, mais seulement le *hash* de ce document** (*cf.* partie 1.2 de l'annexe I). Dans une telle situation, il est peu vraisemblable que le *hash* soit qualifié d'écrit intelligible : il n'est pas possible de *retrouver une signification* au *hash*, mais seulement de constater qu'un document a un *hash* donné.

Cependant la présence du *hash* dans la *blockchain* prouve le fait juridique de l'existence des informations auxquelles il se rapporte, fait dont la preuve peut être apportée par tout moyen. Il peut par exemple être analysé comme un élément extrinsèque permettant de compléter un commencement de preuve par écrit.

Enfin, lorsque le *hash* vise à prouver l'existence d'un acte juridique, son inscription dans une *blockchain* pourrait être assimilée à une « *mention d'un écrit sous signature privée sur un registre public* », valant commencement de preuve par écrit selon l'article 1362 du Code civil.

**Compte tenu de ce qui précède, les exigences d'intelligibilité des inscriptions n'apparaissent pas constituer un obstacle à l'utilisation des *blockchains*.**

[20] Les programmes informatiques sont écrits dans un langage de programmation qui n'est pas le langage naturel (français ou anglais par exemple), mais qui comporte des règles syntaxiques rendant celui-ci intelligible par un programmeur. Cependant, la machine n'exécute pas directement ce code : il doit être transformé par un processus appelé la compilation en « langage machine », une suite d'instructions qui seront exécutées une par une. Dans la plupart des cas, il sera très difficile voire quasiment impossible, même pour un programmeur spécialisé, de comprendre le comportement du programme en se fondant uniquement sur le langage machine. Le code source du programme est en fait indispensable à la compréhension de son comportement.

### 3.2.2. Il n'apparaît pas opportun de modifier les règles de preuve pour présumer l'intégrité des données inscrites dans des *blockchains* publiques

**Apporter la preuve de l'intégrité des inscriptions figurant dans une *blockchain* pourrait constituer une seconde difficulté**. Autrement dit, il pourrait exister un risque que le juge refuse de reconnaître le caractère immuable et infalsifiable des données. **La FFPB propose en conséquence d'inscrire dans le code des postes et des communications électroniques une présomption d'intégrité des données inscrites dans un dispositif d'enregistrement électronique partagé** vérifiant des conditions fixées par décret en Conseil d'État. Le texte proposé par la FFPB présumerait également le bon ordre chronologique et le bon horodatage de ces données.

Néanmoins une telle modification de la loi n'apparaît ni utile, ni souhaitable.

En effet, **aucun élément porté à la connaissance de la mission ne tend à montrer que le juge refuserait de tirer les conséquences juridiques du fonctionnement technique des *blockchains***. L'introduction dans la loi d'une telle présomption reviendrait à postuler que l'autorité judiciaire ferait preuve d'un doute radical quant à la fiabilité des écritures électroniques figurant sur une *blockchain*.

En tout état de cause, si l'intégrité des inscriptions figurant sur une *blockchain* (ou plus exactement, sur une copie de cette *blockchain*) devait être contestée, les parties seraient en mesure de produire des éléments à l'appui de leurs présomptions et le juge pourrait recourir à l'expertise pour emporter sa conviction. Comme le rappelle la réponse du secrétaire d'État chargé du numérique de 2019, il est opportun que les parties disposent de cette possibilité de contestation : bien que les *blockchains* soient conçues de façon à être immuables, des failles restent envisageables, par exemple à la suite d'erreurs dans le code source des logiciels qui les manipulent, et des attaques ne sont pas exclues (attaque des 51 % en particulier, *cf.* section 2 de l'annexe I). Des évolutions technologiques pourraient en outre, à l'avenir, rendre faillibles des systèmes qui jusque-là étaient fiables. L'intégrité de la *blockchain* en elle-même n'impliquerait par ailleurs pas automatiquement que le fichier présenté au juge est lui-même intègre : encore faudrait-il prouver que ce fichier est bien une copie authentique de la chaîne, dans une version où elle fait consensus. Certes, la consécration d'une présomption n'interdirait pas à une partie de la renverser, néanmoins, un tel renversement serait probablement extrêmement difficile à réaliser.

La proposition de règlement modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement d'un cadre européen relatif à une identité numérique, émise par la Commission européenne le 3 juin 2021 (« proposition de règlement eIDAS 2 »), comporte des dispositions relatives à la présomption d'intégrité des données inscrites sur des registres électroniques. La section 11 de la proposition prévoyait initialement une définition harmonisée des services de registres électroniques, des services de registres électroniques *qualifiés* garantissant un niveau élevé de confiance, ainsi que des dispositions imposant aux États membres de :

- reconnaître une présomption d'intégrité aux données figurant sur un registre électronique, lorsque celui-ci a le statut de registre électronique *qualifié* ;
- ne pas refuser l'effet juridique ni la recevabilité des registres électroniques en justice au seul motif qu'ils ne sont pas des registres électroniques *qualifiés*.

Cependant, conformément à la philosophie générale du règlement, seuls les registres électroniques tenus par des prestataires de services de confiance *qualifiés* pourraient être eux-mêmes *qualifiés*. Pour les registres prenant la forme de *blockchain*, cela impliquerait en particulier qu'il s'agisse de *blockchains* privées (*cf.* encadré 6 de l'annexe I), écartant en particulier les *blockchains* grand public telles que *Bitcoin* ou *Ethereum* : ces dernières ne pourraient donc pas bénéficier de la présomption établie par le projet de règlement. La reconnaissance, en droit interne, d'une présomption d'intégrité pour des registres décentralisés trancherait donc avec l'économie générale du projet de règlement.

En tout état de cause, l'examen du texte par le Parlement européen en mars 2023 a conduit à la suppression de la section 11[21], et donc de toute référence aux registres électroniques, du texte qui est, à la date de ce rapport, en phase de trilogue.

### 3.2.3. Le fonctionnement technique des dispositifs de signature électronique peut le plus souvent assurer l'imputabilité des inscriptions

Les règles techniques de fonctionnement des *blockchains* prévoient que toute inscription qui y est réalisée est signée électroniquement[22] par son auteur.

La signature électronique repose sur des moyens de cryptographie asymétrique, présentés en section 1.3.2 de l'annexe I. Un utilisateur souhaitant émettre des signatures électroniques produit, par un procédé algorithmique, un couple indissociable constitué d'une clef publique et d'une clef privée. La clef publique constitue son identifiant (ou adresse, ou pseudonyme) rendu public et la clef privée est un moyen technique de prouver son identité, qui doit rester secret. À partir de n'importe quel document et de sa clef privée, il peut générer une signature électronique qui a deux propriétés :

- cette signature électronique ne peut être produite que par une personne qui avait en sa possession à la fois le document et la clef privée ;
- toute personne peut, si elle dispose du document, de la clef publique du signataire et de la signature, vérifier que les trois informations sont compatibles.

La signature des transactions intervenant sur les *blockchains* est fondée sur des algorithmes bien connus et documentés, appelés *RSA* et *ECDSA*. Ces sont ces algorithmes qui décrivent les transformations mathématiques successives à réaliser pour mettre en pratique les idées qui fondent la cryptographie asymétrique[23]. Plusieurs décennies de recul dans leur utilisation ont permis d'éprouver la robustesse des logiciels qui se fondent sur ces algorithmes.

La signature électronique permet donc de créer un lien techniquement fiable entre une paire de clefs et un document. Cependant, il reste encore à assurer le lien entre une personne et une paire de clefs (comment savoir que l'adresse X correspond bien à la personne Y ?). Cette question peut être comparée à un problème de même nature dans le monde réel : comment assurer qu'une signature corresponde bien à une personne physique donnée alors que son nom n'apparaît pas dans la signature ?

---

[21] Sous l'effet de l'amendement n° 39, adopté par la commission de l'industrie, de la recherche et de l'énergie (ITRE) lors de l'examen en commission le 9 mars 2023 et repris en séance plénière le 16 mars 2023.

[22] Par analogie avec les règles probatoires applicables aux écrits, le droit français distingue la signature électronique (lorsque l'auteur est une personne physique) du cachet électronique (lorsque l'auteur est une personne morale représentée par une personne physique). Il n'y a cependant, d'un point de vue technique, pas de différence entre les deux technologies.

[23] L'algorithme RSA, du nom de ses inventeurs Ronald Rivest, Adi Shamir et Leonard Adleman en 1977, repose sur l'asymétrie qui existe entre l'opération de multiplication de deux nombres premiers et l'opération de décomposition d'un nombre donné en facteurs premiers, inverses l'une de l'autre. L'algorithme ECDSA (*elliptic curve digital signature algorithm*), inventé en 1992, est quant à lui fondé sur l'asymétrie entre deux opérations réalisées sur des manipulations d'objets algébriques complexes appelés des courbes elliptiques.

Le seul moyen d'avoir la certitude absolue du lien entre la personne et sa signature écrite ou sa clef publique est d'observer la personne produire la signature en sa présence, après avoir contrôlé son identité[24]. Une telle procédure est cependant longue et peut être coûteuse : elle est donc, en pratique, rarement mise en œuvre. Néanmoins, **cette difficulté d'avoir une absolue certitude quant au lien entre une clef publique et une signature ne constitue pas un élément spécifique aux *blockchains* : les mêmes problématiques existent quant à l'imputabilité d'une signature à l'encre.**

Ainsi, dans le cas où la preuve est libre, un éventuel désaccord quant à l'auteur réel d'une inscription signée électroniquement peut techniquement être résolu par des méthodes analogues à celles qui ont cours pour les signatures à l'encre sur papier :

- dans le cas où une personne souhaite prouver qu'elle est l'autrice d'une inscription signée, c'est-à-dire établir qu'elle possède bien la clef utilisée pour la signature, elle peut, sous les yeux du juge, prouver ce fait en signant un document quelconque ;
- si au contraire, une personne nie être à l'origine d'une signature, son adversaire peut invoquer d'autres inscriptions signées avec la même clef pour convaincre le juge du fait qu'elle est l'autrice authentique ;
- les parties à un contrat peuvent s'échanger par avance les clefs publiques qu'elles entendent utiliser par la suite.

### 3.2.4. Le recours à une convention de preuve permet aux parties de s'accorder par avance sur l'admissibilité des inscriptions

Les articles 1356 et 1368 du Code civil autorisent la formation de contrats portant sur la preuve. Les parties à un contrat dont la bonne exécution dépend d'inscriptions sur la *blockchain* peuvent ainsi inclure, dans ce contrat, des stipulations portant sur la façon dont la preuve de ces inscriptions pourra être établie :

- en reconnaissant que les inscriptions figurant sur la *blockchain* sont présumés intègres ;
- en s'accordant sur le sens à donner à ces inscriptions ;
- en précisant les clefs publiques qui sont utilisées pour les signer et donc assurer leur imputabilité.

De même, les parties souhaitant passer par la suite des contrats *via* une inscription sur une *blockchain* peuvent prévoir une convention cadre précisant de quelle façon la *blockchain* peut être utilisée à cette fin.

La FFPB propose ainsi un modèle de convention de preuve, qui peut être adapté aux besoins et usages spécifiques de chaque contrat, ce que pourrait beaucoup plus difficilement faire une loi ou un règlement.

**Ainsi, dans les cas où la preuve et la forme des contrats sont libres, la valeur juridique des inscriptions sur les *blockchains* publiques n'est pas source de difficultés.**

[24] Sous réserve, cependant, que le document d'identité n'ait lui-même pas été falsifié, que la personne ne soit pas confondue avec un sosie, *etc.* En réalité, le problème du lien entre l'identité d'une personne et sa signature n'a pas de solution absolue et systématique. La notion même d'identité d'une personne reste difficile à définir précisément, aussi bien d'un point de vue technique que juridique, voire philosophique.

## 3.3. Des difficultés subsistent dans le cas où la loi exige un écrit en raison des dispositions applicables aux signatures électroniques, mais cette entrave est conforme à l'intention du législateur

### 3.3.1. Le recours à l'écrit est obligatoire pour certains actes juridiques correspondant à des cas d'usage courants des *blockchains*

Dans certaines situations, en revanche, la loi impose le recours à l'écrit, que ce soit *ad probationem* ou *ad validitatem* ; la finalité est le plus souvent de protéger l'une des parties en garantissant, par des conditions de forme, sa correcte information quant aux engagements qu'elle prend ou en réduisant le risque probatoire. **L'exigence est donc liée à la volonté du législateur de protéger un intérêt public.**

Les situations dans lesquelles la loi rend l'écrit obligatoire (actes relatifs à l'état des personnes, contrats de travail à temps partiel, sûretés, *etc.*) correspondent rarement à des cas d'usage des *blockchains*. **Une telle exigence s'impose néanmoins pour un cas d'usage essentiel : celui des cessions de créances et de droits de propriété intellectuelle intervenant en cas de vente de jeton**. Dans ces deux cas, la cession doit être constatée par écrit (art. 1322 du Code civil et L. 131-2 du code de la propriété intellectuelle).

En outre, la qualification, pour une inscription sur une *blockchain*, d'écrit plutôt que de commencement de preuve par écrit en ferait une preuve parfaite, qui s'imposerait au juge même sans élément probatoire complémentaire.

En conséquence, il est utile, pour le développement des *blockchains* à des fins commerciales, que les inscriptions qui y figurent puissent être considérées comme des écrits. Se pose donc la question de savoir dans quelle mesure des inscriptions électroniques telles que celles qui figurent sur une *blockchain* peuvent constituer des écrits au sens du Code civil, en dehors de dispositions créées *ad hoc* (*cf.* encadré 3).

**Encadré 3 : L'exception des minibons**

L'ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse a créé un régime spécifique aux minibons, c'est-à-dire aux bons de caisse émis sur internet. L'article L. 223-12 du code monétaire et financier (CMF), dans sa rédaction issue de cette ordonnance, autorisait l'inscription des bons de caisse dans une *blockchain*.

Dès lors que la vente de bons de caisse constitue une cession de créance, l'article 1322 du Code civil imposait en principe l'existence d'un écrit. Afin d'éviter tout risque contentieux quant à la qualification d'écrit pour les inscriptions passées sur une *blockchain* et correspondant à un transfert de propriété de bon de caisse, l'ordonnance a prévu à l'article L. 223-13 que l'inscription de la cession dans la *blockchain* « *tient lieu de contrat écrit pour l'application des articles 1321 et 1322 du code civil* ». En revanche, conformément à l'article L. 223-12 du CMF, les conditions dans lesquelles une *blockchain* peut être utilisée comme registre de propriété de minibons sont fixées par le pouvoir réglementaire.

L'ordonnance n° 2021-1735 du 22 décembre 2021 modernisant le cadre relatif au financement participatif a par la suite abrogé les articles L. 223-12 et L. 223-13 du CMF.

### 3.3.2. Le Code civil prévoit une définition de l'écrit qui exclut les inscriptions électroniques signées avec des clefs autocertifiées, comme c'est principalement le cas sur les *blockchains*

**À la suite de deux interventions du législateur en 2000 et 2004[25], le Code civil prévoit qu'une inscription intelligible sous forme électronique peut avoir la même valeur qu'un écrit : l'inscription est alors qualifiée d'*écrit électronique***. Conformément à l'article 1174, les conditions d'admissibilité de l'écrit électronique *ad probationem* et *ad validitatem* sont identiques.

Les conditions dans lesquelles l'écrit électronique a la même force probante que l'écrit parfait sur support papier sont définies aux articles 1366 et 1367 du Code civil :

- la personne dont il émane doit pouvoir être « *dûment identifiée* » ;
- il doit être « *établi et conservé dans des conditions de nature à en garantir l'intégrité* » ;
- il doit être signé électroniquement. La signature électronique « *consiste en l'usage d'un procédé fiable d'identification* » garantissant le lien entre son auteur et l'acte auquel elle s'attache. Cette fiabilité peut être présumée dans certains cas fixés par décret en Conseil d'État. Le décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique accorde cette présomption aux seuls processus de signature électronique dits « qualifiés », au sens où l'entend le règlement européen sur l'identification électronique (« eIDAS »)[26]. Cette classification de « qualifié » est réservée à des procédés mis en œuvre par des tiers de confiance certifiés par les pouvoirs publics et respectant un cahier des charges particulièrement exigeant.

L'établissement et la conservation des écritures dans des conditions de nature à en garantir l'intégrité ne sont pas sources de difficulté, pour les mêmes raisons qu'exposées en 3.2.2.

**Il en va différemment, en revanche, de l'identification de l'auteur et de l'admissibilité des signatures électroniques.**

#### *3.3.2.1. Le législateur a entendu exiger, pour les seules signatures électroniques, une certification du lien entre l'auteur et sa clef publique*

Les textes précédemment cités imposent, pour la reconnaissance de la valeur de l'écrit électronique, des conditions plus strictes qu'une simple imputabilité de l'acte. Il importe en effet que l'auteur soit *personnellement* identifié. Autrement dit, **il ne suffit pas que l'inscription ou le document comporte une empreinte électronique qui garantit son lien avec une clef publique, il faut par surcroît qu'il existe un certificat assurant que cette clef publique appartient à l'auteur, identifié nominativement**. Si le terme « *signature électronique* » désigne, dans le domaine des sciences informatiques, la seule *empreinte* obtenue à partir du document et de la clef privée, il correspond, dans le domaine juridique, à la réunion de cette empreinte avec le certificat, qualifié de *certificat de signature électronique*.

---

[25] La loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information a dans un premier temps permis l'utilisation d'inscriptions électroniques dans les cas où l'écrit est exigé *ad probationem* (art. 1316-1 et 1316-4 du Code civil, depuis renumérotés 1366 et 1367). L'article 25 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique a par la suite introduit un article 1108-1 (depuis renuméroté 1174) permettant l'utilisation de l'écrit électronique *ad validitatem* dans les mêmes conditions.

[26] Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (en anglais, *electronic identification and trust services* – eIDAS).

Cette exigence ne se déduit pas immédiatement de la lettre de la loi. L'interprétation est toutefois cohérente avec les débats parlementaires tenus lors de l'adoption de la loi du 13 mars 2000[27]. Surtout, elle se déduit du fait que, parallèlement à l'adoption de cette loi, les colégislateurs européens préparaient l'adoption d'une première directive sur la signature électronique[28] explicitant l'exigence d'un certificat pour qu'un procédé puisse être qualifié de « signature ». De façon cohérente, les décrets d'application successifs définissant les conditions dans lesquelles une signature électronique est présumée fiable[29] prévoient un cahier des charges portant d'une part sur de la production de l'empreinte de signature, d'autre part sur la fiabilité de l'émission du certificat de signature.

Le juge suit donc cette interprétation de la loi et vérifie bien, pour reconnaître à un écrit électronique la même force probante et la même validité qu'à un écrit papier, l'existence du certificat[30] ainsi que la fiabilité du processus de son émission.

**Les exigences pesant sur la signature électronique sont donc strictement plus lourdes que celles qui pèsent sur la signature manuscrite[31].** Pour les premières, il est indispensable que les données permettant de créer la signature (la clef publique) aient été préalablement reliées à la personne de l'auteur par un tiers certificateur, alors qu'une telle exigence n'existe pas pour les secondes : à titre d'exemple, un individu n'est pas obligé d'utiliser comme signature le même symbole que celui qui figure sur ses documents d'identité. Cette différence existe bien que l'article 1367 du Code civil donne à la signature manuscrite la même fonction d'identification de l'auteur qu'à la signature électronique.

Les articles 287 à 295 du code de procédure civile traitent ainsi de façon distincte les cas de contestation de l'auteur d'un document selon que ce dernier est papier ou électronique : pour une signature manuscrite, le juge peut procéder à une vérification d'écriture et retenir tous les documents utiles à cette fin ; pour une signature électronique, il est tenu de vérifier si les conditions de fiabilité des écrits définies aux articles 1366 et 1367 du Code civil sont satisfaites. Dans ce cadre, s'il constate que la signature électronique ne vérifie pas ces conditions, il ne peut régulariser le vice originel en recherchant lui-même l'auteur de l'acte. Autrement dit, le contentieux de la dénégation de signature, qui est un contentieux de la preuve pour les écrits physiques, est élevé au niveau de contentieux de la validité pour les écrits électroniques.

---

[27] Ainsi, lors de l'examen du texte en séance publique au Sénat le 8 février 2000, la garde des sceaux, ministre de la justice énonçait : « *Je précise, afin d'éviter toute équivoque sur le rôle de ces prestataires, que, dans l'optique de la directive, ceux-ci seront chargés de délivrer des certificats électroniques garantissant le lien entre l'identité d'une personne et un dispositif permettant de vérifier la signature électronique émise par cette personne. Leur rôle est donc d'« identifier » le signataire, mais en aucun cas de certifier le contenu des messages.* » (https://www.senat.fr/seances/s200002/s20000208/sc20000208025.html, consulté le 4 mai 2023).

[28] Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.

[29] Décret n°2001-272 du 30 mars 2001, puis décret n° 2017-1416 du 28 septembre 2017 renvoyant au règlement européen eIDAS.

[30] Voir par exemple : Cour de cassation, première chambre civile, 6 avril 2016, n° 15-10.732.

[31] Il ressort des travaux préparatoires à la loi du 13 mars 2000 que le législateur avait bien l'intention d'exiger un lien entre l'auteur et la signature plus solide pour les écrits électroniques que pour les écrits papiers. Ainsi, le rapport n° 203 du sénateur Charles Jolibois au nom de la commission des lois, déposé le 2 février 2000, cite les travaux d'un groupe d'experts présidé par le professeur Pierre Catala et proposant de « *reconnaître explicitement le statut des écrits électroniques comme mode de preuve, à condition que soit dûment identifiée la personne dont émane le document électronique* » (https://www.senat.fr/rap/l99-203/l99-2034.html#toc30, consulté le 4 mai 2023). Ce choix n'a pas été contesté lors des débats parlementaires.

**En cas de contestation, dans le cas où le certificat de signature reliant la clef publique à l'auteur n'existe pas ou n'a pas été émis de façon fiable, le document électronique perd sa qualité d'écrit et ne constitue plus en principe qu'un commencement de preuve par écrit.** Seules des circonstances particulières pourront permettre au juge de « sauver » la valeur de l'écrit électronique ou du contrat qu'il comporte lorsque l'écrit constitue une condition de validité[32].

#### *3.3.2.2. Les signatures électroniques autocertifiées ne sont pas regardées comme fiables au sens du Code civil et n'assurent donc pas la perfection de l'écrit*

Les signatures utilisées pour réaliser des inscriptions sur les *blockchains* publiques sont des signatures au sens cryptographique du terme, c'est-à-dire qu'elles consistent en une empreinte sans nécessairement de certificat. En l'absence de certificat, une inscription « signée » par une telle empreinte ne constitue pas un écrit fiable au sens des articles 1366 et 1367 du Code civil.

Les émetteurs de ces signatures électroniques ont par ailleurs la possibilité de générer eux-mêmes un certificat déclarant le lien entre leur clef publique et leur identité. De telles signatures sont dites *autogénérées* ou *autocertifiées*. Néanmoins, un tel procédé ne présente en lui-même aucune fiabilité et sera vraisemblablement rejeté en cas de contestation[33].

**Aussi est-il essentiel, en droit positif, pour que la validité de l'écrit électronique soit reconnue, que le certificat de signature électronique émane d'un tiers, qui lui-même le signe électroniquement.** Un tel certificat peut être émis dans des conditions sécurisées (vérification d'une pièce d'identité du futur utilisateur en sa présence) qui en font un certificat *qualifié* de signature électronique, permettant à la signature électronique ensuite utilisée d'être elle-même *qualifiée* au sens du règlement eIDAS et de bénéficier d'une présomption de fiabilité. De telles vérifications sont toutefois particulièrement lourdes et difficiles à mettre en œuvre.

À défaut, il est possible d'utiliser des certificats dits « éphémères » ou « à la volée », liés à une clef utilisée pour signer un unique document. De tels certificats sont générés par certains prestataires de services de signatures en ligne, après une vérification de l'identité de l'auteur, par exemple par l'envoi d'un SMS. Un tel procédé ne bénéficie manifestement pas d'une présomption de fiabilité, mais peut être admis par le juge[34], selon la robustesse du dossier de preuve produit pour attester de la fiabilité du procédé.

**Cette exigence de recours à un tiers est cohérente avec la philosophie générale du droit des services de confiance dans l'Union européenne.** Ainsi, en particulier, la construction du règlement eIDAS repose sur le recours à des prestataires de services de confiance accrédités par des autorités publiques. L'utilisation purement décentralisée des *blockchains* va à l'encontre de cette conception.

### 3.3.3. Il n'est pas opportun de créer une modification *ad hoc* du droit de la preuve pour les inscriptions figurant sur une *blockchain*

**Il suit de ce qui précède que les inscriptions sur une *blockchain* peuvent, à droit constant, constituer des écrits parfaits**, sous réserve que la signature électronique utilisée soit associée à l'auteur par un certificat électronique émis par un tiers.

---

[32] Ainsi, l'inscription reste qualifiée d'écrit tant que la fiabilité du procédé de signature n'est pas contestée (Cour de cassation, première chambre civile, 11 juillet 2018, n° 17-10.458) ou que l'identité de l'auteur n'est pas débattue (Cour de cassation, chambre sociale, 14 décembre 2022, n° 21-19.841). Un état de la jurisprudence est présenté par Thibault Douville, « Désordre dans le contentieux de la signature électronique », *Recueil Dalloz*, 2022, p. 121.

[33] Thibault Douville, « Désordre dans le contentieux de la signature électronique », 2022, *op. cit.*

[34] Voir en particulier : Cour d'appel de Nancy, deuxième chambre civile, 14 février 2013, RG n° 12/01383.

Certes, cette exigence constitue une lourdeur et provoque une perte de fluidité par rapport à des inscriptions directes sur les *blockchains* signées par des clefs non certifiées. Cependant, **un grand nombre d'usages des *blockchains* supposent déjà pour les utilisateurs de recourir à des tiers**, en particulier des prestataires de services sur cryptoactifs (CASP, *cf.* annexe V). Ces tiers pourraient naturellement opérer le service de confiance consistant en l'émission et la conservation du certificat de signature électronique, en particulier lorsqu'ils ont l'obligation de vérifier l'identité de leurs clients.

Au-delà de cette possibilité, plusieurs adaptations du droit peuvent être envisagées.

L'ordonnance du 28 avril 2016 relative aux bons de caisse (*cf.* encadré 3, p. 18) prévoyait ainsi que l'ensemble des inscriptions sur des *blockchains* portant transfert de propriété d'un minibon tenaient lieu de contrat écrit. Les propositions de la FFPB visent quant à elles à présumer l'intégrité des *blockchains* et la fiabilité des signatures utilisées sur celles-ci, ce qui revient donc à présumer que les conditions de qualification d'un écrit sont remplies.

**La mission relève toutefois qu'une telle modification *ad hoc* créerait une sérieuse incohérence dans le droit.** En effet, les conditions dans lesquelles un écrit est signé, le niveau de sécurité technique de la signature et la capacité à identifier son auteur sont indépendants du fait que l'écrit soit finalement inscrit sur une *blockchain*. Il est possible de produire des écrits signés à l'aide de clefs non certifiées ou autocertifiées y compris sans *blockchain* et, au contraire, d'inscrire dans une *blockchain* des écrits signés à l'aide de clefs certifiées par un tiers de confiance. L'inscription sur une *blockchain* n'apporte techniquement aucune garantie quant à la fiabilité de la signature et, surtout, quant à la fiabilité du lien entre la clef et l'auteur.

Si les pouvoirs publics souhaitaient favoriser la reconnaissance juridique des écrits électroniques réalisés sans passer par un tiers de confiance, qu'ils soient inscrits sur une *blockchain* ou sur un autre type de support, il serait préférable à cette fin de modifier le régime des écrits électroniques. Une telle évolution pourrait en particulier passer par un assouplissement de l'obligation de certification par un tiers du lien entre la clef de signature et l'auteur de l'acte et par un alignement des régimes applicables aux signatures manuscrites et électroniques. De tels travaux devraient être pilotés par le ministère de la justice, plus précisément par la direction des affaires civiles et du sceau, en partenariat éventuel avec l'institut des études et de la recherche sur le droit et la justice, lequel avait déjà conduit les travaux de recherche conduisant à la loi du 13 mars 2000. Une telle évolution du droit des signatures électroniques dépasse néanmoins le cadre du présent rapport.

## 4. Les NFT « artistiques » ne peuvent pas représenter des droits de propriété sur des œuvres d'art, mais les auteurs d'œuvres d'art peuvent leur associer une concession de droits d'exploitation

Un cas d'usage majeur des JVC dans le secteur de l'art consiste en la **création de NFT liés à des œuvres d'art, chaque œuvre étant associée à un nombre limité de NFT pointant vers elle** (*cf.* section 2 de l'annexe III).

Pour mémoire, un NFT correspond à l'enregistrement sur une *blockchain* d'un ensemble de données associées à l'adresse (numéro de portefeuille) d'une personne présentée comme le « propriétaire » du jeton. Dans les cas d'usage artistiques, les données du NFT permettent d'identifier un fichier numérique correspondant à une œuvre d'art : une image (format JPEG ou PNG par exemple), un fichier audio ou encore une vidéo.

Dans l'immense majorité des cas, le NFT contient en réalité un lien (URI, *cf.* encadré 6 de l'annexe II) indiquant à quelle adresse le fichier et ses métadonnées peuvent être téléchargés publiquement sur internet. Comme pour tout fichier numérique, il est aisé pour toute personne de réaliser une copie conforme et indiscernable de l'original.

## Annexe IV

L'objectif de la présente section est d'identifier les droits que pourrait conférer à une personne la détention d'un NFT artistique, c'est-à-dire pointant vers un fichier numérique incluant une œuvre d'art. La qualification des jetons artistiques est en effet sujette à des difficultés particulières au regard du droit français de la propriété intellectuelle (*cf.* encadré 4).

**Encadré 4 : Principes fondamentaux du droit d'auteur**

En droit français, l'auteur d'une œuvre de l'esprit jouit sur celle-ci, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous, qualifié de droit d'auteur. Ce droit existe que l'œuvre soit attachée à un support matériel (tableau, sculpture, photographie analogique matérialisée par son négatif) ou non (musique, photographie numérique). Lorsque l'œuvre est liée à son support matériel, le droit d'auteur est distinct de la propriété corporelle du support ; cette dernière respecte les règles de droit commun posées par le Code civil.

Le droit d'auteur comporte deux composantes. La première est constituée des droits moraux de l'auteur qui sont personnels, incessibles, inaliénables et éternels : l'auteur a droit au respect de son œuvre et de son nom et jouit d'un certain nombre de privilèges quant à l'œuvre, par exemple l'exclusivité du choix de la divulguer au public. La seconde réside dans ses droits patrimoniaux : l'auteur jouit d'un monopole sur l'exploitation de l'œuvre et dispose d'un droit de suite lorsque le support de l'œuvre, le cas échéant, est vendu. Le monopole d'exploitation recouvre tant la reproduction de l'œuvre que sa représentation, quelles qu'en soient les formes. Les droits patrimoniaux ont une durée limitée et expirent en principe 70 ans après le décès de l'auteur ; à l'extinction de ce droit, l'œuvre entre dans le domaine public[35]. Les droits de l'auteur sont exercés par ses ayants-droits après son décès.

Contrairement aux droits moraux, les droits patrimoniaux peuvent faire l'objet d'une cession, toujours partielle et limitée dans le temps : l'auteur peut ainsi passer un contrat exclusif d'édition contre rémunération (par exemple, pour l'impression et la diffusion d'un livre) ou donner son accord pour une représentation de l'œuvre selon des modalités qu'il établit (par exemple, autoriser la mise en ligne d'une photographie sur un site internet). La loi ne prévoit pas de distinction, parmi les contrats d'exploitation des œuvres, entre les simples concessions pour l'« utilisation » d'une œuvre et les situations dans lesquelles l'auteur se dépossède d'une partie de son monopole d'exploitation : l'ensemble de ces contrats relèvent d'une même catégorie des cessions de droits. Pour chaque contrat, le périmètre exact des droits cédés relève de la liberté contractuelle.

La loi prévoit des exceptions, de portées limitées et toujours interprétées de façon restrictive, au monopole de l'auteur sur l'exploitation de l'œuvre. En particulier, la copie et la représentation d'une œuvre à des fins strictement privées et non commerciales sont possibles dans certaines situations. En revanche, en principe, toute représentation publique, même non directement lucrative, suppose la cession préalable d'un droit : un particulier ne peut, par exemple, diffuser une photographie dont il ne détient pas les droits sur internet, y compris sur un réseau social.

Le code de la propriété intellectuelle établit, par de nombreuses dispositions d'ordre public, un niveau élevé de protection de l'auteur vis-à-vis de ses cocontractants. La cession est en effet limitée dans son objet, réalisée *intuitu personæ* et soumise à un important formalisme. Elle doit obligatoirement prévoir une rétribution de l'artiste lorsque l'exploitation des droits donne lieu à des recettes. L'artiste, quant à lui, conserve au titre de ses droits moraux des privilèges exorbitants vis-à-vis de son cocontractant, notamment un droit de résiliation du contrat moyennant indemnisation (dit droit de repentir).

*Source : Livre I^er du code de la propriété intellectuelle.*

[35] Cette notion de domaine public en droit de la propriété intellectuelle est distincte du domaine public en droit de la propriété des personnes publiques.

## 4.1. L'utilisation des NFT est portée par une promesse de maîtrise des droits des artistes et de création d'authenticité sur des œuvres numériques, qui seraient sinon aisément copiables

### 4.1.1. Les « œuvres d'art sous la forme de NFT » sont présentées par leurs promoteurs comme un nouveau type de support artistique

**De nombreux promoteurs des NFT dans le domaine artistique présentent le jeton comme étant indissociable de l'œuvre.** Cette vision les conduit par exemple à parler d'« art NFT » ou d'« œuvre d'art sous forme de NFT » ainsi qu'à désigner comme « NFT de tableau » le tout indissociable que constitueraient, selon eux, l'œuvre et le jeton pointant vers celle-ci (*cf.* encadré 5).

Autrement dit, selon cette vision, qui est la plus optimiste quant aux « NFT artistiques », l'écriture dans la *blockchain* du nom du détenteur du jeton serait équivalente à la propriété de l'œuvre d'art vers laquelle pointe le jeton. Par ailleurs, bien que le fichier numérique correspondant à l'œuvre (image JPEG par exemple) soit copiable à l'infini, la seule copie « authentique » serait celle que détient, à un moment donné, le titulaire du jeton. Les copies détenues par les autres personnes ne seraient que des copies « pirates », dépourvues de toute valeur, comme peut l'être par exemple un fichier numérique reproduisant un tableau célèbre ou un tirage illicite d'une photographie. Pour cette raison, le NFT est parfois présenté comme un « certificat d'authenticité » d'une œuvre au format numérique.

Au sein de cette tendance, **une première vision consiste à assimiler le NFT à l'œuvre**. Le titulaire du NFT posséderait donc une propriété, entendue comme le droit de jouir et de disposer de l'œuvre de la façon la plus absolue ; la cession du NFT emporterait donc cession de l'œuvre. Dans une vision maximaliste, elle emporterait même cession de l'ensemble des droits associés à l'œuvre, y compris celui de l'exploiter commercialement. Cette vision maximaliste a notamment été portée par le projet *Bored Apes Yacht Club Collection* de l'entreprise *Yuga Labs*, une série d'images représentant des singes dont chacune est associée à un NFT : un contrat de licence conforme au droit de l'État américain du Delaware garantit au titulaire de chaque jeton des droits très étendus sur l'œuvre d'art associée.

**Une seconde vision, portée par la majorité des acteurs rencontrés par la mission défendant l'« art NFT », voit plus modestement dans le NFT un « support immatériel », pour l'art « natif », ou un « double numérique » pour les œuvres « tokénisées ».** Le titulaire du NFT disposerait également, selon cette vision, d'un droit de propriété sur l'œuvre, mais une dissociation devrait être réalisée entre :

- d'une part, l'œuvre de l'esprit (c'est-à-dire le fichier sous-jacent, le plus souvent, une image), à laquelle sont associés des droits de propriété intellectuelle ;
- d'autre part, le « support immatériel », c'est-à-dire le NFT, qui serait assimilable à un bien meuble incorporel.

Cette distinction est directement inspirée de celle qui est prévue en droit français, pour les œuvres corporelles, entre la propriété du bien meuble constituant son support matériel et la propriété intellectuelle incorporelle sur l'œuvre (art. L. 111-3 du code de la propriété intellectuelle – CPI). Le titulaire d'une « œuvre d'art graphique sous forme de NFT » jouirait ainsi, vis-à-vis de l'œuvre, de droits comparables à ceux du propriétaire d'un tableau ou d'une sculpture. La situation dans laquelle plusieurs NFT pointent vers la même œuvre serait quant à elle assimilable à celle d'une photographie ayant fait l'objet de plusieurs tirages : chaque tirage correspond à la même œuvre de l'esprit mais constitue un support différent, ayant son propre propriétaire.

**Les défenseurs de l'« art NFT » voient dans ce modèle une occasion de mieux protéger les droits des auteurs contre les copies piratées de leurs œuvres**, puisqu'à tout moment, un seul propriétaire « authentique » disposerait du droit de jouir d'un exemplaire de l'œuvre sur laquelle porte le NFT. L'auteur, en choisissant le nombre de NFT qu'il édite sur son œuvre, fixerait ainsi le nombre de copies licites qu'il accepte de voir circuler.

**Encadré 5 : Exemples d'écrits assimilant un NFT à une œuvre d'art, à son support ou à un certificat d'authenticité**

La vision d'un NFT comme indissociable de l'œuvre d'art sur laquelle il porte est répandue dans le débat public, y compris dans la communication d'entités publiques.

Ainsi, un article[36] publié sur le site du centre national d'art et de culture Georges-Pompidou, à l'occasion de sa première acquisition de NFT en février 2023 indique en chapeau : « *le Centre Pompidou est la toute première institution dédiée à l'art moderne et contemporain à faire l'acquisition d'un* ***ensemble d'œuvres*** *traitant des relations entre blockchain et création artistique,* ***parmi lesquelles*** *ses premiers NFT* » (nous soulignons). Au début de l'article, on peut lire : « *le Musée national d'art moderne vient de faire entrer en collection ses premiers NFT* » ou encore « *qu'est-ce qu'un NFT ? Certificat d'authenticité garanti par le système de la blockchain ou « chaîne de blocs » (une technologie de stockage de l'information en réseau assimilable à un registre partagé, décentralisé et crypté), le NFT est par définition unique* ».

La lettre de mission du président du conseil supérieur de la propriété littéraire et artistique à M. Jean Martin, avocat à la Cour, sur les jetons non-fongibles, datée du 2 novembre 2021, affirme quant à elle : « *le musée russe de l'Ermitage propose sous forme de NFT la* Madone Litta *de Léonard de Vinci*, les Lilas *de Vincent Van Gogh, ou encore le* Coin de jardin Montgeron *de Claude Monnet* » puis : « *le NFT est un fichier de données non fongible situé sur une chaîne de blocks («* blockchain *») et destiné à garantir l'authenticité d'une œuvre originale ou de sa reproduction, voire à constituer l'œuvre originale elle-même* ».

### 4.1.2. En l'état actuel du droit, un NFT ne saurait être assimilé à une œuvre d'art ni à son support, comme l'a démontré le rapport remis au conseil supérieur de la propriété littéraire et artistique (CSPLA) en juillet 2021

Dans un rapport remis en juillet 2021 au conseil supérieur de la propriété littéraire et artistique (CSPLA)[37], M. Jean Martin, avocat à la Cour, et Mme Pauline Hot, auditrice au Conseil d'État, établissent que les deux visions précédemment présentées ne sont pas compatibles avec le droit positif.

La reconnaissance d'une œuvre de l'esprit, au sens du code de la propriété intellectuelle (CPI), suppose que soient remplies des conditions d'originalité (expression de la personnalité de l'auteur ou démarche intellectuelle de sa part) et de mise en forme (l'œuvre doit rencontrer une concrétisation et non pas se limiter à une simple idée). Or, le NFT ne constitue que la réunion, dans la mémoire d'un programme autonome sur *blockchain*, de trois éléments :

- l'identifiant d'un détenteur ;
- un lien vers l'emplacement du fichier numérique constituant l'œuvre ;
- d'éventuelles métadonnées.

[36] Séverine Pierron, *Collection : le centre Pompidou passe à l'heure NFT*, 10 février 2023, sur le site du centre national Georges-Pompidou (https://www.centrepompidou.fr/fr/magazine/article/le-centre-pompidou-passe-a-lheure-nft, consulté le 17 mars 2023).

[37] Jean Martin et Pauline Hot, *Rapport de la mission sur les jetons non fongibles : sécuriser le cadre juridique pour libérer les usages*, rapport présenté à la séance plénière du conseil supérieur de la propriété littéraire et artistique du 12 juillet 2022. Voir en particulier p. 18 à 25.

Le programme en question n'est le plus souvent pas original au sens du CPI. L'édition du NFT suppose seulement l'exécution d'une fonction de création qui consiste en un processus automatisé et ne laisse pas de place à la personnalité de l'auteur.

**Le NFT ne saurait donc être assimilé à l'œuvre d'art en elle-même.** Le « jeton » doit être distingué de l'œuvre, représentée sous la forme d'un fichier numérique et existant indépendamment du NFT.

**De la même façon, le NFT ne peut en principe pas être regardé comme le support d'une œuvre.** Le support d'une œuvre de l'esprit, lorsqu'il existe, s'entend par référence à l'article L. 111-3 du CPI, lequel dispose que « *la propriété incorporelle définie par l'article L. 111-1 est indépendante de la propriété de l'objet matériel* ». Le support constitue ainsi un bien matériel soumis aux règles de propriété du Code civil et dissocié de l'œuvre de l'esprit incorporelle soumis aux règles de la propriété intellectuelle. Ce support peut en particulier être transféré (par cession ou vente) et avoir une certaine valeur, en ce qu'il permet la matérialisation de l'œuvre.

Toutefois, dans le cas d'un NFT, le support n'est pas le jeton en lui-même, qui n'a pas de substance. En particulier, le jeton ne « contient » pas de représentation de l'œuvre : celle-ci est en fait codée sous un format numérique binaire conformément à un standard technique partagé (par exemple JPEG pour le codage d'une photographie ou MP3 pour le codage d'un fichier musical) et la suite de données binaires qui en résulte est stockée sur divers supports physiques : disques durs, DVD, cartes mémoires, lecteurs de stockage, le plus souvent en plusieurs exemplaires. Chacun de ces exemplaires constitue donc un support matériel de l'œuvre, mais le NFT n'est qu'un outil technique « pointant » vers l'un de ces supports.

L'identification du NFT à un « support immatériel de l'œuvre », conférant à son détenteur les mêmes droits qu'au propriétaire du support matériel d'une œuvre d'art, apparaît donc infondée en droit positif.

**Enfin, le NFT ne saurait être regardé comme un certificat d'authenticité ou d'unicité de l'œuvre sur laquelle il porte.** En effet, aucun élément n'assure, en cas d'émission d'un NFT « sur » une œuvre d'art, cette authenticité ni cette unicité. Toute personne peut en effet produire un NFT pointant vers une œuvre dont elle n'est pas l'autrice ou émettre plusieurs NFT « sur » une même œuvre. Deux NFT distincts peuvent pointer vers des adresses internet différentes, mais correspondant à des fichiers identiques, voire à des fichiers distincts mais correspondant à des œuvres identiques[38]. En tout état de cause, lorsque l'œuvre n'existe que sous format numérique, la notion d'unicité est délicate à apprécier. Enfin, dans certains cas, la détention du NFT ne prémunit en rien contre une modification du fichier hébergé à l'adresse internet indiquée (*cf.* encadré 9 de l'annexe II).

En réalité, la présentation d'un NFT comme « certificat d'authenticité et d'unicité » témoigne, elle aussi, d'une confusion entre l'œuvre en elle-même et le jeton qui pointe vers celle-ci. Il est vrai que le NFT est identifiable, unique et infalsifiable et que les données enregistrées sur la *blockchain* permettent à tout moment d'identifier son titulaire légitime, nécessairement unique. En revanche, le lien entre le NFT et l'œuvre ne fait l'objet de quasiment aucune garantie.

Dans certaines situations, la nature technique du lien entre le NFT et l'œuvre peut différer de ce qui est présenté ci-dessus : l'œuvre peut, par exemple, être entièrement reproduite dans la mémoire du NFT (à la place d'un simple lien) ou bien être générée à partir des fonctions du programme (*cf.* encadré 6). Cependant, dans tous les cas, il subsiste une distinction entre l'œuvre en elle-même et l'écriture dans la *blockchain* du NFT, c'est-à-dire de l'association d'un « propriétaire » à certaines données.

[38] Il est en effet possible de représenter numériquement de plusieurs façons différentes une même image, une même musique ou une même vidéo, par des choix de format ou d'encodage ou encore par l'ajout de données ignorées lors de la lecture du fichier.

**Aussi, la présentation des NFT comme étant des œuvres d'art, des supports d'œuvres d'art, des « jumeaux numériques d'œuvres d'art » ou encore des certificats d'authenticité est trompeuse et devrait être évitée.**

**Encadré 6 : Situations dans lesquelles la relation entre le NFT et l'œuvre d'art ne se limite pas à la présence d'un lien internet**

Dans certaines situations, la relation entre le NFT et l'œuvre d'art est plus forte que la simple existence, dans la mémoire du programme NFT, d'un lien internet permettant de télécharger le fichier numérique constituant l'œuvre d'art, sans que le raisonnement qui précède s'en trouve affecté.

Une première situation est celle dans laquelle le fichier numérique est « encapsulé » dans le NFT. Plus précisément, dans ce cas, la mémoire du *smart contract* contient, plutôt qu'un lien vers une représentation numérique de l'œuvre, une case mémoire comprenant ladite représentation. Le NFT reste cependant distinct de l'œuvre de l'esprit ; simplement, la mémoire du *smart contract* (dupliquée entre tous les nœuds de la *blockchain*) en devient un support physique supplémentaire. Le lien entre le NFT et l'œuvre est alors garanti (il n'est plus possible de modifier l'œuvre sur laquelle porte le NFT), mais pas l'authenticité ni l'unicité de NFT portant sur cette œuvre.

Il en va de même dans le cas où la mémoire du programme ne comporte pas la représentation numérique de l'œuvre, mais seulement une empreinte identifiant celle-ci (un *hash*, *cf.* section 1.2 de l'annexe I).

Une situation plus complexe est celle dans laquelle l'œuvre de l'esprit réside dans le code source du *smart contract* : par exemple, lorsque ce *smart contract* comporte des fonctions permettant de générer des images ou des sons selon un processus créatif. Néanmoins, même dans ce cas, devrait être distingués d'une part l'œuvre de l'esprit (prenant la forme du code source du *smart contract*) et d'autre part le NFT (écriture dans la mémoire du contrat de l'adresse publique du « détenteur »).

Enfin, peut être envisagé le cas où l'émission du jeton en elle-même constitue une performance artistique ou en est une composante, par exemple parce que l'émission d'un NFT sur un type d'œuvre constitue en elle-même une démarche originale. Ces situations appellent une étude au cas par cas ; cependant, quoi qu'il en soit, l'œuvre ne réside pas dans le jeton en lui-même, mais dans la démarche conceptuelle de son émission.

## 4.2. Sous réserve que des conditions contractuelles le prévoient explicitement, le NFT pourrait constituer un titre de droit d'exploitation d'une œuvre, distinct d'un droit de propriété

Comme le propose la mission en section 2 de la présente annexe, des conditions contractuelles pourraient être associées à un NFT artistique dans le but de donner au détenteur des droits effectifs sur l'œuvre. Il est donc nécessaire d'identifier la nature des droits que pourraient conférer ledit contrat et les conditions dans lesquelles ces droits pourraient être effectifs.

### 4.2.1. Un NFT ne peut pas représenter un titre de propriété sur une œuvre numérique incorporelle

Une première hypothèse, proche de la vision des promoteurs des NFT artistiques, pourrait consister à voir dans le NFT un titre de propriété sur le bien meuble incorporel que constitue l'œuvre d'art numérique.

Cependant, dans le cas des biens immatériels, la notion de propriété suppose l'intervention de la loi pour leur conférer la qualité de biens exclusifs (au sens économique du terme) et ainsi, définir les droits, garantis par la puissance publique, des propriétaires. La seule notion de propriété pertinente sur une œuvre d'art numérique réside donc dans la création, par une fiction législative, de droits exclusifs sur l'œuvre (notamment sur sa copie et sa reproduction). Ces droits exclusifs constituent précisément le droit d'auteur (*cf.* encadré 4, p. 23).

Autrement dit, **il n'y a pas lieu, s'agissant d'une œuvre incorporelle, de concevoir une notion de propriété sur l'œuvre distincte de la propriété intellectuelle**. La distinction prévue par l'article L. 111-3 du CPI entre la propriété intellectuelle sur une œuvre et la propriété de son support corporel ne peut pas être répliquée pour des œuvres numériques.

Puisque le seul droit envisageable sur une œuvre incorporelle est la propriété intellectuelle, il pourrait être envisagé que l'auteur incorpore ses droits de propriété intellectuelle dans le NFT et qu'à tout instant le détenteur du NFT détienne ces droits de propriété intellectuelle. Le droit d'auteur sur l'œuvre serait donc une sorte de bien incorporel changeant de propriétaire.

Or, les droits moraux de l'auteur sont incessibles (art. L. 121-1 du CPI). La seule notion de propriété cessible sur une œuvre pouvant être envisagée en droit français est donc la cession des droits d'exploitation sur l'œuvre : droit de représentation et droit de reproduction. Cette cession ne peut elle-même qu'être partielle : elle est subordonnée à la condition « *que le domaine d'exploitation des droits cédés soit délimité quant à son étendue et à sa destination, quant au lieu et quant à la durée* » (art. L. 131-3 du CPI). Enfin, le code de la propriété intellectuelle restreint le champ des droits concédés, par exemple en imposant en principe une rémunération de l'auteur à proportion des recettes perçues en cas d'exploitation commerciale de son œuvre (art. L. 131-4 du CPI) ou en permettant la résiliation unilatérale de la transmission des droits dans certaines situations (art. L. 131-5-2).

Si le détenteur d'un NFT devait être regardé comme propriétaire d'une fraction des droits sur l'œuvre, cette propriété serait nécessairement très dégradée par rapport à l'idée civiliste de propriété sur une chose comme droit d'en « *jouir de la façon la plus absolue pourvu qu'on n'en fasse pas un usage prohibé par les lois ou par les règlements* » (art. 544 du Code civil)**.**

**Ces analyses plaident donc pour éviter que les NFT liés à des œuvres d'art numériques ne soient présentés, dans la communication publique, comme des titres de propriété sur ces œuvres.**

### 4.2.2. Une vision plus pertinente consisterait à lier le NFT à un contrat d'adhésion portant cession de droits de l'auteur dont le bénéfice serait réservé à une personne détenant le NFT, mais cette solution présente une fragilité

**Sur le fondement des dispositions précitées du code de la propriété intellectuelle, l'auteur d'une œuvre de l'esprit peut, par contrat, céder à un tiers une partie des droits d'exploitation de l'œuvre**. Ces derniers sont susceptibles d'être revendus en application de l'article 1598 du Code civil[39].

Ainsi, conformément à la logique proposée par la mission en section 2, les clauses d'un contrat attaché au NFT pourraient prévoir que l'auteur concède un ensemble de droits d'exploitation (par exemple, le droit de copier et de représenter l'œuvre publiquement sur les réseaux sociaux ou dans un métavers) au détenteur d'un NFT. Le propriétaire du NFT ne serait pas présenté comme propriétaire de l'œuvre, mais comme concessionnaire de droits d'exploitation sur celle-ci.

Une première expérimentation de tels contrats de licence pour confier des droits au détenteur d'un NFT est par exemple proposée par l'entreprise française Exposure Arts, opérant sous la marque *Rhapsody Curated*, pour accompagner les NFT qu'elle commercialise (*cf.* encadré 7).

[39] « *Tout ce qui est dans le commerce peut être vendu lorsque des lois particulières n'en ont pas prohibé l'aliénation.* »

**Encadré 7 : Exemple de contrat de licence permettant d'associer des droits à la détention d'un NFT (contrats *Extended* et *Extended Limited* de Rhapsody curated)**

L'entreprise française *Exposure Arts* propose, sous la marque *Rhapsody Curated*, l'émission de NFT associés à des photographies numériques. L'entreprise acquiert tout d'abord auprès de l'auteur de la photographie le droit d'exploiter l'œuvre sous l'une des licences *Extended* ou *Extended Limited*. Elle émet ensuite un ou plusieurs NFT associés à l'œuvre, comportant dans les métadonnées un lien vers l'un des accords de licence[40].

L'accord de licence *Extended* lie l'entreprise et le propriétaire du NFT. Il confère au propriétaire des droits non-exclusifs sur l'œuvre pour le monde entier et jusqu'à l'extinction des droits patrimoniaux de l'auteur sur l'œuvre. Les droits concédés sont le droit de reproduire et représenter l'œuvre associée au NFT dans un contexte public, sur des réseaux sociaux, des places de marché et des métavers à des fins non-commerciales uniquement, ainsi que le droit de revendre le NFT sur le marché secondaire. Diverses dispositions prévoient les conditions dans lesquelles peuvent survenir la revente « *du NFT et des droits associés* » et précisent en particulier que la revente s'accompagne d'un droit de suite. Elles explicitent les conditions d'exécution du contrat et notamment la façon dont certaines conditions sont exécutées automatiquement par un programme autonome sur *blockchain*. Elles rappellent enfin certaines dispositions d'ordre public, en particulier l'incessibilité des droits moraux de l'auteur et le droit de retrait dont il bénéficie.

L'accord de licence *Extended Limited* est identique au précédent, à l'exception de l'ajout d'un droit pour le concessionnaire de réaliser une impression de la photographie pour un usage strictement privé, non-commercial et personnel.

Les deux accords de licence sont soumis à la loi française et désignent la cour d'appel de Paris comme juridiction compétente pour le règlement judiciaire des litiges.

*Source : Textes des accords de licence* Extended *et* Extended Limited *proposés par SAS Exposure arts.*

**Deux obstacles pourraient toutefois s'opposer à cette approche : l'existence d'un écrit et l'exigence du consentement personnel de l'auteur pour tout transfert de droits de propriété intellectuelle.**

**D'une part, comme pour l'ensemble des jetons incorporant des droits, l'écrit est indispensable pour les reventes sur le marché secondaire** dans la mesure où l'article 1322 du Code civil exige que toute cession de créance soit constatée par écrit. En outre, une spécificité des jetons intégrant des droits de propriété intellectuelle est que l'écrit est également indispensable pour la vente primaire, puisqu'en application de l'article L. 131-2 du CPI, « *les contrats par lesquels sont transmis des droits d'auteur doivent être constatés par écrit* ». La problématique de l'écrit, transversale à l'ensemble des cessions de droits sur les *blockchains*, est traitée en section 3 : la mission considère qu'elle peut être surmontée à droit constant.

**D'autre part, selon la majorité de la doctrine, la loi doit être interprétée comme interdisant la sous-cession de droits sans le consentement de l'auteur.** Une telle prescription figure expressément dans le code de la propriété intellectuelle, dans la section consacrée aux contrats d'édition, aux articles L. 132-7 (« *le consentement personnel et donné par écrit de l'auteur est obligatoire* ») et L. 132-16 (« *l'éditeur ne peut transmettre […] le bénéfice du contrat d'édition à des tiers […] sans avoir préalablement obtenu l'autorisation de l'auteur* »). La majorité de la doctrine[41] estime que le respect du droit moral justifie d'appliquer ce principe à l'ensemble des contrats d'exploitation des droits de l'auteur et de considérer que la cession de droit ne peut être qu'*intuitu personæ*. Ainsi, à première vue, l'auteur ne saurait incorporer ses droits dans un NFT et autoriser que la cession du NFT implique cession de ses droits sans son consentement.

---

[40] Le contrat de licence *Extended Limited*, en particulier, est accessible à l'adresse https://ipfs.io/ipfs/bafkreiht5wkbqontiejvrh7fdz5zqteojdeer4jvewfj3qwmw3ndnoil2a (consulté le 22 mars 2023).

[41] Voir en particulier : André Lucas, Agnès Lucas-Schloetter et Carine Bernault, *Traité de la propriété littéraire et artistique*, 5e éd., LexisNexis, 2017, §749 ; Pierre-Yves Gautier, *Droit de la propriété littéraire et artistique*,

L'interprétation que la doctrine fait de l'article L. 132-7 vise à protéger l'auteur contre les atteintes à son droit moral qui pourraient survenir si, à la suite de sous-cessions successives, un tiers non désiré devenait détenteur des droits de propriété intellectuelle cédés. Or, l'émission d'un NFT associé au contrat de licence envisagé pourrait être interprétée comme l'acceptation explicite, par l'auteur, du fait que tout individu pourrait potentiellement réaliser l'exploitation concédée.

**L'existence des licences ouvertes telles que *Creative commons* montre qu'un auteur peut accepter de concéder des droits à des tiers non identifiés dès lors que cette acceptation est expresse**. Pour la diffusion de certaines œuvres de l'esprit, en effet, l'auteur peut choisir, par un contrat de licence, de concéder certains de ses droits patrimoniaux à un tiers indéfini au moment de la publication de l'œuvre[42]. Ce faisant, il autorise par anticipation tout tiers qui le souhaite et qui respecte les conditions posées par la licence à exploiter l'œuvre. Les droits concédés par la licence peuvent notamment être l'usage, la copie, la diffusion, la modification et la réutilisation de l'œuvre, sous certaines réserves fixées par le contrat (par exemple, respecter la paternité de l'auteur original et publier les œuvres dérivées sous une licence similaire).

Ainsi, en présence d'une licence telle que *Creative Commons* :

- le tiers qui exploite l'œuvre conformément aux conditions de la licence (par exemple, le professeur qui imprime un article de l'encyclopédie en de nombreux exemplaires pour ces élèves) est réputé en approuver les termes. En application d'une vision consensualiste du contrat, son engagement est acquis au moment où il réalise l'acte d'exploitation de l'œuvre, qui ne pouvait être licite qu'en respectant le contrat. Il devient cocontractant de l'auteur et bénéficie donc de la cession des droits ;
- le tiers qui réalise une exploitation non prévue par les conditions de la licence (par exemple, qui réalise un travail dérivé sans respecter les termes de la licence) ne peut se prévaloir d'aucun contrat signé avec l'auteur et se rend donc coupable de contrefaçon.

Le contrat de licence est donc compris comme un contrat d'adhésion aux clauses choisies par l'auteur, la réalisation d'un acte d'exploitation étant réputée valoir approbation du contrat par le concessionnaire. La notion de contrat de licence ne figure pas, en tant que telle, dans la partie du code de la propriété intellectuelle consacrée à la propriété littéraire et artistique : les dispositions prévues pour l'ensemble des cessions de droit sont pleinement applicables. La validité d'une telle cession de droits et l'opposabilité des conditions de la licence au concessionnaire sont établies par la jurisprudence, notamment en ce qui concerne les logiciels[43]. Dans une telle situation, c'est bien l'auteur qui cède à *chaque* personne souhaitant utiliser l'œuvre le droit *personnel* d'exploiter l'œuvre dans les conditions qu'il spécifie, sans *intuitu personæ*.

**De ce qui précède, il ressort qu'il est possible qu'un contrat de licence correctement conçu permette l'incorporation d'une concession cessible de droits d'exploitation d'une œuvre — sous réserve que soit confirmé le fait que l'article L. 132-7 du CPI n'y fait pas obstacle.**

---

éd. LGDJ, 2021, §504 ; ou encore *Code de la propriété intellectuelle*, éd. Dalloz, 2023, commentaire d'introduction du chap. I du titre III du livre I et commentaire de l'art. L. 132-7.

[42] Tel est par exemple le cas de l'encyclopédie Wikipédia, diffusée sous la licence libre « *Creative commons – attribution – partage dans des conditions identiques* » (CC-BY-SA).

[43] Voir par exemple : CA de Paris, 16 septembre 2009, n° 04/24298, *Edu 4 c. AFPA* : les termes d'une licence de concession de droits sur le code source d'un logiciel sont opposables au concessionnaire.

### 4.2.3. Cette qualification n'est pertinente que dans le cas où le NFT est créé par l'auteur de l'œuvre ou par un ayant-droit

L'ensemble des développements précédents présument une situation dans laquelle l'émetteur initial du NFT ou du moins du contrat de licence qui l'accompagne, se trouve être l'auteur de l'œuvre de l'esprit protégée et vers laquelle pointe le NFT. La situation dans laquelle l'émetteur du NFT exerce les droits patrimoniaux de l'auteur décédé peut être traitée de façon similaire. Dans cette situation, une cession de droits par l'auteur *via* l'émission du NFT et du contrat de licence associé est envisageable.

Néanmoins, en 2023, de nombreux NFT portent sur des fichiers numériques qui ne sont pas émis par l'auteur ni par ses ayant-droits. Plusieurs cas doivent alors être distingués.

Tout d'abord, **le fichier vers lequel pointe le NFT peut ne pas être une œuvre de l'esprit protégée par le droit d'auteur**. C'est le cas par exemple d'un NFT pointant vers une capture d'écran du premier tweet de l'histoire du réseau social *Twitter* ou d'un NFT portant vers un fichier constitué de formes géométriques simples et sans originalité[44]. Dans une telle situation, il n'existe pas de propriété artistique et littéraire sur le document pointé vers le NFT.

En deuxième lieu, **le NFT peut pointer vers une œuvre de l'esprit élevée au domaine public, c'est-à-dire sur laquelle les droits patrimoniaux ont expiré** : tel est par exemple le cas d'un NFT de *La Joconde* de Léonard de Vinci.

En troisième **lieu, il peut arriver que le NFT pointe vers une œuvre couverte par des droits patrimoniaux, sans que l'auteur ou l'ayant-droit ait consenti à l'émission du NFT**. L'émission, la vente et la cession d'un NFT pointant vers une représentation numérique d'une œuvre constitue sans ambiguïté une exploitation de celle-ci. En l'absence de consentement de l'auteur, l'exploitation constitue une contrefaçon et le NFT est *a fortiori* sans valeur au titre de la propriété littéraire et artistique.

Enfin, en dernier lieu, plusieurs contraintes peuvent s'opposer à ce qu'une œuvre soit « tokénisée », en particulier les droits moraux exercés par les ayants-droits de l'auteur ou l'obligation dans certaines situations de payer une redevance au propriétaire du support de l'œuvre ainsi reproduite[45]. Dans ce cas, un NFT pointant vers cette œuvre serait illicite.

### 4.2.4. L'analyse des droits conférés par le NFT au titre de la propriété littéraire et artistique est indépendante d'éventuels autres droits concédés, notamment en matière de propriété industrielle ou de consommation

**Indépendamment des droits de propriété littéraire et artistique qu'ils confèrent, certains NFT peuvent représenter des titres de droits d'autre nature.**

Par exemple, l'image associée à un NFT et ses métadonnées peuvent impliquer l'usage d'une marque déposée et le NFT peut être associé à un contrat permettant à son porteur de se prévaloir de l'authenticité de la marque : ce cas d'usage est alors encadré par le droit de la propriété industrielle. De même, le détenteur du NFT peut, dans certains cas, se prévaloir du droit à la livraison d'un bien ou à l'exécution d'un service vis-à-vis de l'émetteur, dans les conditions prévues par le code de la consommation. Un exemple est fourni par les NFT que prévoit d'émettre l'entreprise française *EverRose* (*cf.* encadré 8).

---

[44] Le juge du fond pourrait toutefois considérer que l'originalité de la démarche de « tokénisation » fait du document pointé par le NFT une nouvelle œuvre de l'esprit. Une telle reconnaissance resterait cependant exceptionnelle et réservée aux premières œuvres ainsi « tokénisées ».

[45] Pour une analyse exhaustive des conditions dans lesquelles une telle œuvre peut être « tokénisée », *cf.* Pauline Hot, « Qui peut "tokeniser" *La Joconde* ? Jetons non fongibles et domaine public culturel », *Actualité juridique du droit administratif*, n° 29, 2022, p. 1663-1668.

Dans ce cas, les enjeux relatifs à la définition du NFT « artistique » et les droits associés doivent être dissociés des autres droits cédés, chacun pouvant faire l'objet d'analyses indépendantes. Par exemple, un musée propriétaire d'une œuvre célèbre et élevée au domaine public pourrait souhaiter émettre des NFT sur cette œuvre associée à son nom : dans ce cas, le détenteur du NFT ne pourrait se prévaloir d'aucun droit vis-à-vis de l'œuvre, mais disposerait d'un droit authentique et légitime de se prévaloir de la marque du musée.

**Encadré 8 : L'émission de NFT « souvenirs de monuments » par *EverRose***

À la date de la rédaction du rapport, l'entreprise française *EverRose* projette d'émettre des NFT représentant des « souvenirs de monuments ». Pour chaque monument partenaire, l'entreprise prévoit d'éditer plusieurs modèles de « souvenirs » et d'émettre un nombre limité de NFT pointant vers chacune de ces « cartes postales numériques ». La carte serait formée d'une œuvre graphique numérique — éventuellement animée — représentant le monument, auquel serait associé le nom dudit monument et éventuellement sa marque. Enfin, l'application pourrait permettre de participer à des jeux-concours, avec possibilité à la clef de remporter certains services, par exemple un accès privilégié à un monument.

Ce faisant, l'exploitation des NFT met en jeu aux moins quatre familles de droits concédés à l'acquéreur du NFT :

- le droit d'auteur du créateur de l'image formant la « carte postale » numérique, en particulier lorsqu'il s'agit d'une photographie récente ;
- le droit d'auteur éventuel de l'architecte, lorsque le monument en lui-même n'est pas encore dans le domaine public ;
- la propriété industrielle de l'entité exploitant le monument et pouvant détenir des droits de marque sur son image, son nom, un logotype ou encore l'association de plusieurs de ces éléments ;
- les éventuelles créances acquises par le détenteur du NFT vis-à-vis de l'éditeur ou de l'exploitant du monument pour les prestations de service annoncées.

## 4.3. En pratique, les droits conférés par les NFT sont réduits, de sorte que le NFT est davantage un instrument d'ostentation qu'un titre de droits

### 4.3.1. La cession de droits exclusifs d'exploitation aux détenteurs d'un NFT ne peut faire obstacle au droit à la copie privée ni à la représentation de l'œuvre dans un cercle privatif

Parmi les droits pouvant en théorie être concédés par contrat de licence, pourrait figurer celui de copier l'œuvre et d'en jouir à des fins strictement personnelles. Le postulat des défenseurs de cette idée réside dans le fait que, de même que le propriétaire d'un tableau ou d'un disque vinyle ne possède le droit de l'utiliser qu'à des fins privées (apprécier visuellement le tableau dont on est propriétaire, jouer le disque sur un lecteur), le contrat pourrait donner au détenteur du NFT ces droits vis-à-vis d'une œuvre numérique. Ce **droit d'usage privé conféré au détenteur du NFT sur l'œuvre** permettrait une jouissance « licite » de l'œuvre, par opposition à l'usage « illicite » des internautes téléchargeant le fichier sur internet sans en avoir les droits.

**Cependant, l'existence des droits de représentation familiale et de copie privée rend impossible une telle distinction entre copie licite et copie illicite.**

Le code de la propriété intellectuelle protège en principe, au titre des droits patrimoniaux, l'exploitation des œuvres, c'est-à-dire leur reproduction ou leur représentation (art. L. 122-1 du CPI). Toutefois, l'article L. 122-5 du CPI exclut notamment du périmètre de la protection :

- les représentations privées et gratuites effectuées exclusivement dans un cercle de famille (1°) ;

- les copies de certaines œuvres de l'esprit destinées à l'usage privé du copiste, excluant toute utilisation publique, sous réserve que la source de la copie soit licite (2°). Cette exception est qualifiée d'exception pour copie privée. La loi exclut de cette exception les « *copies des œuvres d'art destinées à être utilisées pour des fins identiques à celles pour lesquelles l'œuvre originale a été créée* », mais cette disposition est considérée comme visant les seules œuvres inséparables de leur support corporel[46]. Il est en tout cas admis qu'elle ne restreint pas la copie de vidéos, musiques ou photographies numériques[47]. Les auteurs reçoivent, en contrepartie de cette exception, une rémunération issue du produit de la redevance pour copie privée.

Des exceptions identiques s'appliquent, le cas échéant, aux droits voisins du droit d'auteur (art. L. 211-3 du CPI), notamment les droits des artistes-interprètes, producteurs de phonogrammes et vidéogrammes.

Or, lorsqu'un artiste émet un NFT sur une œuvre d'art qu'il crée, l'œuvre est rendue accessible à toute personne de façon licite : il suffit, pour obtenir une copie de l'œuvre, de suivre le lien figurant dans la mémoire du NFT. En conséquence, **chacun peut réaliser une copie privée de l'œuvre et en réaliser une représentation privée et gratuite, ce qui lui permet d'en jouir de la même façon que s'il possédait le NFT assorti des conditions contractuelles envisagées précédemment.**

Certes, des mesures techniques de protection peuvent être prévues par les titulaires des droits pour limiter la copie des œuvres. Cependant, conformément à l'article L. 331-7 du CPI, ces mesures ne peuvent avoir pour effet de porter atteinte à l'exercice de l'exception de copie privée.

Ainsi, le seul moyen pour un ayant-droit d'éviter que ne s'applique l'exception de copie privée est d'empêcher l'accès licite à l'œuvre. Par exemple, plutôt que de rendre l'œuvre accessible publiquement à l'adresse internet vers laquelle pointe le NFT, il peut faire en sorte que seul le détenteur du NFT à un instant donné puisse la télécharger[48]. Cependant, une telle mesure n'aurait pas pour effet de distinguer des copies « authentiques » de copies « illicites », mais constituerait seulement un outil technique pour gérer l'accès à un fichier numérique. Enfin, **en tout état de cause, le titulaire du NFT à un instant donné pourrait, avant de céder le NFT, réaliser une copie privée** : la perte du NFT n'entraînerait alors pas de perte de la jouissance privée de l'œuvre.

**Ce faisant, le NFT ne peut pas recréer sur une œuvre numérique un droit identique à celui dont dispose le propriétaire du support d'une œuvre physique et ainsi être utilisé comme le témoin de détention d'une version « authentique » de l'œuvre.** Il faut, pour que le NFT apporte effectivement des droits au détenteur, que l'artiste accepte de concéder une exploitation allant au-delà de la seule jouissance privée.

---

[46] Voir notamment André Lucas, Agnès Lucas-Schloetter et Carine Bernault, *Traité de la propriété littéraire et artistique*, 5e éd., LexisNexis, 2017, §414, note n° 918 : « *Il semble toutefois conforme à l'intention du législateur de limiter l'application de la disposition aux cas où l'œuvre prend corps dans un objet corporel dans un objet séparable.* » Les commentaires sous l'art. L. 122-5 dans le *Code de la propriété intellectuelle*, éd. Dalloz, 2023, précisent que la jurisprudence n'a pas permis d'apprécier l'étendue de cette disposition.

[47] Selon le site de la société Copie France, chargée de la collecte de la redevance pour copie privée : « *Nous pouvons tous copier librement des films, séries, photos, documentaires, musiques ou encore livres numériques, sur tous nos appareils (smartphone, box, disques durs externe…), pour notre usage personnel : c'est l'exception de copie privée.* » (https://www.copiefrance.fr/fr/copie-privee/a-quoi-sert-la-copie-privee, consulté le 19 mars 2023).

[48] Par exemple, le serveur correspondant à l'URL du NFT peut distribuer non pas l'œuvre, mais une version de l'œuvre chiffrée avec la clef publique (*cf.* section 1.3 de l'annexe 1) du détenteur du NFT tel qu'il figure dans la *blockchain*. Il peut aussi n'accepter d'envoyer l'œuvre que sous réserve d'authentification avec la clef du détenteur du NFT et répondre par un message d'erreur « accès non autorisé » (erreur 403) dans le cas contraire.

### 4.3.2. Il restera en tout état de cause difficile de distinguer les droits conférés par la détention du NFT des contrefaçons couramment tolérées, de sorte que cette détention restera le plus souvent purement ostentatoire

Une difficulté importante réside dans l'application effective d'une « licence NFT » comme celle envisagée en section 4.2.2. La lutte contre l'utilisation contrefaite d'images, en particulier sur internet, présente en effet un coût élevé en comparaison du préjudice économique que peuvent subir les auteurs. Cette situation conduit en particulier à tolérer des usages d'œuvres sur internet, notamment sur les réseaux sociaux, alors même qu'ils sont contrefaits.

Ainsi, si une « licence NFT » conférait une gamme de droits restreints (droit de copier l'œuvre à des fins personnelles, de la diffuser sur des réseaux sociaux, *etc.*), le détenteur du NFT n'aurait, dans les faits, aucun droit supplémentaire par rapport aux comportements qui auraient pu être les siens en l'absence de détention du NFT et qui seraient tolérés.

**La mission estime donc probable que les NFT artistiques restent, en réalité, des jetons à valeur essentiellement ostentatoire : le détenteur du NFT ne pourrait, dans les faits, pas faire davantage qu'afficher qu'il est le seul à avoir payé pour ce NFT.**

En complément, le NFT peut être associé à certains services délivrés par des tiers, permettant d'accroître sa valeur ostentatoire. Par exemple, les réseaux sociaux *Twitter* et *Instagram* proposent à leurs abonnés d'associer à leur compte une adresse publique sur une *blockchain* et leur offrent la possibilité d'afficher une image de profil spéciale (avec un contour en couleur, par exemple), si cette image correspond à un NFT qu'ils détiennent. De façon similaire, l'horloger TAG Heuer commercialise une montre connectée affichant comme fond une image, sous condition toutefois que le propriétaire de la montre détienne un NFT pointant vers ladite image (*cf.* section 3 de l'annexe III).

### 4.3.3. D'autres cas d'usage des NFT peuvent être envisagés à moyen terme, moyennant une privatisation plus forte des contenus numériques

Au-delà de cette valeur ostentatoire, deux autres utilisations des NFT artistiques, aujourd'hui marginales, pourraient se développer à droit constant ou quasi-constant.

D'une part, **les artistes pourraient souhaiter étendre le périmètre des droits cédés aux consommateurs de contenus artistiques et culturels**. En conférant, par le NFT, des droits plus importants que les usages *de facto* tolérés aujourd'hui, les auteurs pourraient donner un intérêt juridique réel à la détention du jeton. Tel est par exemple le cas de la collection des *Bored Apes Yacht Clubs*, dont la licence de cession de droits autorise une utilisation commerciale[49]. Un tel mouvement correspondrait à un déplacement consenti des droits des artistes au profit de ceux des détenteurs du NFT.

D'autre part, à l'inverse, **des éditeurs de matériel audiovisuel pourraient chercher à restreindre techniquement les exceptions de copie privée et de représentation familiale des œuvres afin de les réserver au détenteur d'un NFT**. De nombreux interlocuteurs rencontrés par la mission envisagent par exemple le développement de métavers dans lesquels il serait rendu techniquement impossible de représenter une image sans détenir un NFT associé à celle-ci. L'idée de cadres de photographie numérique bridés, n'affichant une image que si le propriétaire du cadre détient un NFT associé, est également envisageable.

[49] Les conditions sont disponibles à l'adresse https://boredapeyachtclub.com/#/terms (consultée le 23 mars 2023). La licence présente comme exemple de droit concédé au détenteur du NFT celui d'imprimer l'œuvre sur un T-shirt et de le mettre en vente.

Une telle vision impliquerait toutefois de surmonter de nombreuses difficultés techniques et apparaît inenvisageable sans un mouvement de forte centralisation dans la certification des droits détenus[50], en contradiction frontale avec les objectifs poursuivis par les promoteurs des *blockchains*. Elle induirait un important mouvement de privatisation des droits des utilisateurs vis-à-vis des contenus numériques, les NFT deviendraient un outil de contrôle et de restriction des usages des technologies de l'information et de la communication.

Enfin, les modèles économiques sous-jacents seraient difficilement concevables sans intervention de l'État, puisque l'utilisateur final verrait peu d'intérêt à acheter un matériel informatique bridé. Le bénéfice économique qu'en tireraient les auteurs, en comparaison des intermédiaires, reste en outre incertain.

## 4.4. L'action des pouvoirs publics devrait se concentrer sur l'accompagnement des auteurs pour les aider à définir les droits qu'ils souhaitent concéder, sans qu'une modification législative soit *a priori* requise

### 4.4.1. Une modification des textes régissant la propriété littéraire et artistique n'apparaît pas souhaitable

Comme établi en sections 4.1.2 à 4.2.2, la qualification juridique des NFT liés à des œuvres numériques est complexe et le droit de la propriété intellectuelle en vigueur ne permet pas d'aboutir à une qualification correspondant à la vision qu'en ont les promoteurs des NFT artistiques : œuvres d'art incorporelles, supports d'œuvres d'art, titres de propriété sur des œuvres d'art ou encore « doubles numériques » d'œuvres d'art. En particulier, il est manifestement impossible de garantir, en l'état actuel du droit, des droits sur une œuvre numérique représentés par le NFT qui imiteraient les droits que détient le propriétaire d'une œuvre corporelle.

Il n'apparaît cependant pas pertinent de modifier le code de la propriété intellectuelle pour créer une catégorie juridique correspondante. Aucun des acteurs rencontrés par la mission n'a en effet été en mesure d'exposer en quoi pourrait consister une propriété régie par les règles du Code civil sur une œuvre d'art incorporelle indistincte de sa représentation numérique et donc par nature copiable et non-rivale, sinon en le droit d'auteur en lui-même.

**Le développement des NFT artistiques semble pouvoir advenir dans le cadre juridique en vigueur, par le mécanisme de la licence de droits au détenteur du NFT *via* un contrat d'adhésion. Il n'apparaît pas souhaitable de créer un cadre juridique *ad hoc* pour les NFT adossés à des œuvres d'art.**

Les seules modifications du droit de la propriété intellectuelle qui pourraient être envisagées pour accompagner l'utilisation des NFT artistiques portent sur l'article L. 132-7 relatif à l'exigence d'un consentement personnel de l'auteur en cas de sous-cession de droits de propriété intellectuelle.

[50] Supposons en effet qu'un éditeur de métavers ou d'écrans bridés interdise l'usage d'une image si l'utilisateur ne détient pas un NFT associé : une telle protection pourrait être aisément contournée, car l'utilisateur pourrait *minter* un NFT sur l'image sans détenir les droits. Il serait donc nécessaire, pour que la protection soit efficace, que l'émission du NFT soit le fait de l'ayant-droit, ce qui suppose donc une vérification des droits associés par un tiers de confiance.

### 4.4.2. Les pouvoirs publics devraient initier et accompagner un mouvement de meilleure identification des droits associés aux œuvres

En cohérence avec les développements de la section 2, la protection des consommateurs aussi bien que des auteurs rend souhaitable que les droits associés aux NFT en matière artistique soient mieux identifiés.

**Compte tenu de ce qui précède, les pouvoirs publics et les organismes publics, incluant en particulier les musées, devraient en premier lieu veiller, dans leur communication, à ne pas employer de qualifications inexactes pour les NFT, susceptibles de contribuer à la confusion du grand public.** Devraient en particulier être évitées les références à des œuvres d'art, des supports d'œuvres d'art, des « doubles numériques » d'œuvres d'art, des certificats d'authenticité sur des œuvres d'art ou des titres de propriété d'œuvres d'art.

Au-delà de cette recommandation négative, un enjeu consiste à permettre aux auteurs de disposer de contrats de licence conformes aux dispositions d'ordre public du code de la propriété intellectuelle et permettant d'octroyer des droits clairement identifiés aux détenteurs. Compte tenu des difficultés juridiques identifiées en section 4.2.2, liées notamment à l'exigence d'un consentement personnel de l'auteur à chaque nouvelle cession de droits, une communication des pouvoirs publics sur l'état du droit serait souhaitable.

Afin d'aboutir à une position et une doctrine partagée, le ministère de la culture et le ministère chargé de la transition numérique pourraient donc engager une réflexion sur la validité de contrats de concession en matière de droits d'auteur pour :

- informer le public sur les clauses que doivent contenir les documents contractuels, voire proposer des modèles clefs en main de contrats de licence ;
- le cas échéant, confirmer ou infirmer les analyses précédentes de la mission sur la nécessité ou non de modifier l'article L. 132-7 du CPI pour autoriser de tels contrats de licence.

Dans le cas éventuel où une incompatibilité serait identifiée, dans un souci de neutralité technologique, la modification de l'article L. 132-7 ne devrait pas conduire à insérer des dispositions spécifiques aux NFT mais à revoir de façon générale les conditions dans lesquelles l'auteur peut renoncer à l'*intuitu personæ* en cas de cession de droits.

**<u>Proposition n° 2</u> : Confirmer la compatibilité des dispositions du CPI relatives aux cessions de droit d'auteur (article L. 132-7) avec une licence de cession de droits à une personne identifiée par la détention d'un jeton, et envisager une modification de ces articles dans le seul cas où une incompatibilité serait identifiée. Fournir un modèle de contrat de licence qui pourrait être utilisé par les acteurs économiques.**

# ANNEXE V

# Risques associés aux cryptoactifs faisant l'objet d'une régulation à l'échelle de l'Union européenne

**Annexe V**

# SYNTHÈSE

Les jetons destinés à un usage principalement commercial se distinguent des jetons à vocation financière sous plusieurs aspects : ils sont le plus souvent non fongibles, destinés à la vente à des particuliers et constituent des biens numériques ayant une utilité économique en soi ou sont échangeables contre des biens ou des services qui existent. Plusieurs corpus de normes du droit dérivé de l'Union européenne encadrent leur utilisation.

**En premier lieu, un règlement européen sur les marchés de cryptoactifs (MiCA), dont l'entrée en vigueur est imminente, a pour objet d'encadrer les pratiques des émetteurs de cryptoactifs et des personnes opérant des services sur ceux-ci.** L'un des principaux objectifs du règlement est de prévenir certains risques inhérents à ces marchés et aux plateformes associées : risque associé à la conservation — illustré par la faillite de l'entreprise américaine FTX en novembre 2022 —, insuffisante transparence des émetteurs de jetons sur les caractéristiques des biens qu'ils offrent ou encore abus de marché par des manipulations de cours ou des opérations d'initiés. Le règlement impose aux émetteurs un ensemble d'obligations, notamment celle de notifier un livre blanc lors de l'émission des jetons, et soumet les prestataires de services sur les jetons à un régime d'agrément obligatoire (l'agrément de prestataires de services sur cryptoactifs, en anglais *crypto-assets service provider*, CASP). Il s'inspire d'obligations mises en œuvre en droit interne français depuis 2019 par la loi PACTE — l'agrément de prestataire de services sur actifs numériques (PSAN) étant toutefois seulement facultatif dans le régime français. Le règlement européen innove par rapport au régime français en introduisant des mesures de prévention et d'interdiction des abus de marché proches de celles qui sont applicables aux instruments financiers (interdiction des opérations d'initié, de l'utilisation d'informations privilégiées, des manipulations de cours). Il devrait entrer en application à la fin de l'année 2024.

**Le champ d'application du règlement MiCA laisse néanmoins subsister des ambiguïtés et des angles morts.** Les jetons non fongibles sont exclus de l'ensemble du règlement, sans qu'il soit précisé si les prestataires de services ne maniant que des jetons non fongibles sont eux aussi exclus ou pas. Par ailleurs, les jetons utilitaires sont inclus dans le champ d'application du règlement mais exemptés de certaines obligations (le livre blanc prévu au titre II, notamment). Certaines activités liées à ces jetons (conservation, services de transfert) ne sont pas soumises à l'agrément de CASP. Enfin, les plateformes d'échange pair à pair ne répondent pas à la définition de la plateforme de négociation de MiCA. Comme la négociation sur une telle plateforme est une condition de l'application des dispositions de MiCA sur les abus de marché, les cryptoactifs échangés sur les plateformes pair à pair échappent à cette réglementation.

**La mission considère que ces exclusions sont dommageables car tous les jetons peuvent présenter des risques similaires aux jetons à vocation financière en matière d'abus de marché et de lutte anti-blanchiment.** En effet, les *blockchains* constituent en elles-mêmes une place de marché où les transactions sont publiques et les jetons cotés en permanence. Le fait que chacun puisse effectuer des transactions sur une *blockchain*, *via* plusieurs portefeuilles qui lui appartiennent, augmente de surcroît les risques de manipulation.

**C'est pourquoi la mission recommande d'inclure dans le champ d'application de MiCA les jetons non fongibles** et de leur appliquer le même régime que les jetons utilitaires (exclusion du titre II mais application des règles sur les abus de marché). Par ailleurs, la mission considère que les dispositions sur les abus de marché doivent être applicables à tout cryptoactif, qu'il soit négocié sur une plateforme centralisée ou pas. **Pour les plateformes de pair à pair, qui ne constituent pas des CASP, un régime allégé prévoyant des obligations de loyauté et de vigilance quant aux opérations à risque en matière de LCB-FT et de manipulations de marché devrait être créé.** Dans le but de renforcer la lutte contre les abus de marché, **la mission recommande d'interdire aux émetteurs de jetons à vocation commerciale le rachat de leurs jetons** et **d'obliger les dirigeants des sociétés émettrices de déclarer aux régulateurs leurs achats de jetons**, sur le modèle des obligations relatives aux titres financiers.

**À l'occasion d'une refonte des textes européens sur la LCB-FT, les colégislateurs européens ont inclus une référence au règlement MiCA afin de faire des CASP des entités assujetties aux obligations de LCB-FT, suivant en cela les préconisations du groupe d'action financière (GAFI).** À l'entrée en vigueur des différents textes constituant ce « paquet » LCB-FT, les CASP seront en particulier soumis à des obligations de vigilance et de vérification de leur clientèle et devront partager des informations relatives aux flux de cryptoactifs qu'ils s'échangent pour le compte de leurs clients (« *travel rule* »), ce qui permettra de créer au sein des *blockchains* un environnement régulé dans lequel les personnes à l'origine des transactions peuvent être identifiées par les autorités. La mission s'interroge toutefois sur le caractère suffisant de ces obligations, compte tenu des risques consubstantiels à l'utilisation de *blockchains* et de cryptoactifs, aggravés par le développement de certaines technologies d'anonymisation (*privacy coins*, mixeurs, *layers 2* parmi lesquels le *Lightning Network*). En outre, il reste aisé pour les utilisateurs de quitter l'environnement régulé, notamment par l'intermédiaire des portefeuilles autohébergés. Or, le risque que les jetons soient utilisés à des fins de blanchiment altère en effet la confiance des clients, des investisseurs et des banques et affecte le développement de l'écosystème.

**La mission propose donc de rendre obligatoire la vérification de l'identité du détenteur d'un portefeuille autohébergé pour un paiement supérieur à 1 000 € réalisé vers ou depuis un CASP ou ayant un caractère professionnel.** Cette mesure permettrait de mieux tracer les flux entre l'environnement régulé et l'environnement non régulé. Elle ne permettrait néanmoins pas de remédier à tous les problèmes de blanchiment que posent les *blockchains*, car les flux entre portefeuilles autohébergés demeurent intraçables. Le caractère numérique, donc mobile et immatériel, des cryptoactifs les rend encore plus propices au blanchiment et pourrait justifier un traitement plus strict, si les mesures précédentes étaient considérées comme insuffisantes. Dans un tel cas, la mission propose d'étudier une interdiction de tout transfert de plus de 1 000 € entre un portefeuille hébergé par un CASP et un portefeuille autohébergé, rendant la frontière entre les univers régulé et non régulé encore plus étanche.

**Une dernière source de difficultés réside dans l'application du droit des données personnelles aux utilisateurs de cryptoactifs** puisque par conception, les *blockchains* accueillent des données personnelles rendues publiques de façon irréversible. L'application du règlement général sur la protection des données (RGPD) n'est pas totalement incompatible avec l'utilisation d'une *blockchain* ; elle suppose cependant la mise en œuvre de solutions techniques conduisant à stocker en réalité les données personnelles hors de la *blockchain* et à n'inscrire sur celle-ci que des dérivés de ces données. Aussi, le plein respect du RGPD suppose en pratique une forte recentralisation, incohérente avec l'objet même des *blockchains*.

# SOMMAIRE

## Annexe V

La présente annexe étudie la façon dont les usages commerciaux des *blockchains* sont régis par trois ensembles de réglementations de l'Union européenne :

- la règlementation des émetteurs et prestataires de services sur cryptoactifs (règlement MiCA), destinée principalement à traiter les risques liés aux marchés de ces cryptoactifs et aux plateformes qui les opèrent ;
- le corpus de règlementation applicable en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT) ;
- le règlement général sur la protection des données (RGPD).

**L'axe conducteur de cette analyse repose sur l'identification des spécificités liées aux jetons à vocation commerciale, par opposition aux jetons dont la vocation principale est technique ou financière.** Cette dernière catégorie recouvre notamment les jetons échangeables conçus comme des supports d'échange concurrents aux monnaies étatiques, comme des instruments financiers, comme des produits de placement, ou encore comme titres de droits sur un bien ou un service non encore existant et dont la mise en œuvre dépend de la réussite d'un projet. Les jetons à vocation commerciale (JVC), au contraire, se caractérisent par un faisceau d'indices :

- ils sont principalement proposés à la vente à des particuliers ou, lorsqu'ils le sont à des entreprises, comme consommations intermédiaires ou en vue d'une distribution à des particuliers ;
- ils donnent accès à des biens ou à des services ou constituent eux-mêmes un bien immatériel procurant une jouissance directe à son utilisateur ;
- ils ne sont généralement pas fongibles d'un point de vue technique ; en revanche, ils peuvent l'être d'un point de vue économique lorsqu'ils sont émis en grandes séries ou grandes collections ;
- ils ne sont pas couramment acceptés comme moyens d'échange ;
- ils ne représentent pas de titre de droit à un flux financier futur ;
- les opérations de publicité et de démarchage commercial pour ces jetons se fondent sur des arguments de vente autres que la possibilité d'en retirer un rendement financier ou une plus-value de cession ;
- leur émetteur entend placer les relations contractuelles avec les particuliers qui les détiennent sous l'égide du droit de la consommation plutôt que sous celle du droit monétaire et financier.

Des exemples de jetons à vocation commerciale figurent en annexe III : il s'agit notamment des NFT artistiques, des jetons qui représentent des objets de jeu ou des monnaies de jeu dans des jeux vidéo ou encore des produits de luxe utilisables dans un métavers. La distinction entre les différentes catégories de jetons constitue un exercice complexe, car leurs émetteurs jouissent d'une grande liberté dans les possibilités techniques et les droits juridiques qu'ils confèrent aux détenteurs des jetons (*cf.* annexe IV). La mission ne propose donc pas dans le présent rapport de critère unique permettant de définir cette catégorie qui pourrait être utilisé en droit pour fonder l'application d'un régime juridique.

# 1. Le régime français de régulation des cryptoactifs et le régime européen qui s'y substituera en 2024 visent à encadrer des risques de nature financière associés à leur manipulation

## 1.1. Les cryptoactifs à vocation commerciale et à vocation financière présentent des risques comparables, quoiqu'à des degrés divers

Dans la présente sous-section, les notions de *cryptoactif* et d'*actif numérique* sont utilisées indépendamment pour désigner tout bien incorporel doté d'une valeur, échangé sur la *blockchain*, indépendamment de sa qualification technique (monnaie de chaîne, jeton ERC 20 ou ERC 721, *cf.* annexe II) ou juridique (titre financier, minibon, actif numérique, bien incorporel innomé, *etc.*). Le droit français utilise, dans son état actuel de la loi PACTE, le terme d'actif numérique, tandis que le règlement européen MiCA utilise celui de cryptoactif.

Les cryptoactifs, parce qu'ils sont avant tout des actifs immatériels détenant une valeur et peuvent être achetés et revendus sur des marchés, y compris par des particuliers, sont *a priori* susceptibles de présenter des risques similaires aux actifs financiers (perte de valeur, abus de marché, *etc.*), ce d'autant plus que la *blockchain* constitue en elle-même une place d'échanges instantanés et publics, permettant de valoriser les biens avec un haut niveau de confiance et d'accroître leur liquidité. Un tel constat justifie en particulier le choix fait par le législateur français puis européen (*cf.* section 2.1) d'assujettir intégralement les cryptoactifs présentant les caractéristiques d'instruments financiers (*security tokens)* à la réglementation prévue pour ces derniers. Néanmoins, les *security tokens* ne sont pas les seuls à présenter ces risques : c'est le cas de l'ensemble des cryptoactifs, y compris ceux qui ont une vocation commerciale.

**La réglementation des instruments financiers vise, en premier lieu, à protéger les épargnants contre le risque de perte de valeur des titres achetés.** Elle suppose en particulier une obligation pour l'émetteur, avant l'émission d'actifs financiers ou de leur admission à la négociation sur un marché réglementé, de produire un prospectus d'information et d'obtenir un visa du régulateur[1].

En ce qui concerne les cryptoactifs destinés à un usage commercial, l'objet de l'actif n'est pas, en théorie, d'en faire un support d'investissement. Néanmoins, la mission a pu constater que certains de ces cryptoactifs étaient, dans les faits, utilisés comme tels par leurs acquéreurs. La volatilité de leur valeur sur les marchés secondaires de revente provoque d'ailleurs des pertes, qui peuvent être importantes pour des consommateurs peu avisés. Ce risque reste moins important que pour les actifs financiers dans la mesure où les émetteurs des jetons à vocation commerciale ne mettent pas en avant le rendement potentiel du jeton. Dans le cas où un tel cryptoactif serait présenté comme un support d'investissement avec promesse de rendement, cette activité serait comparable à une intermédiation en biens divers, dont le régime préexiste aux jetons dans le droit français (*cf.* art. L. 551-1 *sq* du code monétaire et financier).

[1] Cette obligation est prévue, à l'échelle européenne, par le règlement (UE) 2017/1129 du Parlement européen et du Conseil du 14 juin 2017 concernant le prospectus à publier en cas d'offre au public de valeurs mobilières ou en vue de l'admission de valeurs mobilières à la négociation sur un marché réglementé, et abrogeant la directive 2003/71/CE.

**Les problématiques liées à l'activité de conservation d'actifs constituent une deuxième catégorie de risques inhérents aux actifs financiers et susceptibles d'apparaître dans l'économie des jetons**. La faillite, en novembre 2022, de la société américaine FTX, qui opérait une plateforme de négociation de cryptoactifs, en est l'illustration. La réglementation impose des exigences de ségrégation des valeurs détenues en propre de celles qui sont détenues pour le compte de clients, une interdiction de placer les valeurs détenues pour le compte des tiers sans leur consentement exprès, ainsi que des obligations de capitalisation et de détention de fonds propres.

Toutefois, ces problématiques découlent en grande partie de la fongibilité des actifs manipulés. S'agissant d'actifs non fongibles (comme les NFT), dont la détention est donc traçable sur une *blockchain*, les risques sont moindres car le suivi individualisé des jetons est possible.

**En troisième lieu, la régulation des cryptoactifs vise à éviter des manipulations de marché comparables à celles qui existent sur les marchés financiers.** De telles manipulations peuvent par exemple consister en la passation de nombreux ordres destinés à faire artificiellement monter ou baisser un cours (*wash trading*), dont certains peuvent être retirés avant leur exécution (*spoofing*), ou encore en la diffusion de fausses informations.

Ces risques sont redoublés lorsque le marché concerné présente une forte liquidité et un caractère potentiellement spéculatif. En effet, les manipulations de marché visent à tirer profit des « bulles » en les amplifiant, voire en les créant, et reposent donc sur la dimension mimétique de certains marchés, comme les marchés financiers. Ces caractéristiques étant retrouvées sur les marchés de cryptoactifs, quelle que soit leur finalité, les risques en matière de manipulations de marché se posent.

**Enfin, en quatrième et dernier lieu, les marchés de cryptoactifs peuvent être affectés par des usages d'informations privilégiées.** Les informations pouvant influencer leur valeur peuvent être de natures extrêmement diversifiées et dépendre des comportements d'acteurs non-financiers. Ainsi, la valeur d'une collection de NFT à caractère exclusivement ostentatoire (bien de luxe dans un métavers, par exemple) pourra dépendre d'annonces publiques de l'intention de célébrités d'acquérir des jetons de la série. La liberté dont jouissent les émetteurs de jetons pour créer des montages économiques potentiellement très complexes peut conduire à la création de biens dont la valorisation dépend de nombreuses sources de données réelles. Les NFT émis par l'entreprise *Sorare*, qui représentent des joueurs de football et permettent de participer à des tournois dont l'issue dépend des performances du joueur représenté dans le monde réel, illustrent ce phénomène : la valeur des cartes dépend directement des performances sportives des joueurs, qui n'émettent pas les jetons et ne sont pas directement liés à l'émetteur. Toutes ces informations affectant la valeur d'un cryptoactif sont autant d'informations privilégiées potentielles qui ne sont pas contrôlées par l'émetteur et qui peuvent donner lieu à des abus de marché.

**En conséquence, le développement des jetons à usage commercial doit être accompagné d'une régulation des risques liés à la transparence des marchés sur lesquels ils s'échangent** : manipulation des marchés et utilisation d'informations privilégiées, selon des mécanismes proches de ceux qui sont valables pour les actifs financiers. Les problématiques associées à la conservation des actifs par des tiers et à la protection des épargnants quant au risque de pertes financières sont en revanche moins prégnantes pour ces jetons.

*

Le droit français comporte depuis 2019 des dispositions visant à réguler deux aspects de l'économie des cryptoactifs : leur émission et la prestation de services associés (achat, vente, conservation, négoce, *etc.*). Ces dispositions, en grande partie inspirées de celles qui sont applicables aux actifs financiers, ont pour objet de couvrir les divers risques financiers qui relèvent, en France, de la compétence de l'Autorité des marchés financiers (protection des épargnants, lutte contre les manipulations de marché, *etc.*) ainsi que les risques de blanchiment d'argent et de financement du terrorisme.

## 1.2. Depuis la loi PACTE de 2019, le droit français régule les émissions de jetons et la prestation de services sur actifs numériques

**À la date de rédaction du présent rapport, les activités liées aux *blockchains* sont encadrées par la réglementation dite des *actifs numériques*, issue de la loi n° 2019-486 du 22 mai 2019 relative à la croissance et à la transformation de l'économie (« loi PACTE »).**

La loi PACTE, en particulier ses articles 85 et 86, introduit dans le code monétaire et financier (CMF) le régime des actifs numériques.

Celui-ci repose sur plusieurs concepts :

- les *dispositifs d'enregistrement électronique partagés* (DEEP), qui ne sont pas expressément définis mais avaient été introduits dans le droit français par une ordonnance de 2017[2]. Cette notion est conçue pour inclure tout registre dont le contenu est distribué, à l'instar des *blockchains*, dans le respect de la neutralité technologique ;
- les *jetons*, définis à l'article L. 552-2 comme les « *bien[s] incorporel[s] représentant, sous forme numérique,* ***un ou plusieurs droits*** *pouvant être inscrits, conservés ou transférés au moyen d'un dispositif d'enregistrement électronique partagé permettant d'identifier, directement ou indirectement, le propriétaire dudit bien* » ;
- les *actifs numériques*, qui peuvent être, conformément à l'article L. 54-10-1 du CMF :
  - soit des *jetons*, à l'exclusion de ceux « *remplissant les caractéristique*s » des instruments financiers et des bons de caisse ;
  - soit « *toute représentation numérique d'une* ***valeur*** *qui n'est pas émise ou garantie par une banque centrale ou par une autorité publique, qui n'est pas nécessairement attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d'une monnaie, mais qui est* ***acceptée par des personnes physiques ou morales comme un moyen d'échange*** *et qui peut être transférée, stockée ou échangée électroniquement* ».

La définition utilisée en droit positif des *jetons* est donc plus restrictive que la définition technique introduite en annexe II du présent rapport. En effet, **la qualification de *jeton* au sens de l'article L. 552-2 du CMF suppose l'existence de droits sous-jacents** : un bien tel qu'un NFT « nu », sans droits associés, (*cf.* sections 1 et 2 de l'annexe IV) ne constitue, *a priori*, pas un *jeton* au sens du code. Par ailleurs, les jetons ayant les caractéristiques d'instruments financiers ou de bons de caisse sont exclus de la catégorie des actifs numériques et les régimes précédemment établis leur restent applicables : le législateur a ainsi entendu confirmer une approche de la régulation des actifs financiers par la substance (quelles sont les caractéristiques des biens et leurs utilisations possibles ?) plutôt que par la forme.

Les « *représentations numériques de valeurs* » recouvrent, quant à elles, principalement les cryptomonnaies[3] de chaînes telles que le bitcoin (*cf.* section 1 de l'annexe II) : ces biens ne représentent en effet un titre de droit sur aucun individu en particulier, mais ont vocation à être acceptés comme moyen d'échange.

**Les dispositions issues de la loi PACTE encadrent deux catégories d'opérations liées aux actifs numériques : les émissions de jetons offerts au public (en anglais « *initial coin offerings* » – ICO) et la prestation de services sur actifs numériques.**

---

[2] 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. Les dispositions de cette ordonnance visaient à autoriser l'utilisation des *blockchains* comme registres de tenue de certains titres financiers, en particulier les bons de caisse (dénommés « minibons »).

[3] Le terme « cryptomonnaie » ne figure pas dans le droit positif afin d'éviter toute ambiguïté quant au fait que ces biens ne sont pas des *monnaies* et, en particulier, n'ont pas de pouvoir libératoire.

### 1.2.1. Le régime du visa facultatif des émissions de jetons offertes au public (ICO) n'a connu qu'un succès limité

Le régime des émissions de jetons offerts au public est prévu aux articles L. 552-1 à L. 552-7 du code monétaire et financier, dans un titre du code également consacré aux intermédiaires en biens divers. Il est conçu pour s'appliquer aux opérations de levées de fonds par l'émission de jetons, par exemple des jetons utilitaires permettant de bénéficier des produits financés par la levée de fonds en jetons ou des jetons de gouvernance permettant de participer à l'élaboration du projet en cours. **La règlementation est prévue à titre subsidiaire** : les régimes établis par les sections du code monétaire et financier relatifs à la monnaie (livre Ier), aux instruments financiers et produits d'épargne (livre II), aux services bancaires, services de paiement et services d'investissement (livre III), au financement participatif (chapitre VIII du titre IV du livre V) et à l'intermédiation en biens divers (chapitre Ier du titre V du livre V) s'appliquent par priorité.

**Les émetteurs de jetons souhaitant les offrir au public disposent de la faculté, optionnelle, de produire un document d'information (livre blanc) sur l'offre et de solliciter un visa de l'Autorité des marchés financiers (AMF).**

Les modalités d'octroi et de retrait du visa sont fixées par le règlement général de l'AMF (art. 711-1 à 715-2). Le document d'information doit en particulier préciser les droits associés aux jetons, les modalités techniques de leur émission, le modèle économique sous-jacent et une estimation des risques associés à l'acquisition des jetons. Il précise la façon dont les fonds collectés sont conservés et utilisés. L'émetteur obtient un visa dont la durée ne peut excéder six mois et a obligation de communiquer publiquement le résultat de l'offre.

Le visa du document d'information associé à l'émission initiale des jetons s'inspire des obligations de prospectus applicables en cas d'émission ou d'admission à la négociation de valeurs mobilières[4], tout en prévoyant un formalisme allégé. **Surtout, contrairement au régime du prospectus, la sollicitation du visa est optionnelle pour les documents d'information sur les émissions de jetons.**

Ce régime facultatif n'a connu qu'un succès limité : au 1er avril 2023, seuls quatre documents d'informations relatifs à des ICO avaient reçu un visa de l'AMF, respectivement en décembre 2019, mai 2020, octobre 2020 et janvier 2023.

### 1.2.2. 71 prestataires de services sur actifs numériques se sont enregistrés auprès de l'AMF, mais aucun n'a sollicité l'agrément facultatif

Le régime de régulation des **prestataires de services sur actifs numériques** (PSAN) vise dix types de services :

- la conservation pour le compte de tiers d'actifs ou des moyens d'accès à ces actifs (c'est-à-dire des clefs cryptographiques qui permettent de les manipuler) ;
- l'achat et la vente d'actifs numériques en monnaie ayant cours légal (fonds ou « monnaie *fiat* »[5]) ;
- l'échange d'actifs numériques contre d'autres actifs numériques, avec ou sans interposition du compte propre du prestataire ;

[4] Obligations prévues par le règlement (UE) 2017/1129 du Parlement européen et du Conseil du 14 juin 2017 concernant le prospectus à publier en cas d'offre au public de valeurs mobilières ou en vue de l'admission de valeurs mobilières à la négociation sur un marché réglementé, et abrogeant la directive 2003/71/CE.

[5] Le terme « *fiat* », couramment utilisée dans l'écosystème des *blockchains*, désigne les monnaies étatiques, qui ont une valeur du seul fait que la loi leur confère unilatéralement un pouvoir libératoire (d'où l'usage du latin *fiat*, subjonctif passif de *faciō*, faire, soit littéralement : « *qu'il soit fait* »).

- l'exploitation d'une plateforme de négociation d'actifs numériques. Ce service est défini comme l'exploitation de « *plateformes de négociations d'actifs numériques, au sein desquelles de multiples intérêts acheteurs et vendeurs exprimés par des tiers pour des actifs numériques contre d'autres actifs numériques ou en monnaie ayant cours légal peuvent interagir d'une manière qui aboutisse à la conclusion de contrats* » (art. D. 54-10-1 CMF) ;
- la réception et la transmission d'ordres sur des actifs numériques pour le compte de tiers ;
- la gestion de portefeuille d'actifs numériques pour le compte de tiers ;
- le conseil aux souscripteurs d'actifs numériques ;
- la prise ferme et le placement garanti ou non d'actifs numériques.

Les prestataires de ces services sont supervisés par l'Autorité des marchés financiers (AMF). **Deux niveaux de régulation sont possibles : un enregistrement ou un agrément.** L'enregistrement est obligatoire pour l'exercice des prestations de conservation, d'achat et vente, d'échange et d'exploitation d'une plateforme de négociation. L'agrément est facultatif pour l'ensemble des services.

**Lors de l'enregistrement d'un prestataire de services sur actifs numériques**, **l'AMF mène des vérifications d'honorabilité et de compétence de ses dirigeants, s'assure qu'il est établi dans l'espace économique européen et qu'il est en mesure (pour les services de conservation, d'achat-vente et d'échange uniquement) de respecter certaines obligations au titre de la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT)** : identification de la clientèle (*customer due diligence*, CDD) et vigilance vis-à-vis de celle-ci, vigilance vis-à-vis des flux suspects, mise en œuvre des mesures de gels d'avoirs. Elle recueille l'avis conforme de l'Autorité de contrôle prudentiel et de résolution (ACPR), compétente en matière de LCB-FT.

**L'agrément suppose, outre le respect des conditions de l'enregistrement, que soient notamment remplies les conditions suivantes** :

- pour tous les services, le fait de disposer d'une **assurance responsabilité civile professionnelle ou alternativement d'un niveau de fonds propres suffisant**[6], d'un dispositif de sécurité et de contrôle interne adéquat, d'un système informatique résilient et sécurisé et d'un système de gestion des conflits d'intérêt ;
- pour les conservateurs, l'établissement d'une **politique de conservation**, la **ségrégation** des actifs propres et des actifs des tiers et l'absence d'utilisation des actifs ou des clefs des tiers sauf consentement exprès ;
- pour les prestataires de services d'achat, de vente et d'échange, la **publication du prix ferme des actifs ou de la méthode de détermination de ces prix** et la **publication du volume et du prix des transactions réalisées** ;

[6] Le niveau de fonds propres exigé pour l'obtention de l'agrément est fixé par le règlement général de l'AMF, qui renvoie lui-même à une instruction. L'instruction DOC-2019-23 fixe plusieurs conditions cumulatives sur le niveau de ces fonds propres. En premier lieu, le capital social du prestataire doit être au moins égal à 50 000 € ou 150 000 € selon le type de service. En second lieu, les fonds propres doivent être d'au moins 25 % des frais généraux annuels du prestataire. En troisième lieu, ils doivent être d'au moins 4,5 % de la valeur des actifs numériques détenus en propre. En dernier lieu, ils doivent dépasser un seuil dépendant du service effectué et du niveau d'activité de ce service, lequel est en particulier de 2 % de la valeur des actifs conservés pour l'activité de conservation et de 0,05 % du volume de transactions réalisé au cours des trois exercices précédents pour les activités d'achat, de vente, d'échange ou d'exploitation de plateforme de négociation.

- pour les exploitants de plateformes de négociation, la définition de règles de fonctionnement[7] et la **publication du détail des ordres de transactions conclues**. En outre, les exploitants de plateformes ne peuvent engager leurs propres capitaux sur les plateformes qu'ils gèrent que pour assurer la liquidité sur la plateforme ou si « *le montant des transactions réalisées est proportionné à la capitalisation totale du marché de l'actif numérique concerné* ».

**Ainsi, si l'enregistrement, obligatoire, vise avant tout à permettre l'identification des entités, à assurer l'honorabilité de leurs dirigeants et à garantir qu'elles sont en mesure de mettre en œuvre les obligations relatives à la LCB-FT et au gel d'avoirs, seul l'agrément optionnel est de nature à prévenir les risques financiers exposés en section 1.1.** Pour les prestataires bénéficiant d'un simple enregistrement, le seul moyen dont disposent les régulateurs de prévenir ces risques repose sur l'interprétation de l'obligation d'honorabilité et de compétence[8].

Or, si l'enregistrement obligatoire a bien été sollicité et obtenu, au 5 avril 2023, par 71 PSAN[9], **aucun n'a, à la même date, sollicité l'agrément facultatif.** Les PSAN rencontrés par la mission expliquent ce désintérêt par la faiblesse de l'incitation à obtenir l'agrément (le gain réputationnel étant à mettre en regard des coûts de conformité) et par la difficulté à obtenir une assurance responsabilité civile professionnelle (RCP) — étant précisé, toutefois, que cette condition ne constitue qu'une alternative au respect des seuils de fonds propres.

[7] Ces règles de fonctionnement précisent notamment les conditions dans lesquelles l'opérateur dispose d'un pouvoir discrétionnaire sur l'exécution des ordres, les règles de priorité dans l'exécution des ordres ainsi que les règles de suspension des négociations.

[8] La seule décision de radiation d'un PSAN enregistré pour manquement à ses obligations, prononcée le 27 septembre 2022 par le collège de supervision de l'AMF contre la société BYKEP SAS, est fondée d'une part sur les défaillances dans les procédures de LCB-FT et d'autre part sur le fait que « *les informations collectées [...] démontrent notamment i) des opérations effectuées au débit de portefeuilles de clients sans le consentement de ceux-ci, et ii) une information infidèle et inexacte du solde de leur compte* », ce que l'AMF analyse comme des « *manquements aux exigences [...] d'honorabilité et de compétence des dirigeants* ». La décision est publiée sur le site de l'AMF : https://www.amf-france.org/sites/institutionnel/files/private/2022-09/decision_de_radiation_-_bykep_0.pdf.

[9] Dont deux ont été radiés en septembre 2022 : l'un à la suite de l'arrêt de son activité, l'autre pour non-respect des exigences d'enregistrement (*cf.* note 8 *supra*).

## 1.3. Le règlement européen sur les marchés de cryptoactifs (MiCA), dont l'adoption définitive est prévue au second trimestre 2023, s'inspire du droit français issu de la loi PACTE

### 1.3.1. Le règlement MiCA régule les émissions et la prestation de services sur les cryptoactifs, avec une attention particulière portée aux cryptoactifs utilisés comme substituts de monnaies

La Commission européenne a soumis, le 24 septembre 2020, une proposition de règlement sur les marchés de cryptoactifs (*markets in crypto-assets, MiCA*)[10]. Le texte a fait l'objet d'un accord politique entre le Parlement européen et le Conseil le 5 octobre 2022 et a été adopté dans sa version définitive par le Parlement européen le 20 avril 2023. À la date de rédaction de la présente annexe, l'adoption définitive du texte et sa promulgation sont attendues de façon imminente. Les références aux dispositions du règlement visent le texte en français adopté par le Parlement européen le 20 avril 2023[11].

Le projet de règlement a été conçu et rédigé dans le contexte du lancement, par l'entreprise *Facebook* (par la suite devenue *Meta*), d'un projet de *stablecoin* appelée *Libra* (par la suite renommé *Diem*). Ce *stablecoin*, dont la valeur aurait été assise sur un panier de devises et d'actifs financiers, était présenté par *Facebook* comme destiné à une utilisation par le grand public, en concurrence avec les monnaies étatiques. Le projet de règlement MiCA prévoit, en conséquence, un traitement spécifique pour les jetons destinés à devenir des moyens d'échanges. Cette architecture subsiste dans le texte définitif, bien que le projet *Libra* ait depuis été abandonné.

**Le règlement encadre un ensemble d'actions relatives à l'émission et à l'utilisation de cryptoactifs.** Ces derniers sont définis à l'article 3(1)(5) du règlement comme « ***une représentation numérique d'une valeur ou d'un droit pouvant être transférée et stockée de manière électronique, au moyen de la technologie des registres distribués ou d'une technologie similaire*** ». Contrairement à la définition des actifs numériques introduite en droit interne par la loi PACTE, un jeton sans droit associé constitue un cryptoactif au sens du règlement du seul fait qu'il possède une valeur, et ce, quand bien même cette valeur ne suffirait pas à en faire un moyen d'échange couramment accepté.

**Le règlement se focalise sur les cryptoactifs à vocation financière[12] qui ne relèvent pas déjà d'une autre règlementation.** Sont donc exclus de son champ d'application les instruments financiers, les dépôts ou dépôts structurés, les fonds (monnaie *fiat*[13]), les positions de titrisation, les produits d'assurance, produits de retraite ou d'épargne-retraite, ainsi que les produits de sécurité sociale. Par ailleurs, la plupart des jetons à vocation commerciale sont exclus du champ du règlement ou de certaines parties de celui-ci.

---

[10] Proposition de règlement du Parlement européen et du Conseil sur les marchés de cryptoactifs et modifiant la directive (UE) 2019/1937 (COM/2020/593 final). Document EUR-Lex n° 52020PC0593.

[11] Texte adopté n° P9_TA(2023)0117 (https://www.europarl.europa.eu/doceo/document/TA-9-2023-0117_FR.pdf, consulté le 24 avril 2023).

[12] Les jetons assimilés à des instruments financiers (*security tokens*) ne sont pas inclus dans le champ d'application du règlement MiCA et font l'objet d'un régime de régulation spécifique, plus strict, prévu par les directives « prospectus », « MiFID » et « MAR ».

[13] L'expression « monnaie *fiat* », présent dans la version française de la proposition législative de la Commission, a été remplacée par le terme « fonds » lors du travail des jurislinguistes à l'automne 2022, par cohérence avec les choix de traduction opérés dans d'autres textes. Aussi, au sens des définitions ayant cours en droit dérivé de l'Union européenne, des bitcoins, éthers ou autres cryptoactifs utilisés comme monnaie ne peuvent pas être regardés comme des *fonds*.

Au sein des cryptoactifs, sont distinguées trois catégories :

- les *jetons de monnaie électronique* (*e-money tokens*, EMT, appelés dans le langage courant « *stablecoins* »[14]), soit les jetons qui « *visent à conserver une valeur stable en se référant à la valeur d'une monnaie officielle* » (art. 3(1)(7)) et sont nécessairement remboursables en échange de leur contre-valeur monétaire ;
- les *jetons se référant à un ou des actifs* (*asset-referenced tokens*, ART), soit les jetons qui ne sont pas des EMT et qui visent à « *conserver une valeur stable en se référant à une autre valeur ou un autre droit ou à une combinaison de ceux-ci, y compris une ou plusieurs monnaies officielles* » (art. 3(1)(6)) ;
- les autres cryptoactifs, désignés dans le texte comme « *cryptoactifs autres que des jetons se référant à un ou des actifs ou des jetons de monnaie électronique* ».

Les deux premières catégories de jetons ont pour point commun d'être conçus comme de potentiels moyens d'échange, sans toutefois, contrairement à la monnaie, avoir de caractère libératoire. Ces jetons sont, par nature, fongibles. En vertu des titres III et IV du règlement, la supervision des opérations qui leur sont associées relève principalement de la compétence de l'Autorité bancaire européenne (ABE) et de son réseau, en France, l'Autorité de contrôle prudentiel et de résolution (ACPR). L'étude de ces jetons et des dispositions qui leur sont applicables ne relève pas du périmètre de la présente mission.

La catégorie des *autres jetons* accueille quant à elle des biens dont la finalité est potentiellement très diverse ; elle inclut en particulier l'ensemble des actifs numériques destinés à la consommation, qui constituent l'objet de la mission. En vertu du titre II du règlement, la supervision des opérations sur ces jetons relève principalement de l'Autorité européenne des marchés financiers (AEMF) et de son réseau, en France, l'Autorité des marchés financiers (AMF).

**L'organisation du règlement est la suivante :**

- **le titre I** comporte les définitions et le champ d'application ;
- **les titres II, III et IV** portent sur les obligations qui reposent sur les émetteurs de jetons : respectivement des *autres jetons*, des ART et des EMT ;
- **le titre V** définit le régime des prestataires de services sur cryptoactifs (CASP) ;
- **le titre VI** formule les prescriptions en matière d'abus de marché ;
- **le titre VII** porte sur les pouvoirs des autorités de régulation ;
- **les titres VIII et IX** incluent les dispositions transitoires, finales et relatives aux pouvoirs délégués à la Commission.

**Dans la présente annexe, la mission se concentre sur l'application des titres II, V et VI aux jetons à vocation commerciale et aux personnes et entités qui les manipulent.** Les sections 1.3.2 à 1.3.4 présentent les règles que prévoient ces trois titres pour les cryptoactifs qui relèvent de leur champ. La façon dont ces différents titres s'appliquent aux jetons à vocation commerciale est quant à elle discutée *infra* en section 2.1.

[14] Les ART peuvent également être qualifiés de *stablecoins* mais, en l'absence de précision, un *stablecoin* désigne plus souvent un cryptoactif se référant à une monnaie officielle qu'un cryptoactif assis sur un panier composite d'actifs.

### 1.3.2. Le titre II du règlement prévoit une obligation de notification d'un livre blanc pour les cryptoactifs offerts au public pour plus de 1 M€ ou admis à la négociation

Les dispositions relatives à l'émission de jetons diffèrent selon la catégorie de jetons concernés. En ce qui concerne les cryptoactifs autres que les EMT et les ART, objets de la mission, le régime est celui de la notification préalable d'un livre blanc (*white paper*). L'offreur au public doit établir et notifier un livre blanc : cette règle est inspirée du régime des prospectus notifiés à l'émission d'actifs financiers, bien que leur contenu diffère significativement. Le contenu et la forme du livre blanc sont fixés par l'article 6 du règlement, de façon à informer l'investisseur potentiel quant à la nature des produits achetés, à l'utilisation des fonds collectés et aux risques potentiels associés (*cf.* encadré 1).

Cette obligation de notification d'un livre blanc ne s'applique cependant pas à certains jetons qui, du fait de leur nature, sont exclus du périmètre du règlement (jetons non fongibles) ou du seul titre consacré aux émissions de jetons (certains jetons utilitaires, *cf.* section 2.1.3). Elle ne porte par ailleurs que sur les cryptoactifs qui présentent un enjeu significatif de protection du public, parce qu'ils entrent dans l'une de ces deux catégories :

- ils sont offerts à au moins 150 personnes, ne sont pas réservés à des investisseurs qualifiés[15] et représentent un montant d'au moins 1 M€, ces critères étant cumulatifs (exceptions *de minimis*). Le livre blanc est alors rédigé par l'émetteur ;
- ils sont admis à la négociation sur une plateforme de négociation de cryptoactifs. Le livre blanc est alors rédigé par la personne qui demande l'admission à la négociation ou par l'exploitant de la plateforme de négociation.

Cette obligation est donc essentiellement conçue pour la prévention des risques financiers associés aux cryptoactifs utilisés comme placements ou comme moyens de levée de fonds et offerts au public.

Le titre II comporte par ailleurs des dispositions relatives aux communications promotionnelles réalisées par les offreurs de jetons.

**Encadré 1 : Contenu et forme des livres blancs sur les cryptoactifs autres que des EMT et des ART**

Conformément à l'article 6 du règlement MiCA, le livre blanc associé à un cryptoactif doit contenir les informations suivantes :

- des informations sur l'émetteur (nom, forme juridique, adresse, contacts, société-mère, situation financière) ;
- des informations sur l'offreur ou la personne qui demande l'admission à la négociation et, dans ce dernier cas, sur l'exploitant de la plateforme de négociation concernée ;
- des informations sur le cryptoactif, sur l'opération d'offre publique ou les conditions de sa négociation, sur les mesures prises pour la protection des acquéreurs (conditions de remboursement, de rétractation) et, lors d'une offre publique, sur l'utilisation des fonds collectés ;
- des informations sur la technologie sous-jacente, notamment la technologie de consensus utilisée sur la *blockchain* considérée (preuve de travail ou d'enjeu ou tout autre mode de création de consensus, *cf.* annexe I) et sur d'éventuels audits menés à ce sujet ;
- des informations sur les droits associés aux cryptoactifs et en particulier sur la façon dont ces droits peuvent être modifiés. En revanche, il n'est pas exigé que le livre blanc définisse les conditions contractuelles associées aux jetons (*cf.* section 2 de l'annexe IV) ;

[15] Ces investisseurs correspondent aux « clients professionnels » au sens de la directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers (directive MiFID). Il s'agit, en particulier, des établissements de crédit, entreprises d'investissement, de certaines grandes entreprises, des États et investisseurs institutionnels publics, *etc.*

- des informations sur les risques associés à l'offre ou à la négociation du cryptoactif.

Les informations précises exigées dans le livre-blanc sont décrites à l'annexe I du règlement.

Ce livre blanc doit par ailleurs inclure certaines mentions visant à attirer l'attention de l'investisseur potentiel contre les risques associés à ces jetons, utilisés comme outils de placement. Ces mentions sont en particulier :

- les phrases « *Le présent livre blanc sur les cryptoactifs n'a pas été approuvé par une autorité compétente d'un État membre de l'Union européenne. L'offreur du cryptoactif est seul responsable du contenu du présent livre blanc sur les cryptoactifs* »[16] ;
- des déclarations claires et univoques selon lesquelles les cryptoactifs peuvent perdre l'intégralité ou une partie de leur valeur, ne sont pas toujours cessibles ni liquides et ne sont pas concernés par les dispositifs d'indemnisation des investisseurs ni de garantie du dépôt.

### 1.3.3. Le titre V du règlement prévoit un agrément obligatoire pour les prestataires de services sur cryptoactifs (CASP)

À l'instar de la loi PACTE, le règlement MiCA définit une catégorie de prestataires de services, qualifiés de *prestataires de services sur cryptoactifs* (en anglais *crypto-assets service providers*, CASP). Les catégories de services sur cryptoactifs sont similaires à celles qui sont prévues par le droit français, puisqu'il s'agit (art. 2(16)) :

- de la conservation et de l'administration de cryptoactifs pour le compte de clients ;
- de l'exploitation d'une plateforme de négociation de cryptoactifs ;
- de l'échange de cryptoactifs contre des fonds, c'est-à-dire de la monnaie *fiat*, ou contre d'autres cryptoactifs ;
- de l'exécution ou de la réception et transmission d'ordres sur cryptoactifs pour le compte de clients ;
- de la fourniture de services de transfert de cryptoactifs pour le compte de clients ;
- du placement et de la gestion de portefeuilles de cryptoactifs ;
- de la fourniture de conseils en cryptoactifs.

**Le règlement MiCA soumet la prestation de services sur cryptoactifs à l'obtention d'un agrément (art. 59), valable sur l'ensemble du territoire de l'Union.**

Les conditions de l'agrément et les obligations auxquelles sont assujettis les prestataires de services sont prévus par les articles 59 à 85 du règlement. Elles s'apparentent à celles qui sont prévues par la loi PACTE pour le régime français des PSAN.

L'ensemble des CASP ont une obligation de compétence et d'honorabilité et doivent en particulier apporter la preuve de leur absence de condamnation au titre de certaines catégories d'infractions (en matière commerciale, d'insolvabilité, de services financiers, de LCB-FT, de fraude ou de responsabilité professionnelle). Ils font face à des obligations prudentielles, qui supposent un niveau de fonds propres calculé de façon comparable aux dispositions du droit interne, auxquels peuvent partiellement se substituer une police d'assurance[17]. Dès lors qu'ils détiennent des cryptoactifs pour le compte de leurs clients, ils séparent ceux-ci des cryptoactifs qu'ils détiennent en propre.

---

[16] Alors que la loi PACTE prévoit une possibilité optionnelle d'agrément du livre blanc associé à une ICO, le règlement MiCA ne prévoit aucun visa ni agrément de l'autorité de régulation pour les émissions de jetons relevant du titre II. Seuls les jetons se référant à des actifs (ART) qui représentent un montant supérieur à 5 M€ relèvent d'un régime d'agrément, lequel est obligatoire (art. 16 à 18).

[17] Il existe d'une part une obligation de capitalisation minimale dépendant du type de services opérés et du niveau d'activité et, d'autre part, une obligation prudentielle pouvant être réalisée par la détention de fonds propres ou la souscription à une police d'assurance, pour un montant au moins égal à cette obligation minimale de capitalisation et à un quart des frais généraux annuels.

L'assujettissement des CASP à des obligations au titre de la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT) découlera d'un projet de règlement se substituant à la directive (UE) 2015/849 du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme (*cf.* 3.2). Le règlement MiCA leur impose par ailleurs de mettre en œuvre des « *mécanismes, politiques, vérifications et procédures de contrôle interne […] qui permettent de détecter, d'évaluer et de gérer les risques, notamment en matière de blanchiment de capitaux et de financement du terrorisme* » (article 62).

Outre ces obligations valables pour l'ensemble des CASP, le règlement MiCA prévoit des obligations spécifiques à chaque catégorie de services sur cryptoactifs. Ainsi :

- les prestataires de services de **conservation** ont l'obligation de définir une politique de conservation, de tenir à jour un registre des positions de chaque client et de séparer juridiquement et fonctionnellement les actifs détenus des actifs conservés en propre ;
- les exploitants de **plateformes de négociation** définissent des règles de fonctionnement dont la teneur est prévue par le règlement. Leurs systèmes d'information doivent permettre de traiter des volumes élevés d'ordres et de messages, de rejeter automatiquement des ordres manifestement erronés et doivent rester fonctionnels pendant des périodes de tension du marché, ce qu'un *stress test* doit être en mesure de démontrer. Ils sont tenus de publier de façon continue certaines informations relatives aux négociations en cours. **Par ailleurs, il appartient aux exploitants de ces plateformes de garantir le respect des dispositions relatives à l'existence d'un livre blanc pour les actifs qu'ils admettent à la négociation** ; autrement dit, les plateformes de négociation ne peuvent admettre à la négociation un jeton relevant du champ du titre II du règlement MiCA qu'après avoir vérifié qu'un tel livre blanc avait bien été notifié.

### 1.3.4. Le titre VI du règlement établit des prescriptions relatives à la prévention des abus de marché sur cryptoactifs, avec lesquelles le droit interne devra être mis en cohérence

Le titre VI du règlement MiCA instaure des règles sur le comportement des personnes intervenant sur les marchés de cryptoactifs, quel que soit leur rôle, dans le but de prévenir les abus de marché. Il s'agit d'une innovation par rapport au cadre réglementaire de la loi PACTE, qui ne comportait pas de dispositions en la matière.

#### *1.3.4.1. Le cadre de régulation des abus de marchés est établi par référence à celui qui est prévu pour les instruments financiers, sous réserve d'assouplissements*

Les opérations passées sur les cryptoactifs relèvent d'un régime établi par référence à celui qui est prévu pour les instruments financiers par le règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché, dit règlement sur les abus de marché (*market abuse regulation*, MAR). Il est en revanche volontairement assoupli par rapport à ce règlement. Les colégislateurs estiment en effet (considérant 95) qu'« *il est important d'assurer la confiance dans les marchés de cryptoactifs et l'intégrité de ces marchés. Il est dès lors nécessaire d'établir des règles visant à dissuader tout abus de marché pour les cryptoactifs qui sont admis à la négociation. Toutefois, étant donné que les émetteurs de cryptoactifs et les prestataires de services sur cryptoactifs sont très souvent des PME, il serait disproportionné de les soumettre à l'ensemble des dispositions du règlement (UE) n° 596/2014 du Parlement européen et du Conseil* ».

Ainsi, à l'instar du règlement sur les abus de marché, le titre VI du règlement MiCA prohibe et prévient deux principales catégories d'infractions :

- les abus liés aux informations privilégiées : opérations d'initiés et divulgation illicite d'informations privilégiées. Il prévoit également les conditions dans lesquelles les émetteurs, offreurs et personnes qui demandent l'admission à la négociation de cryptoactifs rendent publiques les informations privilégiées dont ils disposent ;
- les manipulations de marchés.

L'article 86 précise le champ d'application de ce titre. **Celui-ci couvre les cryptoactifs « *admis à la négociation ou ayant fait l'objet d'une demande d'admission à la négociation* ».** Sont couverts l'ensemble des agissements relatifs à ces cryptoactifs, quelle que soit la personne qui les accomplit : « *toute transaction, tout ordre ou tout comportement* », qu'il s'agisse d'« *actions menées* » ou d'« *omissions commises* », doit respecter les dispositions du titre VI. Le lieu réel ou virtuel sur lequel interviennent les actions ou omissions est sans conséquence sur l'applicabilité du titre : les actions et omissions sont couvertes indépendamment du fait qu'elles surviennent ou non sur une plateforme de négociation et qu'elles aient lieu dans l'Union européenne ou dans un pays tiers.

Le champ d'application de ce titre VI apparaît donc particulièrement large et peut sembler de nature à couvrir l'ensemble des cryptoactifs pour lesquels il existe un marché où est susceptible d'être commis un abus que le règlement a pour objectif de prévenir. **Néanmoins, seuls les cryptoactifs admis à la négociation sur une place de marché centralisée ou faisant l'objet d'une demande d'admission sur une telle place de marché sont couverts par le titre VI, ce qui exclut les cryptoactifs échangés de pair à pair (*cf.* section 2.3.1).**

#### *1.3.4.2. L'usage et la publication d'informations privilégiées sont encadrés et les opérations d'initiés et manipulations de marché interdites, sous le contrôle des plateformes de négociation centralisées*

**Le règlement encadre, d'une part, la façon dont sont traitées les informations privilégiées.** Une information privilégiée est définie à l'article 87, de façon similaire au règlement sur les abus de marché, la référence aux actifs financiers étant remplacée par une référence aux cryptoactifs. Une information privilégiée est définie comme une information remplissant trois critères :

- elle a un caractère précis, c'est-à-dire qu'elle fait référence à un ensemble de circonstances ou à un événement qui s'est produit ou dont on peut raisonnablement penser qu'il se produira et permet d'en tirer une conclusion quant à l'effet possible sur le prix de cryptoactifs ;
- elle concerne un ou plusieurs cryptoactifs ou bien un ou plusieurs émetteurs, offreurs ou personnes qui demandent l'admission à la négociation de cryptoactifs ;
- elle serait susceptible d'influencer de façon sensible le prix du cryptoactif ou d'un cryptoactif lié aux cryptoactifs ou personnes visées au point précédent si elle était rendue publique.

Cette définition est donc large, puisqu'elle recouvre l'ensemble des informations précises pouvant affecter le prix des cryptoactifs, y compris si elle n'a pas pour origine l'émetteur du cryptoactif ou une personne qui lui est liée.

Les émetteurs, offreurs et personnes qui demandent l'admission à la négociation de cryptoactifs ont obligation de rendre publiques les informations privilégiées qui les concernent directement ; ils ont cependant la possibilité de différer la publication si cela permet de protéger leurs intérêts légitimes sans induire le public en erreur et si l'information peut être maintenue confidentielle, sous réserve d'en informer le régulateur.

L'abus d'utilisation d'informations privilégiées constitue une opération d'initié interdite. Une telle opération d'initié est réputée se produire lorsque sont réunies les conditions suivantes :

- une personne détient une information privilégiée ;
- elle en fait usage en acquérant ou en cédant des cryptoactifs ou annule ou modifie un ordre ou une offre concernant un cryptoactif auquel l'information se rapporte ;
- l'une des trois conditions suivantes est remplie :
  - soit elle a acquis cette information du fait de ses fonctions auprès de l'émetteur du cryptoactif, de son offreur, de la personne qui demande son admission à la négociation, ou de fonctions qu'elle exerce dans le secteur des technologies *blockchains* ;
  - soit elle l'a acquise en participant à des activités criminelles ;
  - soit elle sait ou devrait savoir qu'il s'agit d'une information privilégiée. Autrement dit, dans le cas où l'information n'a pas été acquise du fait des fonctions précitées ou d'activités criminelles, l'agissement n'est qualifié d'opération d'initié que si la preuve de la connaissance du caractère privilégié de l'information est apportée.

De même, l'utilisation d'une recommandation ou d'une incitation fondée sur des informations privilégiées, en connaissance de cause, est interdite.

Enfin, la divulgation illicite d'informations privilégiées, en dehors du cadre normal de l'exercice d'un emploi, d'une profession ou de fonctions est interdite. Le règlement MiCA n'apporte pas de définition de ce qui constitue une divulgation *illicite*. Cette définition pourrait être entendue comme identique à celle établie par l'article 10 du règlement sur les abus de marché : « *une divulgation illicite d'informations privilégiées se produit lorsqu'une personne est en possession d'une information privilégiée et divulgue cette information à une autre personne, sauf lorsque cette divulgation a lieu dans le cadre normal de l'exercice d'un travail, d'une profession ou de fonctions* ». Ce dernier règlement précise que l'infraction s'applique aux mêmes personnes que celles qui sont visées par l'interdiction des opérations d'initié, c'est-à-dire celles qui ont acquis l'information à l'occasion de leurs fonctions auprès de l'émetteur, d'activités criminelles ou qui savent ou devraient savoir qu'il s'agit d'une information privilégiée. Une telle précision ne figure cependant pas dans le règlement MiCA. De l'avis de la mission, au vu en particulier du considérant (95), il est raisonnable de considérer que cette infraction de divulgation illicite concerne les mêmes personnes que l'interdiction des opérations d'initié.

**En ce qui concerne les manipulations de marché, la définition des opérations interdites est fixée par l'article 91.**

Les manipulations de marchés englobent :

- l'ensemble des ordres, transactions ou comportements qui donnent des indications fausses ou trompeuses en ce qui concerne l'offre, la demande ou le prix d'un cryptoactif ou qui sont susceptibles de fixer à un niveau anormal ou artificiel le prix d'un cryptoactif ;
- les procédés fictifs ou toutes les formes de tromperies ou d'artifice visant à influencer le prix d'un ou plusieurs cryptoactifs ;
- la diffusion, en connaissance de cause, d'informations fausses ou trompeuses ayant le même effet.

En outre, sont considérés comme des manipulations de marché :

- le fait de s'assurer d'une position dominante permettant de fixer les prix d'achat ou de vente ou d'assurer des conditions de transaction inéquitables ;
- le fait de perturber le fonctionnement d'une plateforme de négociation de cryptoactifs ou de compliquer la reconnaissance des véritables ordres ;
- le fait de créer une indication fausse ou trompeuse quant à l'offre, la demande ou le prix d'un cryptoactif en exacerbant les tendances de marché ;

- le fait d'utiliser un accès aux médias pour émettre un avis sur un cryptoactif après avoir pris des positions sur celui-ci de façon à profiter des conséquences de cet avis sur le prix du cryptoactif.

#### *1.3.4.3. La mise en œuvre de ces interdictions repose sur des sanctions administratives et pénales, qui seraient rendues plus lisibles par une mise en cohérence du droit interne*

L'application des prescriptions du titre VI repose sur un régime de régulation *a priori* et de sanction *a posteriori*.

L'application de ces prescriptions repose, en amont, sur une obligation de notification des comportements suspects par les personnes opérant ou intervenant sur les marchés à titre professionnel :

- les CASP exploitant une plateforme de négociation de cryptoactifs, d'une part « *informent leur autorité compétente lorsqu'ils constatent des cas d'abus de marché ou des tentatives d'abus de marché commis sur ou via leurs systèmes de négociation* ». Ils sont soumis à la régulation de l'AEMF ;
- les autres personnes qui organisent ou exécutent à titre professionnel des transactions sur cryptoactifs doivent disposer « *de dispositifs, de systèmes et de procédures efficaces pour prévenir et détecter les abus de marché* » et notifier à leur autorité compétente leurs soupçons. Celle-ci est ensuite chargée d'informer l'autorité de supervision de la plateforme de négociation. Les spécifications de ces dispositifs, systèmes et procédures ainsi que les modalités de coordination des autorités doivent être précisées par des normes techniques de l'AEMF 18 mois après la date d'entrée en vigueur du règlement.

En ce qui concerne la régulation *a posteriori*, l'article 111 du règlement MiCA prévoit que les États membres doivent donner aux autorités compétentes, en droit interne, le pouvoir de prendre des sanctions administratives contre les auteurs des infractions aux dispositions du titre VI. La palette de sanctions administratives prévues par le droit interne des États doit au moins inclure :

- une déclaration publique précisant l'identité de la personne responsable et la nature de l'infraction ;
- une injonction de mettre fin au comportement constituant l'infraction ;
- la restitution du montant des profits issus de l'infraction ;
- le retrait ou la suspension de l'agrément de CASP et l'interdiction pour les responsables de l'infraction d'exercer des fonctions de direction au sein d'un CASP à titre provisoire ou à titre définitif pour une durée pouvant atteindre dix ans ;
- l'interdiction pour les responsables de l'infraction de négocier pour leur compte propre ;
- des amendes administratives pouvant atteindre le plus élevé des niveaux suivants :
  - trois fois le montant des profits obtenus du fait de l'infraction ou des pertes que l'infraction a permis d'éviter,
  - un montant fixe dépendant de l'infraction et du fait que la personne est une personne physique ou morale, compris entre 1 M€ et 15 M€ selon les cas,
  - pour les seules personnes morales, une proportion du chiffre d'affaires comprise entre 2 % et 15 % selon l'infraction.

Les États membres ont la possibilité de prévoir des sanctions administratives plus lourdes.

**Le règlement prévoit uniquement une obligation pour les États membres d'instituer des sanctions administratives.** Les sanctions pénales relèvent de la compétence propre de chaque État membre et ne sont pas obligatoires ; par ailleurs, les États membres peuvent ne pas établir de sanctions administratives si leur droit interne prévoit déjà des sanctions pénales. Dans le cas où le droit interne d'un État membre prévoit à la fois des sanctions pénales et administratives pour ces comportements, il lui appartient de prévoir les modalités d'articulation entre les deux corpus de sanctions dans le respect du principe *non bis in idem*.

En droit interne français, la sanction des abus de marché d'instruments financiers prévus par le règlement (UE) n° 596/2014 sur les abus de marché relève de deux séries de dispositions :

- les sanctions administratives sont prononcées par l'AMF, conformément aux dispositions de l'article L. 621-15 du CMF. Ce texte prévoit, quelle que soit la catégorie de l'infraction, des sanctions pouvant atteindre 100 M€, le décuple de l'avantage retiré de l'infraction et 15 % du chiffre d'affaires annuel, ce qui égale ou excède les montants minimaux de sanctions qu'impose le règlement (UE) n° 596/2014[18] ;
- des sanctions pénales prévues aux articles L. 465-1 à L. 465-3-6 du CMF.

**Compte tenu de la complexité des dispositions définissant les différentes infractions prévues par le règlement (UE) n° 596/2014 et de leur proximité avec les nouvelles infractions que définit le règlement MiCA, la mission recommande d'harmoniser en droit interne les sanctions administratives et pénales visant les auteurs des infractions prévues par ces deux règlements.**

Ainsi, en ce qui concerne les sanctions administratives, l'ajout à l'article L. 621-15 d'une mention des infractions prévues par le règlement MiCA en complément de chacune des deux occurrences du règlement (UE) n° 596/2014 constituerait une adaptation garantissant la cohérence des sanctions tout en respectant les dispositions du règlement MiCA.

En ce qui concerne les sanctions pénales, une adaptation cohérente pourrait consister à :

- étendre la définition de l'« *information privilégiée* » fixée par le C du I de l'article L. 465-1 du CMF en ajoutant une référence à l'article 87 du règlement MiCA ;
- élargir la définition des manipulations de marché interdites aux articles L. 465-3-1 et L. 465-3-2 par une référence aux cryptoactifs au sens du règlement MiCA, en complément des références aux instruments financiers ;
- mentionner les cryptoactifs en sus des instruments financiers au 1° du I de l'article L. 465-3-4 définissant les actifs auxquels la section est applicable.

La notion de comportement légitime prévue au B du I de l'article L. 465-1 devrait en revanche être restreinte de façon à ne couvrir que les opérations impliquant des informations privilégiées portant sur des instruments financiers. En effet, cette notion de comportement légitime est absente de la définition d'opération d'initié dans le règlement MiCA et ne doit pas être étendue aux délits d'initié sur des cryptoactifs. De même, pour le B du I de l'article L. 465-3-1, la notion de « motif légitime » devrait n'être entendue au sens du 9 du 1 du règlement (UE) n° 596/2014 que pour les manipulations concernant des marchés d'instruments financiers et non pour celles concernant des marchés de cryptoactifs.

Si ces choix d'adaptation sont retenus, il n'apparaît pas nécessaire, en revanche, de modifier les autres articles[19] de cette section du code monétaire et financier.

---

[18] L'article 30 du règlement prévoit que les États membres doivent doter leurs autorités administratives compétentes d'un pouvoir de sanction administrative d'au moins un montant maximal de : 500 000 € à 15 M€, ou trois fois le montant de l'avantage retiré de l'infraction, ou 2 à 15 % du chiffre d'affaire annuel, selon la nature de l'infraction et la nature physique ou morale de la personne à l'origine de l'infraction.

[19] En particulier, il n'est pas nécessaire d'étendre aux cryptoactifs l'infraction prévue par l'article L. 465-3-3 puisque la notion de manipulation d'indice n'est pas prévue par le règlement MiCA.

**Le droit interne des États peut prévoir d'autres interdictions à peine de sanctions administratives ou pénales.** Dans le rapport n° 2022-M-062-02 « *Donner un cadre juridique aux jeux à objets numériques échangeables* », la mission préconisait d'interdire aux professionnels du sport de participer à des jeux reposant sur l'utilisation de cryptoactifs et incluant des données issues de compétitions sportives réelles. **Il pourrait, de la même façon, être défendu à ces professionnels de détenir des cryptoactifs dont le cours est susceptible d'être altéré par les résultats de compétitions sportives dans leur discipline.** Une telle interdiction reviendrait, en substance, à présumer de façon irréfragable que les interventions de ces professionnels sur le marché de ces cryptoactifs constituent une opération d'initié.

### 1.4. Le règlement MiCA ne sera rendu pleinement applicable par substitution au régime de la loi PACTE qu'à l'issue d'une période transitoire de 18 mois

L'entrée en vigueur du règlement MiCA est prévue 20 jours après sa publication, qui devrait intervenir à la fin du printemps 2023. Son application interviendra 18 mois après son entrée en vigueur, soit à compter de la fin de l'année civile 2024.

À compter de sa date d'entrée en application, le règlement sera immédiatement applicable :

- aux offres au public de cryptoactifs autres que des EMT et des ART qui prennent fin après l'entrée en application, même si elles ont débuté avant cette date ;
- aux admissions à la négociation demandées à partir de cette date ;
- aux prestations de services sur cryptoactifs qui débuteraient après la date d'entrée en application.

Néanmoins, une période transitoire s'appliquera pour les jetons préexistants et opérations déjà engagées. Ainsi, conformément à l'article 143 du projet de règlement :

- pour les cryptoactifs admis à la négociation avant l'entrée en application du règlement, les exploitants de plateformes de négociation auront l'obligation de veiller à ce qu'un livre blanc soit publié dans les 36 mois, soit avant la fin de l'année 2027 ;
- pour les prestataires de services sur cryptoactifs ayant commencé leur activité avant l'entrée en vigueur du règlement, un délai de 18 mois leur sera accordé pour obtenir un agrément conformément aux dispositions nouvelles. Pendant cette période, les États membres ont la possibilité d'appliquer un régime transitoire par lequel les prestataires qui, à la date d'application du règlement, étaient autorisés[20] au titre de dispositions de leur droit national, peuvent obtenir l'agrément au titre du règlement MiCA selon une procédure simplifiée.

Les articles 8 et 9 de la loi n° 2023-171 du 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 (DDADUE) visent à tirer les conséquences de l'entrée en vigueur imminente du projet de règlement.

[20] En droit français, le seul fait d'avoir été enregistré (et non pas agréé) suffit à bénéficier de la prolongation de période transitoire (*cf.* III de l'article 9 de la loi DDADUE).

Le I de l'article 8 modifie le chapitre du code monétaire et financier relatif aux PSAN afin de créer un régime qualifié d'« **enregistrement renforcé** ». Ce régime impose, entre autres, des obligations supplémentaires par rapport au régime de l'enregistrement simple, qui relevaient auparavant du régime de l'agrément :

- pour l'ensemble des services, **l'obligation de disposer d'un contrôle interne adéquat, d'un système de gestion des conflits d'intérêts et d'un système informatique résilient et sécurisé**. L'Autorité des marchés financiers acquiert par ailleurs la capacité de vérifier la sécurité de ces systèmes d'information ;
- pour le seul service de conservation, l'obligation d'établir une politique de conservation et de ségréguer les détentions.

Ainsi, à compter du 1er janvier 2024 (date d'entrée en vigueur du I de l'article 8 de la loi DDADUE), l'exercice des activités d'un PSAN est soumis de façon obligatoire au régime de l'enregistrement renforcé, l'agrément restant facultatif. Le III de l'article 8 prévoit que les PSAN opérant conformément aux conditions prévues par le droit interne français (c'est-à-dire, exerçant des services non soumis à obligation d'enregistrement, s'étant enregistrés ou ayant obtenu l'agrément facultatif) peuvent poursuivre leurs opérations jusqu'à la fin de la période transitoire prévue par le règlement MiCA, c'est-à-dire jusqu'à mi-2026. À cette date, le chapitre du code monétaire et financier consacré aux PSAN cessera d'être applicable.

Enfin, l'article 9 de la loi DDADUE habilite le Gouvernement à prendre, par voie d'ordonnance, avant le 8 mars 2024, toute mesure pour adapter les dispositions du code monétaire et financier et le cas échéant d'autres codes ou lois pour assurer leur cohérence avec le règlement MiCA à compter de son entrée en application et définir les compétences de l'AMF et de l'ACPR pour l'application du règlement. Cette disposition pourrait être utilisée pour assurer la mise en cohérence proposée par la mission en section 1.3.4.

Compte tenu de l'effet direct du règlement MiCA et de l'ampleur des obligations qu'il fait peser sur les CASP, la mission recommande en outre de modifier l'articulation existant entre le régime applicable aux actifs numériques et celui valable pour les intermédiaires en biens divers : ce dernier devrait ainsi être rendu subsidiaire (et non l'inverse, comme c'est le cas dans le droit actuel).

## 2. Les failles existantes dans le traitement des risques de marché par le règlement MiCA doivent être résolues par l'extension du champ d'application de certaines règles

### 2.1. Le règlement MiCA est centré sur l'encadrement des cryptoactifs à vocation financière

**À l'instar du régime français des PSAN, le règlement MiCA a été conçu dans le but de réguler les cryptoactifs à vocation financière**, soit comme moyens d'échange, soit comme produits d'investissement, soit comme moyen de levée de fonds. Cet objectif explique en particulier :

- l'attention importante portée à la protection de l'épargnant, par le prisme notamment de l'obligation de notifier un livre blanc, ainsi qu'au fonctionnement des marchés d'échange de ces cryptoactifs ;
- l'exclusion des jetons non fongibles du champ d'application du règlement et le petit nombre de règles applicables aux jetons utilitaires fongibles.

### 2.1.1. La version définitive du règlement MiCA exclut les cryptoactifs économiquement non fongibles

**Les cryptoactifs non fongibles sont exclus du champ d'application du règlement, sans que cette notion de fongibilité ou non-fongibilité soit par la suite utilisée dans le corps du règlement en lui-même.**

L'article 2(3) dispose ainsi que « *le présent règlement ne s'applique pas aux cryptoactifs qui sont uniques et non fongibles avec d'autres cryptoactifs* ». En effet, selon le considérant 10, « *s'il est vrai que les cryptoactifs uniques et non fongibles pourraient être négociés sur les marchés et accumulés de manière spéculative, ils ne sont pas aisément interchangeables et la valeur relative d'un tel cryptoactif par rapport à un autre, chacun étant unique, ne peut être déterminée par comparaison avec un marché existant ou un actif équivalent. De telles caractéristiques limitent la mesure dans laquelle ces cryptoactifs peuvent avoir une utilisation financière, ce qui restreint les risques pour les détenteurs et le système financier et justifie leur exclusion du champ d'application* ».

Le considérant 11 restreint en revanche la définition des jetons non fongibles. La non-fongibilité doit s'entendre dans un sens économique et non technique, de façon cohérente avec les risques que vise à prévenir le règlement : « *l'émission de cryptoactifs en tant que jetons non fongibles en grande série ou collection devrait être considérée comme un indicateur de leur fongibilité. La seule attribution d'un identifiant unique à un cryptoactif ne suffit pas en soi pour le classer comme unique et non fongible. Pour que le cryptoactif soit considéré comme unique et non fongible, il convient que les actifs ou les droits représentés soient également uniques et non fongibles. […] Le présent règlement devrait également s'appliquer aux cryptoactifs qui semblent être uniques et non fongibles, mais dont les caractéristiques de fait ou les caractéristiques qui sont liées à leurs utilisations de facto les rendraient soit fongibles, soit non uniques. À cet égard, lorsqu'elles évaluent et classent les cryptoactifs, les autorités compétentes devraient adopter une approche qui privilégie le fond par rapport à la forme, de sorte que les caractéristiques du cryptoactif en question déterminent le classement et non sa désignation par l'émetteur* ». Une telle définition, justifiée pour éviter le contournement des exigences imposées aux cryptoactifs fongibles, supposera des analyses au cas par cas et a pour inconvénient de ne pas donner de critères précis, qui auraient créé des effets de seuil. Un travail d'interprétation devra donc compléter le texte du règlement pour préciser les contours de son champ d'application.

Pour pallier le manque de visibilité quant aux risques et incertitudes qui entourent le développement des marchés de cryptoactifs non fongibles, **l'article 142 du règlement prévoit dans les 18 mois suivant l'entrée en vigueur du règlement (soit à la fin de l'année 2024), la remise par la Commission d'un rapport sur les dernières évolutions intervenues en matière de cryptoactifs accompagné, le cas échéant d'une proposition législative.** Ce rapport doit inclure « *une évaluation de l'évolution des marchés de cryptoactifs uniques et non fongibles et du traitement réglementaire approprié de ces cryptoactifs, y compris une évaluation de la nécessité et de la faisabilité d'une réglementation applicable aux offreurs de cryptoactifs uniques et non fongibles ainsi qu'aux prestataires de services liés à ces cryptoactifs* ».

### 2.1.2. Il existe une incertitude sur l'applicabilité des titres V et VI du règlement aux prestataires de services sur des actifs non fongibles et aux marchés de ces actifs

**Les colégislateurs européens ont exclu les cryptoactifs non fongibles du champ d'application du règlement défini à l'article 2, mais le fait qu'un jeton soit non fongible ne suffit pas à l'exclure de la définition d'un cryptoactif.** En conséquence, l'applicabilité de certaines dispositions faisant référence à la catégorie des cryptoactifs est incertaine. Cette situation diffère par exemple de celle des jetons incessibles, dont le considérant 17 précise explicitement qu'ils « *ne relèvent pas de la définition des cryptoactifs* ».

Le premier projet présenté par la Commission ne prévoyait une exclusion des cryptoactifs non fongibles que pour les dispositions relatives à l'émission et à l'admission à la négociation des jetons (obligation de livre blanc, en particulier). Au cours des phases de trilogue de 2022, la présidence française du Conseil a négocié une rédaction excluant l'applicabilité de l'ensemble du règlement aux cryptoactifs non fongibles, contre l'avis de la Commission, qui défendait une exclusion des seules dispositions consacrées à l'émission des jetons (titres II à IV) et un maintien dans le champ des titres V (CASP) et VI (abus de marché). L'exclusion des jetons non fongibles a cependant été restreinte par l'ajout du considérant 11, prévoyant que la fongibilité s'apprécie sous un angle économique plutôt que technique.

Une lecture possible de ce texte pourrait consister à considérer que l'exclusion prévue par l'article 2 porterait sur les cryptoactifs en eux-mêmes *en tant que produits* et devrait donc être regardée comme s'appliquant aux spécifications des jetons, mais pas aux opérations qui les impliquent. Autrement dit, selon cette lecture, les titres V et VI devraient être applicables respectivement aux CASP manipulant des cryptoactifs non-fongibles et aux abus sur les marchés de cryptoactifs non-fongibles. Néanmoins, la lecture des considérants ne laisse pas d'ambiguïté quant au fait que l'intention du Conseil, lors de l'adoption des dispositions excluant les cryptoactifs non fongibles du texte, était de ne rendre celui-ci applicable *dans son ensemble* qu'aux jetons fongibles à titre transitoire et d'attendre une stabilisation de l'écosystème et de l'économie des jetons non fongibles avant de légiférer[21].

Cette dernière interprétation du texte est cohérente avec les dispositions de l'article 142 du projet de règlement prévoyant que le rapport sur les évolutions récentes en matière de cryptoactifs inclue une évaluation « *de la nécessité et de la faisabilité d'une règlementation applicable aux offreurs de cryptoactifs uniques et non fongibles ainsi qu'aux prestataires de services liés à ces cryptoactifs* », ce qui suggère que les dispositions de MiCA ne constituent pas une telle réglementation. Elle l'est également avec le choix explicite des colégislateurs, sur le règlement relatif aux transferts de fonds et de cryptoactifs (*cf.* section 3.2), d'exclure les transferts de cryptoactifs non-fongibles et donc les prestataires de services sur cryptoactifs non-fongibles.

**C'est donc cette interprétation du texte qui est retenue par la mission pour les besoins du présent rapport.** La mission souligne que la Commission européenne est compétente, sur le fondement de l'article 3(2), pour adopter des actes délégués afin de compléter le règlement en précisant davantage les éléments techniques des définitions. Un tel acte délégué pourrait donc utilement confirmer cette interprétation du texte.

**La question de l'assujettissement au régime des CASP pour prestataires de services impliquant simultanément des jetons fongibles et non fongibles ne laisse en revanche pas place au doute.** Il en va ainsi, par exemple, de l'exploitation de plateformes d'échange entre cryptoactifs non-fongibles et cryptoactifs fongibles. Les définitions figurant à l'article 3 du règlement ne font pas référence, pour définir ces activités, au fait que l'une ou l'autre des branches de l'échange soit fongible. Néanmoins, sur ce point précis, aucune interprétation du texte ne paraît permettre d'exclure les services d'échange d'un cryptoactif fongible (donc couvert par le texte) contre un autre cryptoactif au seul motif que ce dernier n'est pas fongible. Il suit donc, selon la mission, que les prestataires de services d'échange et de négociation de cryptoactifs fongibles contre des cryptoactifs non-fongibles devraient être qualifiés de CASP.

Cette analyse n'implique cependant pas que les principales plateformes « *de pair à pair* » d'échange de NFT, telles qu'*OpenSea*, doivent être assujetties au régime des CASP : en effet, selon la mission, elles ne répondent pas à la définition d'une *plateforme de négociation* au sens du règlement MiCA (*cf.* section 2.3.1 *infra*).

[21] En particulier, lors de cette négociation, le Conseil a rejeté une proposition consistant à n'exclure les jetons non fongibles que des titres II à IV et de les maintenir dans le champ des titres V et VI.

### 2.1.3. Les jetons utilitaires donnant accès à un bien ou un service qui existe ou est opérationnel sont exclus du titre II et certains services associés ne relèvent pas du titre V

**L'article 4(3), consacré aux obligations des personnes offrant au public des cryptoactifs autres que des EMT et ART, exclut du titre II les « *jetons utilitaires donnant accès à un bien ou à un service qui existe ou est opérationnel* »[22].** Pour l'application de ces dispositions, un jeton utilitaire est défini comme « *un type de cryptoactif destiné uniquement à donner accès à un bien ou à un service fourni par son émetteur* ». En conséquence, les émetteurs de ces jetons ne sont soumis ni à l'obligation de notifier un livre blanc, ni aux dispositions relatives aux communications commerciales. Cette exception n'est pas applicable, en revanche, aux cryptoactifs donnant accès à des biens ou des services qui ne sont pas encore existants ni opérationnels.

Une ambiguïté existe quant à l'application du titre II aux jetons utilitaires donnant accès à des biens et services existants qui ont été admis à la négociation. En effet, la rédaction choisie à l'article 4(3) exclut ces jetons de l'ensemble du titre II, mais l'article 4 ne porte que sur les obligations faisant suite à l'offre au public d'un cryptoactif. L'article 5, en revanche, prévoit des obligations comparables de notification d'un livre blanc pour tous les actifs qui sont admis à la négociation, sans faire référence aux clauses dérogatoires de l'article 4(3). En outre, conformément à l'article 4(4), l'exception de l'article 4(3) ne s'applique pas « *lorsque l'offreur […] fait connaître dans toute communication son intention de demander l'admission à la négociation* ». La mission interprète donc l'économie générale des articles 4 et 5 comme signifiant que le titre II redevient applicable aux jetons utilitaires donnant accès à des biens existants ou des services opérationnels dès le moment où ceux-ci sont admis à la négociation.

**Les exclusions de l'article 4(3) emportent des conséquences sur le régime applicable aux prestataires de services sur ces jetons, par dérogation au titre V.** En effet, l'article 4(5) prévoit que « *l'agrément en tant que prestataire de services sur cryptoactifs […] n'est pas requis pour la conservation et l'administration de cryptoactifs pour le compte de clients ou pour la fourniture de services de transfert de cryptoactifs en lien avec des cryptoactifs dont les offres au public sont exemptées en vertu du paragraphe 3* ».

Cette exception n'a qu'une portée limitée puisque seuls sont concernés les services de conservation, d'administration et de transfert de cryptoactifs considérés. L'exception permet en particulier d'assurer que les émetteurs de jetons à vocation commerciale qui ouvrent des portefeuilles pour le compte de leurs clients et permettent à ceux-ci de se les échanger ne sont pas assujettis au régime de CASP. En revanche, elle n'a pas pour objet de dispenser de l'agrément de CASP les prestataires de services d'achat et vente de ces cryptoactifs, ni les plateformes de négociation de cryptoactifs. En outre, elle cesse explicitement d'être applicable si les cryptoactifs considérés sont admis à la négociation.

**Parmi les cas d'usage des actifs numériques listés à l'annexe III du présent rapport, la majorité pourraient relever de l'une ou l'autre des exclusions**.

Le tableau 1 résume le régime applicable aux différentes catégories de jetons à vocation commerciale. La majorité de ces jetons sont soit des jetons non fongibles, soit des jetons utilitaires donnant accès à des biens existants ou des services opérationnels. Cette situation n'est toutefois pas systématique, puisque les jetons « *collectibles* » ne donnant accès à aucun bien ni service et émis en grande série ne relèvent d'aucune des deux catégories.

---

[22] Le même paragraphe applique un régime identique à deux catégories de cryptoactifs qui peuvent avoir une vocation commerciale : les cryptoactifs offerts gratuitement et ceux qui ne peuvent être utilisés « *qu'en échange de biens et de services au sein d'un réseau limité de commerçants ayant conclu des accords contractuels avec l'offreur* », c'est-à-dire les cryptoactifs représentant des points de fidélité. Ce même régime s'applique également aux cryptoactifs automatiquement créés en rémunération de la maintenance du registre, c'est-à-dire aux cryptomonnaies de chaînes telles que le bitcoin et l'éther.

**Tableau 1 : Applicabilité des différents titres du règlement MiCA aux jetons à vocation commerciale et aux services et opérations afférents (JVC)**

| Type de JVC | Titre II applicable à l'émission de ces jetons (livre blanc) | Titre V applicable aux prestataires de services sur ces jetons (agrément CASP) | Titre VI applicable aux transactions sur ces jetons (abus de marché) |
|---|---|---|---|
| JVC non fongibles (définis dans un sens économique) | Non | Non. Les services impliquant à la fois des JVC non fongibles et des JVC fongibles sont cependant soumis au titre V. | Non |
| JVC fongibles, utilitaires donnant accès à un bien existant ou à un service opérationnel (*utility tokens*) | Si et seulement s'ils sont admis à la négociation | Oui, exception faite des services de conservation et d'administration de ces jetons pour le compte de clients et de transfert de cryptoactifs en lien avec ces jetons L'exception ne s'applique pas si les jetons sont admis à la négociation | Si et seulement s'ils sont admis à la négociation |
| Autres JVC relevant des exceptions *de minimis*[23] | Si et seulement s'ils sont admis à la négociation | Oui | Si et seulement s'ils sont admis à la négociation |
| Autres JVC fongibles[24] | Oui | Oui | Si et seulement s'ils sont admis à la négociation |

*Source : Mission, d'après le règlement MiCA adopté le 20 avril 2023.*

*Remarque : Les types de jetons sont classés du régime le plus restrictif au régime le moins restrictif. Le régime le moins restrictif s'applique toujours. Ainsi, un JVC utilitaire non fongible est exclu des titres II, V et VI même s'il est utilitaire ou s'il relève de l'exception* de minimis.

À noter toutefois que compte tenu de la définition qui est donnée d'une plateforme de négociation et d'une admission à la négociation (*cf.* 2.3.1 *infra*), la majorité des JVC ne peuvent en réalité pas être considérés comme admis à la négociation. Très peu d'obligations leurs sont donc applicables au titre du règlement MiCA.

## 2.2. Les risques de marché communs à l'ensemble des cryptoactifs justifient un assujettissement des cryptoactifs à vocation commerciale aux règles de prévention des abus de marché

Le législateur européen a entendu, par le règlement MiCA prévoir un régime distinct pour les cryptoactifs destinés à un usage commercial et ceux qui sont destinés à un usage financier, dans le respect du principe de proportionnalité.

[23] Représentant moins de 1 M€ par an, acquis par moins de 150 personnes ou réservés aux investisseurs qualifiés.

[24] Par exemple, grandes séries de *collectibles* ne donnant accès à aucun droit ou service.

De ce fait, le titre VI du règlement MiCA consacré aux abus de marché est applicable aux échanges portant sur un cryptoactif donné lorsque deux conditions cumulatives sont remplies :

- ce cryptoactif est admis à la négociation ou a fait l'objet d'une demande d'admission à la négociation (*cf.* section 1.3.4) ;
- il est fongible au sens du règlement (*cf.* section 2.1).

Les cryptoactifs non fongibles (qui ont généralement une vocation commerciale) sont entièrement exclus du champ d'application du règlement et les cryptoactifs fongibles utilitaires ne sont assujettis qu'à un nombre limité d'obligations. La protection des consommateurs achetant ces cryptoactifs relève donc d'un régime répressif *a posteriori*, par l'application du droit de la consommation.

La mission estime justifié le choix de ne pas appliquer aux émetteurs de jetons à vocation commerciale, en particulier de jetons non fongibles, les dispositions du titre II conçues pour des jetons à vocation financière. Elle adhère par ailleurs au constat selon lequel une application de l'ensemble des dispositions du titre V aux jetons non fongibles ferait peser des obligations disproportionnées sur les sociétés qui conservent et administrent des jetons pour le compte de leurs clients ou permettent des transferts de ces jetons entre leurs clients.

Toutefois, l'exclusion complète des jetons non fongibles du règlement présente un caractère disproportionné. En particulier, elle fait obstacle à l'application de toute règle relative aux abus de marché ainsi qu'à l'ensemble des dispositions relatives au blanchiment de capitaux et au financement du terrorisme (*cf.* section 3.2 *infra*), alors même que ces risques ne sont pas spécifiques aux jetons fongibles.

**En effet, l'ensemble des échanges de cryptoactifs, indépendamment de leur vocation commerciale ou financière et de leur nature fongible ou non, sont susceptibles de faire l'objet d'abus de marché, ce qui justifie que les interdictions prévues par le titre VI leur soient rendues applicables** et que les opérateurs de plateformes d'échange et de négociation soient soumis à des dispositions spécifiques.

Les risques exposés en section 1.1 s'appliquent aux cryptoactifs du seul fait qu'il existe pour eux un marché, pour plusieurs raisons :

- le seul fait que les transactions soient inscrites sur une *blockchain* suffit à ce que les biens aient un cours, même en l'absence de place de marché centralisée. En effet, pour un bien autre qu'un cryptoactif, l'affichage d'un cours suppose qu'un intermédiaire centralisé soit en mesure de synthétiser les montants des transactions réalisées de pair à pair. Pour un cryptoactif, au contraire, ces informations sont publiées en continu dans le registre, y compris si les échanges sont réalisés de façon décentralisée ;
- les cryptoactifs peuvent être échangés de façon automatisée et quasiment instantanée, à l'instar des instruments financiers, ce qui les différencie des biens physiques ou des services qui relèvent de la consommation ;
- l'utilisation d'une *blockchain* facilite la création de fausses transactions entre des portefeuilles en réalité détenus par une même personne.

**La mission propose donc de réintégrer les jetons non fongibles dans le champ du règlement MiCA**, en supprimant l'article 2(3). La majorité des jetons non fongibles à vocation commerciale, parce qu'ils donnent accès à un bien ou un service, relèveraient alors du champ de l'article 4(3), relatif aux *utility tokens*.

Cependant, certains cryptoactifs à vocation commerciale, notamment non fongibles, ne constituent pas des *utility tokens* ; il s'agit en particulier des jetons de collection (*collectibles*). Pour éviter une application du titre II à ces cryptoactifs, qui serait disproportionnée, le champ de l'article 4(3), qui exclut les jetons concernés des obligations du titre II, devrait être étendu à tous les jetons non fongibles. En complément, les actes d'application du règlement pourraient préciser que la catégorie des *utility tokens* inclut les jetons qui constituent en eux-mêmes un bien de consommation ou de collection.

Les mesures à prendre pour assurer la protection des consommateurs faisant l'acquisition de ces jetons, en l'absence de livre blanc, sont traitées en section 2 de l'annexe IV.

**<u>Proposition n° 4</u> : Lors de la révision prévue du règlement MiCA, étendre son champ d'application aux jetons non fongibles. Appliquer aux jetons non fongibles un régime identique à celui des *utility tokens*[25]. Préciser que la catégorie des *utility tokens* inclut les jetons qui constituent en eux-mêmes un bien ou un service déjà existant ou opérationnel.**

**Encadré 2 : L'exemple de l'application des dispositions du titre VI de MiCA aux cartes Sorare**

L'entreprise française Sorare (*cf.* annexe III) émet des NFT associés à des cartes à jouer et à collectionner, lesquelles représentent des joueurs de football. Le jeu proposé permet des gains (sous forme de cartes et de cryptomonnaie) dépendant de la performance du joueur représenté sur la carte. En conséquence, les flux financiers que génère la détention d'une carte, et donc la valeur de la carte elle-même, dépendent directement des performances réelles des joueurs représentés.

De ce fait, une information précise concernant la performance future du joueur (par exemple, le fait qu'il soit sélectionné pour un match ou qu'il soit blessé) constitue une information privilégiée au sens du titre VI du règlement, y compris si elle émane du joueur ou d'une personne de son entourage, alors même que les joueurs ne sont pas les émetteurs des cartes et ne sont pas nécessairement en relation contractuelle directe avec l'émetteur.

Aussi, l'application du titre VI aux jetons non fongibles aurait, dans le cas des cartes Sorare, les conséquences suivantes :

- la réalisation d'une opération d'initié en utilisant ces informations privilégiées serait interdite. Dans le cas des footballeurs et de leur entourage, en revanche, il n'y aurait pas de présomption du fait qu'ils réalisent l'opération en connaissance de cause puisqu'ils n'obtiennent pas ces informations dans le cadre de fonctions qu'ils exercent auprès de l'entreprise qui les émet. Autrement dit, leur connaissance du caractère privilégié de l'information devrait être démontrée ;
- la divulgation illicite de ces informations serait interdite aux mêmes personnes ;
- en revanche, les obligations relatives à l'obligation de divulguer publiquement les informations privilégiées ne s'appliqueraient qu'à l'émetteur, c'est-à-dire à l'entreprise Sorare lorsqu'elle a connaissance de l'information et que celle-ci n'a pas déjà été rendue publique. Au contraire, les joueurs de football représentés sur ces cartes ne seraient pas soumis à cette obligation.

[25] Pour rappel, les *utility tokens* sont soumis aux dispositions sur le livre blanc (titre II) et les abus de marchés (titre VI) à condition d'être admis à la négociation. Les prestataires de services sur ces jetons doivent par ailleurs obtenir l'agrément CASP (titre V).

## 2.3. Les spécificités liées aux cryptoactifs justifient de prévenir et d'interdire les abus de marché même en l'absence de plateformes de négociation centralisées

### 2.3.1. La définition de la négociation retenue par le règlement rend inapplicables les dispositions relatives aux abus de marché pour les actifs échangés de pair à pair

La négociation de cryptoactifs n'est définie qu'à l'article 3(1)(18), par l'intermédiaire de la définition de l'exploitation d'une plate-forme de négociation de cryptoactifs comme « *la gestion d'un ou de plusieurs systèmes multilatéraux, qui réunissent ou facilitent la* ***rencontre de multiples intérêts acheteurs et vendeurs exprimés par des tiers*** *pour des cryptoactifs,* ***au sein du système et conformément à ses règles****, d'une manière qui aboutit à un contrat,* ***soit par l'échange de cryptoactifs contre des fonds, soit par l'échange de cryptoactifs contre d'autres cryptoactifs*** ». Les définitions de l'échange de cryptoactifs contre des fonds ou contre d'autres cryptoactifs figurent ensuite aux 3(1)(19) et 3(1)(20) : il s'agit de « *la conclusion,* ***avec des clients****, de contrats d'achat ou de vente de cryptoactifs contre des fonds* (resp. d'autres cryptoactifs) *avec utilisation de* ***capitaux détenus en propre*** ».

**Une telle définition fait référence à un type précis d'organisation de négociation : les places de marché centralisées** sur lesquelles sont passés des ordres de transactions entre des biens préalablement confiés à l'opérateur de plateforme, celui-ci étant ensuite chargé de définir les conditions de la rencontre entre les intérêts vendeurs et acheteurs, par exemple par la technique du carnet d'ordres. De telles plateformes sont particulièrement adaptées à l'échange d'actifs financiers et d'actifs assimilés, qui ont tous en commun d'être fongibles.

*A contrario*, cette définition n'inclut manifestement pas les plateformes dites « pair à pair », sur lesquelles les acheteurs et les vendeurs rendent publique leur volonté d'acheter ou de vendre des cryptoactifs et peuvent s'échanger des offres, mais restent responsables en dernier ressort de l'acceptation des transactions. Le rôle de la plateforme, dans ce cas, diffère peu de celui d'un site d'annonces (tel que *Leboncoin*) ou d'enchères (tel qu'*ebay*). Ce type de plateformes est particulièrement adapté aux échanges d'actifs à vocation commerciale, notamment non fongibles. L'exclusion des plateformes de pair à pair est donc liée à la question de l'inclusion ou non des cryptoactifs non fongibles dans le champ du règlement MiCA (*cf*. section 2.2).

L'interprétation qu'ont entendu donner les colégislateurs européens à cette notion de « *négociation* » est également précisée par le considérant 95 du règlement MiCA. Celui-ci précise en effet qu'il serait disproportionné de soumettre les cryptoactifs à l'ensemble des dispositions du règlement (UE) n° 596/2014 relatif aux abus de marché d'instruments financiers. Dans la mesure où les dispositions de ce règlement ne couvrent que les marchés organisés d'instruments financiers, ces dispositions sont cohérentes avec une intention du législateur d'exclure de la définition d'« admission à la négociation » le seul fait qu'un cryptoactif soit proposé sur des plateformes d'échange pair à pair.

**Or, les principaux sites mondiaux de négociation de cryptoactifs non fongibles, en particulier *OpenSea*[26], sont des sites d'échanges de pair à pair ou d'annonces et ne peuvent donc pas être regardés comme des plateformes de négociation de cryptoactifs.**

Il est vrai que ces plateformes pourraient entrer dans la catégorie des CASP au titre d'autres activités qu'elles exercent. *OpenSea*, en particulier, propose l'émission de jetons pour le compte de ses clients. En revanche, cette considération ne suffit pas à ce que le titre VI leur soit applicable.

[26] *OpenSea* propose aux utilisateurs de publier des offres d'achat et de recevoir des offres de vente, mais il appartient à l'utilisateur *in fine* de sélectionner l'offre d'achat la plus avantageuse et de réaliser la transaction, qui intervient directement *on chain* sans qu'*OpenSea* détienne les cryptoactifs.

**Une interrogation peut par ailleurs subsister quant au cas des personnes qui opèrent des *layers 2* et plus spécifiquement des *rollups*,** c'est-à-dire des services au sein desquels sont réalisées des transactions de pair à pair dont l'agrégat est ensuite publié sur la *blockchain* principale. Ces services supposent en effet que les actifs soient séquestrés sur la *blockchain* principale pour être ensuite « déplacés » dans le *rollup*. En revanche, dans le *rollup*, les échanges peuvent n'avoir lieu que de pair à pair. Selon le modèle de *rollup* retenu, les clefs autorisant les transactions peuvent être détenues soit par l'opérateur, soit par l'utilisateur. La qualification de plateforme de négociation pour ces *rollups* et de *cryptoactif admis à la négociation* pour les jetons qui y sont échangés est donc incertaine.

### 2.3.2. Compte tenu des risques d'abus de marché intrinsèques aux cryptoactifs, même en l'absence de plateformes de négociation centralisées, une règlementation doit être mise en place

**En réalité, pour les mêmes raisons que celles qui ont été exposées en section 2.3.1, les risques liés aux marchés et aux plateformes sont constitués, y compris pour les cryptoactifs qui ne sont échangés que de pair à pair, la *blockchain* jouant par elle-même le rôle de place de marché automatisée et quasi-instantanée dont peut être déduit un cours.** Le caractère fongible ou non des jetons est sans conséquence sur ce raisonnement.

En conséquence, l'objectif d'intégrité des marchés justifie que des mesures comparables à celles du titre VI du règlement MiCA s'appliquent aux cryptoactifs qui ne sont pas admis à la négociation. Le régime précis applicable aux actifs qui ne sont négociés que de pair à pair devrait cependant prévoir plusieurs ajustements par rapport à celui qui s'applique aux actifs admis à la négociation sur une plateforme centralisée. En effet, dans le régime prévu par le titre VI, les plateformes de négociation centralisées jouent un rôle dans la prévention des abus, puisqu'il leur appartient de prévoir des procédures permettant de les détecter : un tel rôle ne peut pas nécessairement être joué de la même façon par l'opérateur d'une plateforme de négociation pair à pair.

Des analyses qui précèdent, il ressort, en premier lieu, que les dispositions du titre VI interdisant les abus de marché doivent être applicables à l'ensemble des cryptoactifs, indépendamment du fait qu'ils sont négociés sur une place de marché centralisée ou bien seulement de pair à pair. Cette extension du champ d'application du titre VI permet d'énoncer des interdictions et d'appliquer des sanctions *a posteriori* aux personnes qui se rendent coupables de délits d'initiés et de manipulations de marchés.

**<u>Proposition n° 5</u> : Rendre applicables les interdictions du titre VI du règlement MiCA à l'ensemble des cryptoactifs, indépendamment du fait qu'ils soient ou non admis à la négociation sur une plateforme centralisée.** Pour ce faire, la mention « *admis à la négociation ou ayant fait l'objet d'une demande d'admission à la négociation* » devrait être supprimée à l'article 86(1).

Une fois ces interdictions énoncées, doivent être définies les conditions d'un régime préventif reposant sur les plateformes de négociation et sur l'ensemble des personnes qui facilitent la mise en relation des acteurs souhaitant s'échanger des cryptoactifs (plateformes d'échange pair à pair, d'annonces, *etc.*).

<u>S'agissant des plateformes de négociation centralisées</u>, le régime de prévention des abus de marché découle de leur assujettissement au régime des CASP, conformément aux analyses et propositions précédentes. En effet :

- dès lors que les plateformes permettent l'échange de cryptoactifs fongibles, elles relèvent déjà du périmètre du règlement MiCA (y compris, conformément aux analyses menées en section 2.1.2, si elles permettent l'échange de cryptoactifs fongibles contre des cryptoactifs non fongibles) ;

- si les plateformes ne manipulent pas de cryptoactifs fongibles (par exemple, plateforme permettant l'échange de cryptoactifs non fongibles contre des fonds), l'application de la proposition n° 4 *supra* conduirait à leur appliquer le même régime.

Le régime des CASP leur étant applicable, les plateformes seraient notamment tenues de :

- connaître l'identité de leurs clients ;
- établir des systèmes, procédures et dispositifs permettant de prévenir les abus de marché (art. 76(7)(g)) ;
- notifier à l'autorité compétente les abus et tentatives d'abus de marché commis sur leur système de négociation (art. 76(8)).

Les plateformes qui ne constituent pas des places de marché centralisées mais permettent la mise en relation entre un ou plusieurs offreurs et un ou plusieurs demandeurs (plateformes de négociation pair à pair, d'enchères, d'annonces, *etc.*) ne devraient pas être assujetties à l'ensemble des obligations du régime des CASP. En particulier, ne devraient pas leur être rendues applicables les dispositions relatives à l'obtention d'un agrément préalable à l'opération du service, à la gouvernance interne, au mécanisme de traitement des réclamations ou aux ratios prudentiels. Par ailleurs, il ne devrait pas être requis que ces entités définissent des mesures relatives à la liquidité des actifs ni qu'elles prévoient de coupe-circuits.

En revanche, ces plateformes devraient être soumises au moins aux obligations suivantes :

- une obligation de loyauté, de transparence, de neutralité vis-à-vis de leurs clients et de définition de leurs règles de fonctionnement ;
- une obligation de diligence pour retirer les annonces portant sur des jetons émis sans respecter les règles applicables, notamment ceux qui auraient été émis sans livre blanc lorsque celui-ci est exigible, ou en l'absence des documents contractuels que la mission propose de rendre obligatoires en section 2 de l'annexe IV (proposition n° 1) ;
- des obligations de moyens en matière de vigilance et de signalement des opérations et ordres suspects en matière de LCB-FT et d'abus de marché.

Ces plateformes devraient relever d'un régime de régulation adéquat. Même pour les plateformes opérant sur des jetons à vocation commerciale, la régulation devrait relever à titre principal des régulateurs financiers (Autorité européenne des marchés financiers et son réseau), compte tenu de la nature des risques contrôlés.

**Proposition n° 6 : Astreindre les plateformes de mise en relation des offreurs et acheteurs autres que les CASP à un régime allégé prévoyant des obligations de loyauté, de transparence, de diligence et de vigilance quant aux opérations à risque en matière de LCB-FT et de manipulations de marché.**

L'assujettissement des opérateurs de *layer 2*, en particulier de *rollups*, au régime CASP ou au régime que la mission propose de créer pour les autres plateformes dépendra de leurs caractéristiques techniques. Afin de renforcer la sécurité juridique des prestataires, la mission recommande que l'Autorité européenne des marchés financiers précise la délimitation exacte entre ces deux régimes.

## 2.4. La mission propose d'interdire aux émetteurs de jetons à vocation financière de manipuler les cours par des opérations de rachat et d'imposer des obligations déclaratives aux affiliés réalisant des opérations pour leur propre compte

Dès lors qu'ils disposent d'une grande liquidité même en l'absence de plateforme de négociation centralisée, les cryptoactifs sont particulièrement sensibles aux manipulations de cours (*cf.* 2.2) et aux autres phénomènes de mimétisme financier, comme les bulles. Les jetons à vocation commerciale, dont la valeur est souvent purement ostentatoire (*cf.* annexe III), sont d'autant plus susceptibles de connaître ces variations de cours que leur demande repose parfois sur des effets de mode.

En particulier, il est possible pour un émetteur de jetons de déclencher un mouvement spéculatif haussier en rachetant des jetons, afin de maximiser les recettes issues d'une nouvelle émission imminente. Un tel comportement pourrait être qualifié d'abus de marché sur le fondement de l'article 91(3)(a) du règlement MiCA[27], mais cette qualification supposerait de prouver que l'émetteur s'est assuré, par ses rachats, d'une position dominante et a été en mesure de fixer le prix de vente, ce qu'il est difficile de démontrer. En tout état de cause, l'intervention des émetteurs de cryptoactifs sur les marchés constitue une pratique jugée courante et banale par les interlocuteurs de l'écosystème Web 3.0 rencontrés par la mission.

**La mission propose donc de renforcer cette mesure par une interdiction générale pour les émetteurs de jetons à vocation commerciale de procéder à leur rachat.** Une telle interdiction présenterait l'intérêt de lutter contre une manipulation de marché facile à mettre en œuvre et d'éviter que l'économie de ces cryptoactifs fasse apparaître un trop grand nombre de bulles. Elle serait en outre cohérente avec les préconisations de la mission en matière de « jeux Web 3.0 »[28] qui visent à n'autoriser ces jeux que si l'opérateur n'intervient pas sur le marché pour garantir le cours des objets, autrement dit, s'il ne se porte pas contrepartie de la valeur de ces objets. Elle permettrait enfin d'éviter certains schémas de blanchiment simples reposant sur le rachat de jetons[29].

Cette interdiction serait d'autant plus justifiée qu'en matière de jetons à vocation commerciale, il n'existe pas d'objectif de création de liquidité sur le marché qui rendrait légitime un rachat par l'émetteur.

En revanche, cette règle ne devrait pas empêcher les émetteurs de proposer l'échange des cryptoactifs qu'ils ont émis contre d'autres cryptoactifs dont ils sont également les émetteurs ou émis par des personnes agissant de concert — par exemple, l'échange d'une monnaie de jeu vidéo contre des objets de jeu vidéo du même émetteur. Le rachat en monnaie *fiat*, en cryptomonnaies grand public (bitcoin, éther, *etc.*), ou encore contre d'autres cryptoactifs émis par des tiers, devrait en revanche rester interdit.

---

[27] « *Les comportements suivants sont, entre autres, considérés comme des manipulations de marché : (a) le fait de s'assurer une position dominante sur l'offre ou la demande d'un crypto-actif, avec pour effet, réel ou potentiel, la fixation directe ou indirecte des prix d'achat ou des prix de vente ou la création, réelle ou potentielle, d'autres conditions de transaction inéquitables.* »

[28] Présentées dans le rapport n° 2022-M-062-02 de l'Inspection générale des finances, « Donner un cadre juridique aux jeux à objets numériques échangeables » (janvier 2023).

[29] Un malfaiteur ayant acquis des cryptoactifs de manière illégale pourrait acheter des jetons puis les revendre à leur émetteur pour les blanchir. L'interdiction du rachat ne vise donc pas le blanchiment par l'émetteur mais par ses clients. Un tel montage suppose néanmoins que l'émetteur se porte contrepartie des jetons émis et qu'il en informe ses clients.

Un encadrement ou une interdiction de rachat des jetons à vocation financière par leurs émetteurs peut également être envisagée, notamment par cohérence avec les dispositions applicables au rachat d'instruments financiers par les personnes morales qui les émettent[30]. La mission n'a cependant pas examiné l'opportunité ni la faisabilité d'une telle mesure pour les jetons à vocation financière, qui ne relèvent pas de son champ.

**Proposition n° 7 : Interdire aux émetteurs de jetons à vocation commerciale et à toute personne agissant de concert de procéder au rachat des jetons émis en monnaie *fiat* ou en cryptomonnaie grand public (bitcoin, éther, *etc.*).**

**Par ailleurs, la mission relève que le titre VI du règlement MiCA ne prévoit pas d'obligation pour les personnes affiliées à un émetteur de jetons (actionnaires et personnes chargées de la direction ou de l'administration de l'entreprise émettrice ou de son groupe) de déclarer à l'émetteur et à l'AMF les transactions qu'elles réalisent sur ces jetons pour leur compte propre.** Les obligations prévues en la matière pour les instruments financiers par l'article 19 du règlement (UE) n° 596/2014 sur les abus de marché n'ont pas été répliquées, bien que les risques soient similaires. La mission estime donc souhaitable d'étudier l'opportunité d'appliquer un tel régime aux cryptoactifs, quelle que soit leur vocation.

**Proposition n° 8 : Étudier l'opportunité d'une obligation pour les dirigeants d'entités émettant des jetons de déclarer les opérations qu'ils effectuent pour leur compte propre sur ces jetons.**

## 2.5. En matière de conservation, le critère de la fongibilité devrait être maintenu pour définir l'assujettissement au régime des CASP

La conservation d'actifs fongibles requiert en principe de ségréguer les fonds et de prévoir des obligations prudentielles. Leur fongibilité implique en effet une difficulté à déterminer quels actifs sont conservés pour le compte de tiers et quels actifs sont détenus en propre ainsi qu'à connaître le niveau de liquidité et de solvabilité du prestataire.

En revanche, lorsque les cryptoactifs ne sont pas fongibles, ils peuvent être identifiés et suivis de façon individualisée, ce qui limite les risques précédemment cités. Certes, le conservateur pourrait tenter d'utiliser les actifs des tiers pour une finalité que ceux-ci n'ont pas autorisée. Cette utilisation est toutefois plus facile à retracer. En outre, *a posteriori*, une telle utilisation non autorisée constitue un délit d'abus de confiance et est donc interdite et réprimée.

En tout état de cause, c'est ici le caractère techniquement fongible ou non fongible du jeton qui facilite les abus par le prestataire. Aussi, c'est ce critère qui devrait déterminer l'assujettissement ou non du conservateur au régime des CASP et non la vocation financière ou la fongibilité économique des jetons.

En l'état actuel du règlement MiCA, c'est bien ce critère qui prévaut, quoique la conservation de cryptoactifs utilitaires fongibles n'implique pas un assujettissement au régime de CASP conformément à l'article 4(5). En revanche, la mission a recommandé en proposition n° 4 de réintégrer les cryptoactifs non fongibles au règlement MiCA. **En matière de conservation, le critère de fongibilité, entendu dans un sens technique, doit être maintenu.**

[30] Le rachat par une société cotée de ses propres actions est encadré par l'article 5 du règlement (UE) n°596/2014 sur les abus de marché. En droit français, l'article L. 225-209-2 du code de commerce impose l'autorisation des rachats d'actions par l'assemblée générale et fixe des limites aux programmes de rachats tandis que l'article L. 451-3 du code monétaire et financier impose à la société une obligation de déclaration auprès de l'AMF. Pour plus d'informations, se reporter aux articles 241-1 à 241-7 du règlement général de l'AMF.

## 3. L'impératif de lutte contre le blanchiment de capitaux justifie des obligations contraignantes pour les utilisateurs de cryptoactifs

La lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT) repose principalement sur des séries d'obligations imposées à des *entités assujetties*, identifiées *a priori* comme des points de passage probables de flux financiers illicites et dont la liste en droit interne français figure à l'article L. 561-2 du code monétaire et financier (CMF). Ces entités incluent par exemple les banques, les prestataires de services d'investissement, les personnes se livrant au commerce de métaux précieux ou les opérateurs de jeux d'argent et de hasard.

Les obligations qui leur incombent, harmonisées à l'échelle de l'Union européenne par la directive dite *anti-blanchiment*[31] diffèrent selon la catégorie de personnes ; toutes doivent en particulier faire preuve de vigilance à l'égard des flux financiers, signaler à la cellule de renseignement financier TRACFIN les flux suspects, connaître l'identité de leurs clients (*client due diligence* – CDD, procédures parfois également qualifiées de *know your customer* – KYC) et disposer d'un contrôle interne adéquat. Pour les entités dont l'activité économique est régulée (banques, prestataires de services d'investissement, opérateurs de jeux d'argent et de hasard en particulier) la supervision inclut une vérification de la robustesse des procédures internes de surveillance et d'identification des flux financiers suspects. Les prestataires de services de paiement, enfin, ont l'obligation de collecter des informations sur les personnes réalisant des transferts de fonds (« *travel rule* »).

**Cependant, outre les dispositions applicables à ces entités assujetties, certaines prescriptions ayant pour finalité la lutte contre le blanchiment de capitaux et le financement du terrorisme doivent être respectées par toute personne.** Parmi celles-ci, peuvent être mentionnées :

- l'interdiction pour toute personne d'accepter des règlements en espèces d'un montant supérieur à un seuil de 1 000 € lorsque le débiteur agit pour une finalité professionnelle (*cf.* art. D. 112-3 du CMF) ;
- l'obligation pour toute personne intervenant dans des mouvements de capitaux et soupçonnant qu'ils sont issus de certaines infractions de déclarer leurs soupçons au procureur de la République (art. L. 561-1 du CMF) ;
- l'obligation pour toute personne de pouvoir justifier de ses ressources et de l'origine des biens qu'elle détient, l'impossibilité d'en justifier constituant un délit lorsque la personne est en relation de manière habituelle avec d'autres personnes tirant des profits de la commission de certains crimes ou délits (art. 321-6 du code pénal).

Ces obligations, en ce qui concerne les fonds (monnaie *fiat*), sont issues d'un grand nombre de textes de droit interne et de droit dérivé de l'Union européenne, dont l'harmonisation est en cours.

La présente section étudie les risques de blanchiment liés à la manipulation des cryptoactifs ainsi que la façon dont des mesures similaires à celles précédemment exposées, qui ont cours pour les transferts de fonds, pourraient être étendues

[31] Directive (UE) 2015/849 du Parlement Européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme (directive dite « AML4 »), modifiée notamment par la directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 (directive « AML5 »).

## 3.1. L'enjeu du blanchiment de capitaux, consubstantiel à l'usage des *blockchains*, est aggravé par leur utilisation commerciale, laquelle permet aux utilisateurs de ne jamais sortir du Web 3.0

### 3.1.1. Contrairement à ce que peut laisser présumer le caractère transparent de la plupart des *blockchains*, celles-ci présentent des potentialités importantes de blanchiment en l'absence de possibilité d'identifier les utilisateurs

**Dans leur principe même, les *blockchains* publiques, parce qu'elles sont des registres ouverts, paraissent à première vue n'être qu'une source limitée de risques de blanchiment** ou plus généralement de fraude financière.

En effet, sur la plupart des *blockchains* grand public telles que *Bitcoin* ou *Ethereum*, les transactions correspondent à des écrits publics dont toute personne est en mesure de constater l'origine, la destination et le volume, étant précisé que l'origine et la destination des transactions sont des adresses publiques d'individus. Ainsi, lorsqu'une transaction est identifiée comme frauduleuse (par exemple une escroquerie par rançongiciel – *ransomware*) ou douteuse, les fonds qui en sont issus peuvent être suivis[32]. À l'inverse, l'origine de fonds obtenus sur la *blockchain* peut toujours être suivie, c'est-à-dire que les identifiants des comptes d'où proviennent les fonds peuvent être connus.

**Toutefois, la connaissance de l'adresse publique de l'origine ou de la destination des fonds ne permet pas de déterminer la personne morale ou physique correspondante.** Cette difficulte est liee au fait que toute personne peut creer une paire de clefs pour disposer d'un compte sur une *blockchain* publique, sans avoir besoin de justifier son identite (*cf.* annexe I). Un utilisateur peut egalement disposer simultanement de plusieurs « comptes », sans qu'un lien puisse nécessairement être établi entre eux. En outre, des mécanismes de partage de comptes peuvent etre mis en place. Enfin, les donnees des connexions etablies entre les utilisateurs du reseau et les nœuds chargés de la validation des transactions ne sont pas inscrites publiquement sur le registre ni ne sont, en principe, conservees ; elles peuvent en outre facilement etre rendues intraçables par les utilisateurs souhaitant se dissimuler[33]. **Les *blockchains* grand public telles que *Bitcoin* ou *Ethereum* peuvent donc être comparées à des banques opérant des comptes à numéros.**

---

[32] C'est l'objet du projet *Colored Coins* initié en 2012 : celui-ci consiste à marquer certaines transactions comme étant illicites ou frauduleuses puis suivre les bitcoins ayant été manipulés au cours de ces transactions. L'idée sous-jacente est que les bitcoins issus de ces transactions frauduleuses, étant identifiés comme tels, pourraient être refusés par certains acteurs (par exemple les États) et avoir en conséquence une valeur moindre, rendant les fraudes moins profitables.

[33] Pour passer un ordre de transaction sur la *blockchain*, un utilisateur doit se connecter par internet aux validateurs (mineurs ou *stakers*) du réseau et leur envoyer l'ordre. Cette connexion le force à révéler certaines données de connexion, en particulier son *adresse IP*, qui est un identifiant attribué par son fournisseur d'accès à internet (FAI). La connaissance de l'adresse IP permet dans certains cas aux services d'enquête, après interrogation du FAI compétent, d'identifier une personne physique à l'origine d'une opération illicite : c'est notamment sur ce principe que repose la lutte par l'autorité de régulation de la communication audiovisuelle et numérique (ARCOM, ex-HADOPI) contre le partage pair à pair d'œuvres contrefaites. Toutefois, cette méthode n'est efficace qu'à condition 1° que l'adresse IP puisse être identifiée (l'ARCOM doit ainsi opérer une surveillance permanente des flux de données pouvant correspondre à des partages d'œuvres contrefaites) et 2° que l'utilisateur n'utilise pas une technique de dissimulation de son adresse. De telles techniques peuvent être complexes à mettre en œuvre par le grand public, mais sont accessibles à toute personne souhaitant réaliser des activités criminelles.

Afin d'identifier les personnes à l'origine des transactions, les services d'enquête peuvent se reposer sur deux méthodes :

- d'une part, ils peuvent accéder aux données relatives aux clients collectées par certains opérateurs et certaines plateformes *via* leur *customer due diligence* ;
- d'autre part, des enquêtes approfondies et individualisées peuvent permettre d'acquérir un faisceau d'indices identifiant l'individu qui utilise une adresse publique donnée.

Compte tenu du caractère aléatoire et coûteux en ressources humaines de cette dernière méthode, les moyens de lutte contre le blanchiment reposent principalement sur l'obligation de CDD imposée aux acteurs permettant d'entrer ou de sortir de l'écosystème *crypto*.

Afin de sécuriser entièrement les chaînes de paiement et d'assurer l'identification des utilisateurs des *blockchains* à l'origine de transactions suspectes, il est essentiel que la CDD soit assurée par l'un ou l'autre des acteurs suivants :

- ou bien les personnes qui permettent **l'entrée et la sortie d'argent de l'environnement *blockchain***. Il s'agit à titre principal des **plateformes d'échange de cryptoactifs contre de la monnaie *fiat*** (euros, dollars). Cependant, toute personne acceptant l'échange de cryptoactifs (par exemple, un professionnel acceptant d'être rémunéré en bitcoins pour des services fournis dans le monde réel) constitue un point potentiel d'entrée ou de sortie ;
- ou bien, si elle existe, la personne qui **crée un compte permettant de manipuler les cryptoactifs**. Cette personne est le plus souvent une plateforme d'échange de cryptoactifs (*exchange*) qui, dans le cadre de son activité, propose à l'utilisateur de détenir ses cryptoactifs pour son compte ou de lui créer une paire de clefs. Dans ce cas, le compte est dit *hébergé* (*hosted wallet*) et l'hébergeur a la possibilité d'assurer la CDD. **En revanche, de nombreux comptes utilisés sur les *blockchains* sont autohébergés (*self-hosted*)** : pour ceux-ci, aucune personne n'est désignée responsable de la CDD.

Compte tenu de ce qui précède, les principaux risques associés au blanchiment surviennent lorsque **une personne accepte d'échanger des cryptoactifs avec un portefeuille autohébergé** : si le paiement représente un montant élevé, alors le flux qu'elle reçoit doit être considéré comme suspect et il est souhaitable qu'elle assure la CDD (par exemple en exigeant une pièce d'identité du client et en la consignant) ou qu'elle refuse l'utilisation des cryptoactifs comme moyen de paiement pour privilégier des services bancaires de paiement, opérés par des acteurs centralisés qui assurent la lutte anti-blanchiment.

Si ces conditions parviennent à être assurées, alors les services d'enquête disposent d'un moyen garanti d'identifier les *individus* tentant de sortir du système avec des capitaux illicites ou suspects. En revanche :

- des technologies d'anonymisation peuvent empêcher cette identification ainsi que le suivi des flux ;
- une fois les crypto-actifs sortis de ce système régulé dans lequel les détenteurs des comptes sont connus, les personnes à l'origine des flux ne peuvent plus être identifiées.

### 3.1.2. Certaines technologies d'anonymisation rendent quasiment impossible toute reconstitution des flux financiers et sont sources de risques comparables à ceux des transactions anonymes en espèces

Les conclusions des développements réalisés en section 3.1.1 ne trouvent à s'appliquer que lorsque les *blockchains* retracent publiquement les transactions réalisées et identifient les comptes pseudonymes qui les opèrent, comme c'est le cas pour *Bitcoin* et *Ethereum*.

Cependant, diverses technologies ont pour objet d'empêcher le suivi des flux de transactions et favorisent de ce fait le blanchiment de capitaux ou le financement du terrorisme.

**En premier lieu, les mixeurs (*mixers*) sont des services qui permettent de mêler les flux de cryptoactifs fongibles, *via* un intermédiaire centralisé.** Les personnes détenant les fonds peuvent, plutôt que de les envoyer directement à leur destinataire réel, les transmettre au compte *on chain* du mixeur et communiquer *off chain* à celui-ci l'adresse du destinataire réel. Le mixeur envoie ensuite les fonds (diminués de frais de transaction) au destinataire réel. Aussi, sur la *blockchain*, les deux flux (de l'émetteur au mixeur et du mixeur au destinataire) apparaissent mais sont impossibles à relier[34]. Seule la saisie des données du mixeur conservées *off chain* — à supposer qu'elles n'aient pas été détruites — peut permettre aux services d'enquête de reconstituer les flux financiers.

**En deuxième lieu, certaines *blockchains* et certains jetons comportent des fonctions d'anonymisation intégrées (*privacy coins*).** Les principaux *privacy coins* en usage sont les cryptomonnaies *Monero* et *Zcash*, qui s'exécutent sur les *blockchains* du même nom et existent depuis respectivement 2014 et 2016. Leur fonctionnement repose, intuitivement, sur l'idée d'une création de comptes à usage unique à chaque transaction : les flux peuvent donc être suivis, mais il est impossible de savoir que deux transactions ont pour destinataire la même personne. En utilisant de plus un système de signatures partagées (« *ring signature* »[35]), il est possible de faire en sorte que chaque transaction ait non pas un émetteur certain, mais plusieurs émetteurs équiprobables — potentiellement plusieurs milliers.

Il s'ensuit que les transactions deviennent réellement anonymes : un observateur extérieur ne peut ni retracer l'origine d'un flux financier, ni connaître la balance d'une personne, ni savoir ce que sont devenues les sommes qui figuraient sur un compte provisoire. Même un remboursement intégral d'un flux de crypto-actifs ne peut pas être rapproché avec certitude du flux original. **Ces *privacy coins* assurent donc un niveau d'anonymisation similaire à de l'argent liquide, tout en étant entièrement dématérialisés.**

**En troisième lieu, des technologies de « seconde couche » (*layer 2*) peuvent permettre d'anonymiser une cryptomonnaie qui n'est pas par conception anonyme (*cf.* section 4.1.3.2 de l'annexe I).**

**C'est en particulier le cas du *Lightning Network*.** Cette technologie, décrite de façon détaillée dans l'encadré 7 de l'annexe I, repose sur la création d'un réseau de canaux d'échange bilatéraux : deux utilisateurs peuvent mettre sous séquestre une somme d'argent, puis effectuer des échanges privés qui ne sont pas inscrits sur la *blockchain* et, au moment où ils le souhaitent, retranscrire publiquement l'agrégation de leurs transactions. En interconnectant les canaux, les utilisateurs peuvent servir d'intermédiaires à des transactions dont ils ne connaissent ni l'origine, ni la destination. Là aussi, les transactions présentent un niveau d'anonymat similaire à l'argent liquide : l'information des montants que les utilisateurs placent dans le *Lightning Network* et celle qu'ils en ressortent est publique, à l'instar des retraits et dépôts d'argent liquide depuis et vers le système bancaire, mais les transactions du réseau sont ensuite intraçables. Le caractère décentralisé du *Lightning Network* rend impossible de suivre les flux de transactions : seuls les donneurs d'ordre les connaissent.

[34] Sous réserve que quelques précautions soient prises : par exemple, le montant des frais de transaction doit inclure une part variable aléatoire ; de même, le délai entre les flux doit également être aléatoire.

[35] Système de signature électronique dans lequel plusieurs signataires peuvent être à l'origine de la signature, sans pour autant partager la clef, et ne peuvent pas être discernés par un tiers.

**Il en va de même des *rollups***, c'est-à-dire des systèmes dans lesquels des transactions sont effectuées entre de multiples utilisateurs sur un système *off chain* (par exemple sur une *blockchain* privée) piloté par un centralisateur, qui publie par la suite une transaction agrégée sur la *blockchain* principale. Les *rollups* peuvent alors avoir certains effets comparables à ceux des mixeurs, puisque les flux ne peuvent pas être reconstitués. En revanche, le centralisateur ou l'opérateur du *rollup* constitue un intermédiaire centralisé qui pourrait être assujetti à des obligations de conservation des historiques des transactions non rendues publiques et de coopération avec les services d'enquête (*cf.* section 2.3.2, en particulier propositions n° 5 et 6 *supra*).

Chacun de ces services peut être utilisé, de bonne foi, dans le but de protéger la vie privée de l'utilisateur qui utilise des services décentralisés (*cf.* section 4.1 *infra*). En revanche, tous ont pour effet de briser la traçabilité des flux pour les services d'enquêteurs. **La seule possibilité de suivi des flux consiste alors à obtenir cette information du dernier individu identifié dans la chaîne des transactions frauduleuses**, étant précisé que l'individu incapable de justifier de ses ressources et étant en relation habituelle avec des personnes tirant un avantage de la réalisation de crimes ou de délits commet de ce seul fait un délit puni de trois ans d'emprisonnement et 75 000 € d'amende (article 321-6 du code pénal).

Ces trois technologies représentent donc des risques majeurs en termes de blanchiment. Ces risques justifient d'empêcher la sortie des flux depuis le système régulé (*blockchains* pseudonymes) vers ces technologies, sauf à ce que les personnes qui les opèrent soient en mesure d'identifier les individus et de retracer les flux à la demande des autorités.

### 3.1.3. L'utilisation commerciale des cryptoactifs est directement liée au développement des *layers 2* et permet aux criminels de ne pas sortir leurs actifs de l'environnement *crypto*, compliquant encore la lutte contre les infractions

L'utilisation commerciale des cryptoactifs est à l'origine de deux nouvelles sources de difficultés en matière de lutte anti-blanchiment.

**En premier lieu, l'utilisation des cryptoactifs par le grand public est directement liée au développement des technologies de seconde couche (*layers 2*).** La diffusion auprès du grand public des technologies *blockchains* implique en effet un accroissement du volume de transactions, que les *blockchains* de premier niveau (*layers 1*) ne sont généralement pas en mesure de supporter. Or, alors que les *blockchains* de premier niveau constituent des registres ouverts, cette propriété est rarement assurée par les secondes couches. En ce qui concerne les cryptoactifs destinés à la consommation, et notamment les NFT, l'usage de telles secondes couches est fréquent dans les projets étudiés par la mission (*cf.* annexe III). Par exemple, en ce qui concerne spécifiquement les jeux vidéo contenant des objets numériques échangeables[36], certaines entreprises éditrices utilisent les secondes couches *ImmutableX* et *Starkware*, qui relèvent de la catégorie des *rollups*.

**En second lieu, le développement des cryptoactifs comme biens de consommation grand public permet en principe de ne pas sortir les capitaux issus d'opérations illicites de l'environnement *blockchain*.** Une personne tirant des revenus d'opérations criminelles *via* une *blockchain* peut en effet utiliser, au moins partiellement, le produit des opérations frauduleuses en acquérant sur cette *blockchain* des cryptoactifs de consommation (objets de jeu vidéo, biens de consommation ostentatoires, « NFT artistiques », *etc.*) et ainsi éviter tout passage par une plateforme réglementée d'échanges de cryptoactifs contre de la monnaie *fiat*.

[36] Tels que *Sorare*, *Metafight*, *Gods Unchained*, *etc.*

## 3.2. Le paquet législatif européen relatif à la lutte contre le blanchiment en cours d'examen impose des obligations aux CASP mais ne porte pas sur les transactions entre portefeuilles autohébergés

**Le règlement MiCA ne traite pas directement de lutte contre le blanchiment de capitaux, à deux exceptions près :**

- **les CASP doivent mettre en œuvre des procédures de contrôle interne** permettant de « *détecter, d'évaluer et de gérer les risques, notamment en matière de blanchiment de capitaux et de financement du terrorisme* » (titre V, article 62) ;
- **l'article 76(3) interdit aux plateformes de négociation de cryptoactifs d'admettre les jetons comportant des fonctions d'anonymisation intégrées** (*privacy coin*), à moins que les détenteurs de ces cryptoactifs et leur historique de transactions ne puissent être identifiés par les CASP qui exploitent la plateforme.

La réglementation en matière de LCB-FT appliquée aux cryptoactifs passe donc par d'autres textes. **Le 20 juillet 2021, la Commission européenne a soumis un ensemble de quatre propositions législatives (« *paquet* ») relatives à la LCB-FT**[37]. L'un des objectifs de ces propositions est de veiller à une meilleure prise en compte des enjeux liés à l'utilisation de cryptoactifs dans les opérations de blanchiment. À la date de rédaction du présent rapport, l'examen des propositions de textes par le Parlement européen est en cours.

### 3.2.1. Le règlement unique sur la prévention du blanchiment (AMLR) sera rendu applicable aux CASP et le règlement sur les transferts (« *travel rule* ») sera étendu aux transferts de cryptoactifs

**En premier lieu, le projet de règlement unique relatif à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux (*anti-money laundering regulation* – AMLR)**[38] **fait entrer les CASP parmi les entités assujetties** (art. 3(3)(g) du projet de règlement, s'inspirant des dispositions du régime français institué par la loi PACTE[39]). En revanche, sans attendre l'entrée en vigueur de ces règlements, les États membres ont la possibilité de prévoir pour les CASP établis sur leur territoire des obligations au titre de la LCB-FT : ainsi, en France, le régime des PSAN préexistant à MiCA prévoyait déjà leur classification parmi les entités assujetties, en droit interne (*cf.* 1.2.2).

Cet assujettissement aux dispositions de l'AMLR implique en particulier une obligation pour les CASP de faire preuve de vigilance à l'égard de leur clientèle et des flux financiers et de signaler à la cellule de renseignement financier les flux suspects. L'adéquation de leur dispositif de contrôle interne au risque de blanchiment est surveillée par le régulateur sectoriel (en France, l'AMF et l'ACPR).

---

[37] Les principales dispositions de droit dérivé relatives à la LCB-FT figurent dans la directive (UE) 2015/849 dite « quatrième directive anti-blanchiment » (AMLD4), modifiée par une « cinquième directive anti-blanchiment ». Le paquet contient quatre textes : un règlement se substituant à l'AMLD4 (dit « règlement unique » ou AMLR), une « sixième directive » (AMLD6) pour les dispositions nouvelles requérant une transposition, un règlement instituant une agence européenne de lutte anti-blanchiment et un règlement relatif aux informations accompagnant les transferts de fonds et de cryptoactifs (« *transfer of funds regulation* », TFR, aussi appelé « *travel rule* »).

[38] Projet déposé le 20 juillet 2021, document n° 2021/0239(COD).

[39] Le régime de la loi PACTE assujettit aux obligations en matière de LCB-FT les PSAN soumis à enregistrement obligatoire, les PSAN agréés et les émetteurs de jetons ayant sollicité le visa de l'AMF (7° bis à 7° quater de l'article L. 561-2 du CMF). L'AMLR assujettit quant à lui l'ensemble des CASP, mais non les émetteurs de jetons.

**En second lieu, la proposition de règlement relatif aux informations accompagnant les transferts de fonds et de certains cryptoactifs étend la « *travel rule* », c'est-à-dire l'obligation pour les prestataires de services de paiement de collecter certaines informations sur les paiements qu'ils réalisent, aux transferts de cryptoactifs.**

Le projet, tel qu'adopté par le Parlement européen le 20 avril 2023[40], refond le précédent règlement (UE) 2015/847 relatif aux transferts de fonds et comporte, en complément des dispositions relatives à ces mouvements, un chapitre III portant sur les transferts de cryptoactifs. Il tire, en cela, les conséquences des recommandations émises par le groupe d'action financière (GAFI) en matière de transfert d'actifs virtuels. Le considérant 30 du projet précise que compte tenu des caractéristiques des transferts de cryptoactifs, ceux-ci « *devraient être soumis aux mêmes exigences* » que les transferts de fonds.

**Lorsque des personnes effectuent des transferts de cryptoactifs entre des portefeuilles hébergés par des CASP, le texte fait peser une obligation sur ceux-ci d'échanger entre eux certaines informations qu'ils détiennent sur leurs clients et de les conserver** : nom, adresse publique, adresse de résidence physique, identifiant d'entité juridique pour les personnes morales. Il appartient en principe au CASP de l'initiateur de la transaction de veiller à ce que la transaction soit accompagnée de l'échange d'informations requis (art. 14(1) et 14(2)) et au CASP du bénéficiaire de vérifier l'exhaustivité des informations. Dans la mesure où les CASP ont l'obligation, conformément à l'AMLR, de vérifier l'identité de leurs clients (*cf.* 3.2.1), cette disposition permet de garantir que les flux entre CASP sont entièrement tracés. Chacun des CASP est soumis à une obligation de vigilance ; le CASP du destinataire a l'obligation de rejeter, renvoyer ou suspendre les transferts pour lesquels des informations sont manquantes ou inexactes (art. 17).

**Dans le cas où seul le portefeuille émetteur ou seul le portefeuille destinataire de la transaction est hébergé par un CASP, il appartient au CASP de recueillir les informations requises sur son client ainsi que sur la personne détenant le portefeuille autohébergé** (art. 14(5) et 16(2)).

Le CASP doit, en cas d'informations insuffisantes, rejeter la transaction. En revanche, ainsi que le précise explicitement le considérant 39 du règlement, **il n'est pas tenu de *vérifier* les informations concernant la personne qui détient le portefeuille autohébergé**, avec laquelle il n'entretient pas de relations contractuelles. La seule obligation de vérification concerne le cas où le client du CASP déclare que le portefeuille autohébergé lui appartient également[41], si le flux de cryptoactif représente plus de 1 000 € : dans ce seul cas, le CASP est tenu de s'assurer que le portefeuille autohébergé est effectivement contrôlé par son client.

**Enfin, aucune règle n'est applicable aux transactions survenant entre des portefeuilles autohébergés.**

[40] Position du Parlement européen n° P9_TC1-COD(2021)0241 (https://www.europarl.europa.eu/doceo/document/TA-9-2023-0118_FR.html, consulté le 12 mai 2023).

[41] C'est-à-dire, au cas dans lequel le client déplace ses cryptoactifs entre deux portefeuilles qui lui appartiennent, l'un hébergé par un CASP et l'autre autohébergé.

### 3.2.2. Ces dispositions créent au sein de l'écosystème *blockchain* un environnement régulé, dans lequel subsistent d'importantes failles

**L'effet cumulé de ces trois séries de dispositions est de créer, au sein de l'environnement des cryptoactifs, un secteur réglementé de portefeuilles hébergés par des CASP dans lequel les transactions sont traçables et les individus qui les réalisent, nominativement identifiés.** Cet environnement se distingue du secteur non régulé où les portefeuilles ne sont pas hébergés par un CASP (portefeuilles autohébergés). L'entrée de fonds dans l'environnement régulé depuis des portefeuilles autohébergés et la sortie de fonds depuis l'environnement régulé vers des portefeuilles autohébergés devraient en principe, en application de la « *travel rule* », être accompagnées d'une déclaration de l'identité du détenteur du portefeuille autohébergé, laquelle peut être mobilisée lors d'enquêtes ultérieures. Par ailleurs, la conversion des cryptoactifs en monnaie ayant cours légal suppose en principe de recourir aux services d'un CASP, ce qui constitue un facteur important d'attraction des utilisateurs vers le secteur régulé.

**En revanche, les frontières de cet environnement régulé ne sont pas étanches.** Il est donc possible de faire entrer et sortir des montants potentiellement élevés de cryptoactifs. Certes, ces mouvements peuvent être détectés et considérés comme suspects, voire le cas échéant bloqués ; en revanche, une fois les cryptoactifs sortis de l'environnement régulé, les flux ne peuvent plus être tracés. Par ailleurs, rien n'oblige un professionnel à utiliser un portefeuille hébergé par un CASP : si l'utilisation de cryptoactifs comme moyen de règlement dans la vie courante se développait, des cryptoactifs d'origine illicite pourraient être utilisés directement auprès de commerçants, sans que la transaction donne lieu à l'application de la *travel rule*.

Pour cette raison, lors de l'examen de la proposition de règlement sur les transferts de fonds et les transferts de cryptoactifs, les députés européens Paul Tang et Aurore Lalucq (groupe *socialistes et démocrates*) ont déposé des amendements visant à interdire aux CASP le transfert de cryptoactifs vers des portefeuilles autohébergés[42]. Ces amendements n'ont toutefois pas été adoptés.

**En outre, l'assujettissement à la *travel rule* des transactions survenant sur le *Lightning Network* est incertain en l'état actuel du texte.** Le règlement sur les transferts est en effet applicable aux transferts de cryptoactifs, entendus par l'article 3(10) comme les transactions « *visant à déplacer des cryptoactifs d'une adresse de registre distribué, d'un compte de cryptoactifs ou d'un autre dispositif permettant le stockage de cryptoactifs vers une ou un autre* [adresse ou compte]». Or, dans le cas du *Lightning Network*, les déplacements de cryptoactifs n'ont lieu qu'au moment de la fermeture du canal entre deux nœuds directement reliés. Une interprétation restrictive pourrait donc conduire à considérer que seuls les transferts agrégés survenant à la fermeture du canal sont assujettis à la *travel rule*, et non les transactions réelles, passées *off chain*.

[42] Amendements n° 131 et n° 303 (https://www.europarl.europa.eu/doceo/document/CJ12-AM-719852_FR.pdf, consulté le 24 avril 2023).

**Par ailleurs, les cryptoactifs non fongibles sont aujourd'hui exclus des dispositions prévues par le législateur européen en matière de lutte anti-blanchiment**. En effet :

- les prestataires de services sur ces cryptoactifs non-fongibles ne constituent pas des CASP au sens du règlement MiCA et ne seront donc pas des entités assujetties au règlement unique sur la lutte anti-blanchiment. Les députés européens Kira Marie Peter-Hansen, Ernest Urtasun, Aurore Lalucq et Csaba Molnár ont déposé lors de l'examen du projet de règlement un amendement visant à assujettir les plateformes autres que les CASP qui opèrent sur des « *cryptoactifs uniques et non fongibles qui représentent la propriété d'un actif numérique ou physique unique, y compris des œuvres d'art, biens immobiliers, objets de collections numériques et articles de jeu et tout autre objet de valeur* ». Cet amendement a été rejeté au cours de l'examen du texte en commission[43] ;
- en ce qui concerne les obligations relatives aux transferts, le texte même du projet de règlement sur les transferts tel qu'adopté par le Parlement européen le 20 avril 2023 exclut explicitement les cryptoactifs non-fongibles**.** Le projet de règlement, dans ses définitions (art. 3(14)), se réfère aux cryptoactifs comme définis par le règlement MiCA « *sauf s'il[s] relève[nt] de la catégorie énumérée à l'article 2, paragraphe 3* » de ce règlement, c'est-à-dire s'ils sont non fongibles. Le considérant 24 du projet précise explicitement que les cryptoactifs uniques et non fongibles sont exclus.

L'application de ces dispositions aux jetons fongibles utilitaires est par ailleurs partielle. En principe, le texte adopté par le Parlement européen rend la *travel rule* applicable aux transferts de jetons fongibles utilitaires (les exceptions de l'article 4(3) du règlement MiCA ne sont pas visées, *cf.* 2.1.3) ; cependant, certains prestataires de services impliquant ces jetons ne sont pas assujettis au régime des CASP (services exclus en vertu de l'article 4(5), *cf.* tableau 1 de la section 2.1.3, et plateformes d'échange pair à pair, *cf.* section 2.3.1).

**Certes, il existe aujourd'hui des outils pouvant être mobilisés par la cellule de renseignement financier, notamment pour lutter contre les outils permettant le brouillage de transactions (*layer 2* et mixeurs en particulier, *cf.* encadré 3).** Néanmoins, ceux-ci sont souvent complexes à mettre en œuvre et supposent d'obtenir *a posteriori* des informations de la part de la dernière personne identifiée nominativement dans le secteur régulé, qui de plus peut ignorer que les cryptoactifs qu'elle reçoit sont issus d'activités illicites.

[43] Amendement n° 353 (https://www.europarl.europa.eu/doceo/document/CJ12-AM-734116_FR.pdf, consulté le 25 avril 2023).

**Encadré 3 : Moyens de lutte, à droit constant, contre les outils permettant le brouillage de transactions**

Le droit positif comporte plusieurs outils qui pourraient être mobilisés pour lutter contre les services permettant le brouillage de transactions, en particulier les mixeurs et le *Lightning Network*.

Le délit de blanchiment, prévu aux articles 324-1 et 324-1-1 du code pénal, pourrait en principe être mobilisé pour poursuivre les intermédiaires opérant des services de mixage ainsi que potentiellement certains fournisseurs de liquidité du *Lightning Network* non coopératifs. L'article 324-1 du code pénal punit en effet de cinq ans d'emprisonnement et de 375 000 € d'amende le fait de « *faciliter, par tout moyen, la justification mensongère de l'origine des biens ou des revenus de l'auteur d'un crime ou d'un délit ayant procuré à celui-ci un profit direct ou indirect* » ou « *d'apporter un concours à une opération de placement, de dissimulation ou de conversion du produit direct ou indirect d'un crime ou d'un délit* ». L'article 324-1-1 précise par ailleurs que « *les biens ou les revenus sont présumés être le produit direct ou indirect d'un crime ou d'un délit dès lors que les conditions […] financières de l'opération de placement, de dissimulation ou de conversion ne peuvent avoir d'autre justification que de dissimuler l'origine ou le bénéficiaire effectif de ces biens ou revenus* ».

Ces dispositions pourraient permettre aux autorités de cibler les mixeurs, puisqu'il s'agit de personnes qui acceptent de collecter des flux financiers et de les redistribuer dans le but d'en faciliter la dissimulation. En ce qui concerne le *Lightning Network*, elles pourraient aider à cibler les nœuds fournissant des liquidités : ceux-ci acceptent en effet d'entrer dans une relation financière avec un tiers, souvent inconnu, pour exécuter des transactions sans en connaître l'origine ni la destination.

**Enfin, les entités opérant des services de mixage ou fournissant de la liquidité sur le *Lightning Network* contre rémunération constitueront vraisemblablement des CASP**, puisqu'elles opèrent, par conception, uniquement des services sur des actifs fongibles et exécutent des ordres sur cryptoactifs pour le compte de leurs clients. Si une telle qualification était retenue, ces entités devraient prouver au régulateur qu'elles sont en mesure de respecter leurs obligations au titre de la LCB-FT une fois l'AMLR entré en vigueur, à peine d'interdiction.

Ces différentes mesures rendent en principe possible de bannir les nœuds du *Lightning Network* et les services de mixage ne respectant pas leurs obligations au titre de la LCB-FT et d'engager des poursuites à leur encontre.

## 3.3. La mission propose en conséquence de renforcer le suivi des flux par les autorités en étendant le champ de l'obligation de vérifier l'identité des utilisateurs

**Plusieurs propositions précédentes de la mission auraient des conséquences en matière de LCB-FT. En effet :**

- la proposition n° 4 conduit à inclure les cryptoactifs non fongibles dans le champ d'application du règlement MiCA. L'application du titre V soumet donc les plateformes d'échange de ces cryptoactifs contre des fonds au régime des CASP et implique une obligation de vérifier l'identité de la personne qui échange ces cryptoactifs. Par ailleurs, l'inclusion dans MiCA serait reflétée par l'inclusion dans le champ du règlement sur les transferts (*travel rule*) ;
- la proposition n° 6 crée par ailleurs un régime *ad hoc* pour les plateformes d'échange pair à pair qui ne constituent pas des plateformes de négociation au sens du règlement MiCA, lequel régime inclurait des obligations de LCB-FT. En particulier, les opérateurs de *rollups* relèveraient de l'un ou l'autre des régimes et seraient donc assujettis ;
- dans une moindre mesure, la proposition n° 7, en excluant la possibilité pour les émetteurs de cryptoactifs à vocation commerciale de procéder à leur rachat, compliquerait certains schémas de blanchiment par leurs clients.

**Néanmoins, ces propositions ne permettent pas de répondre à la problématique des entrées et sorties du secteur régulé**. En particulier, il reste relativement aisé, pour une personne détenant des fonds d'origine illicite, de les transférer entre un portefeuille hébergé par un CASP et un portefeuille autohébergé, à la suite de quoi les personnes physiques qui manipulent les flux ne peuvent plus être identifiées facilement et des services de brouillage peuvent être utilisés.

### 3.3.1. Un premier ensemble de mesures peut consister à interdire les transactions depuis et vers certains professionnels dont l'identité n'a pas été vérifiée

**Compte tenu des risques exposés en section 3.1, les cryptoactifs échangés en dehors du secteur régulé des CASP devraient faire l'objet d'un encadrement au moins comparable à celui de l'utilisation des espèces.** Un premier ensemble de mesures pourrait donc consister à rendre obligatoire la vérification de l'identité du détenteur d'un portefeuille autohébergé dans deux situations :

- lorsque le transfert a lieu depuis ou vers un CASP. Autrement dit, il s'agirait de remplacer l'obligation de collecte de l'identité du détenteur du portefeuille autohébergé prévue par la *travel rule* par une obligation de vérification de celle-ci. Le contrôle du respect de cette mesure par les CASP pourrait être assuré par les autorités de régulation (AMF et ACPR) ;
- lorsque le transfert a une finalité professionnelle (achat de biens et services, paiement d'un salaire, *etc.*). Le respect de cette mesure pourrait être vérifié lors de contrôles *a posteriori* des professionnels.

Dans chaque cas, l'obligation de vérification de l'identité n'aurait lieu qu'au-dessus d'un certain seuil, que la mission propose de placer à 1 000 € par cohérence avec le seuil au-dessus duquel les paiements en espèces sont interdits. Toutefois, ce seuil est spécifique à la France et n'est pas harmonisé à l'échelle de l'Union européenne ; certains États tels que l'Allemagne[44] et l'Autriche n'imposent pas de seuil. La pleine efficience d'une telle mesure supposerait toutefois qu'elle soit appliquée uniformément dans l'ensemble de l'Union européenne, ce qui supposerait donc une négociation sur le montant de ce seuil.

**Une difficulté substantielle réside dans la façon dont l'identité peut être vérifiée.** En ce qui concerne les paiements à finalité professionnelle depuis ou vers un portefeuille autohébergé, l'obligation de vérification d'identité pourrait reposer sur le professionnel[45], dans la mesure où ils sont en relation commerciale avec le détenteur du portefeuille autohébergé. En revanche, pour les règlements n'ayant pas de finalité professionnelle qui interviennent entre un portefeuille hébergé par un CASP et un portefeuille autohébergé, le premier n'est en principe pas en relation avec le détenteur du second. Cette considération justifie d'ailleurs l'absence d'obligation pour les CASP, en l'état actuel de la *travel rule*, de vérifier les données d'identité des détenteurs de portefeuilles autohébergés.

[44] En revanche, le débiteur doit produire un titre d'identité pour un paiement supérieur à 10 000 €.

[45] De la même façon qu'un professionnel peut procéder à la vérification d'identité du débiteur réglant par chèque, sur le fondement de l'article L. 131-15 du CMF.

Néanmoins, des solutions techniques existent pour assurer que l'identité des détenteurs de portefeuilles autohébergés est vérifiée sans faire peser cette obligation sur les CASP ou les professionnels acceptant de réaliser des transactions avec eux. Par exemple, des prestataires de service de confiance pourraient contrôler et conserver l'identité du détenteur d'un portefeuille, sans révéler celle-ci sur la *blockchain*, mais placer *on chain* un témoin du fait que l'identité du portefeuille est connue (*cf.* l'annexe III sur le cas d'usage de l'identité numérique). Les données d'identité ne seraient révélées qu'aux autorités compétentes pour les besoins d'une enquête. Un tel système conduirait en fait à séparer trois secteurs :

- le secteur des portefeuilles hébergés par des CASP, entièrement régulé et dans lequel toutes les transactions peuvent être tracées ;
- le secteur des portefeuilles autohébergés dont l'identité a été vérifiée par un prestataire de service de confiance ;
- le secteur des portefeuilles autohébergés dont l'identité n'a pas été vérifiée.

Seuls les portefeuilles des deux premiers secteurs pourraient initier et recevoir des transactions de plus de 1 000 € avec des CASP ou à finalité professionnelle.

**<u>Proposition n° 9.A</u> : Étendre la *travel rule* aux cryptoactifs non fongibles[46] et aux transferts réalisés par le *Lightning Network*. Rendre obligatoire la vérification de l'identité du détenteur d'un portefeuille autohébergé pour un paiement supérieur à 1 000 € réalisé vers ou depuis un CASP ou ayant un caractère professionnel. Cette vérification d'identité pourrait être déléguée à un prestataire de service de confiance garantissant que le détenteur du portefeuille est identifié.**

### 3.3.2. La mission juge souhaitable d'étudier l'opportunité d'une interdiction complète de transferts entre CASP et portefeuilles autohébergés au-dessus d'un seuil

La proposition précédente permettrait un renforcement du contrôle des flux, notamment des sorties de l'environnement *blockchain* intervenant *via* des paiements professionnels directs. Elle créerait une obligation de résultat pour la vérification de l'identité des personnes entrant et sortant de l'environnement régulé. En particulier, elle compliquerait l'utilisation de cryptoactifs obtenus de façon illicite auprès de CASP ainsi qu'auprès de professionnels qui accepteraient d'être rémunérés en cryptoactifs.

**Toutefois, les flux, une fois sortis de l'environnement régulé, ne pourraient plus être tracés**. En particulier, les portefeuilles autohébergés dont l'identité est vérifiée constitueraient des points de passage entre l'environnement régulé et l'environnement non régulé.

Cette situation peut, à nouveau, être comparée à celle des espèces : le retrait et le dépôt d'espèces auprès des banques est traçable, les paiements importants réalisés en espèces peuvent être tracés ou sont interdits, mais les mouvements monétaires en espèces sont libres et anonymes, sauf franchissement d'une frontière[47].

[46] L'inclusion des jetons non fongibles dans le champ d'application de MiCA, recommandée par la mission en proposition n° 4, aura pour conséquence de leur appliquer aussi la *travel rule*, puisque leur exclusion du règlement sur les transferts est assise sur une référence à l'article de MiCA qui exclut les jetons non fongibles, lequel serait supprimé. Pour une meilleure légistique, une modification du règlement sur les transferts est néanmoins souhaitable.

[47] Le règlement (UE) 2018/1672 relatif aux contrôles de l'argent liquide entrant dans l'Union ou sortant de l'Union impose une déclaration par quiconque franchit une frontière extérieure de l'Union européenne avec une somme d'argent liquide supérieure à 10 000 €. Par ailleurs, l'article L. 152-1 rend cette même déclaration obligatoire pour les franchissements des frontières entre la France et un autre État membre de l'Union européenne.

**Néanmoins, plusieurs éléments pourraient justifier d'adopter des mesures plus restrictives pour les cryptoactifs que pour les espèces et notamment d'interdire la sortie de cryptoactifs de l'environnement régulé des CASP.** En effet, le caractère immatériel des cryptoactifs facilite le brouillage et le transfert illicite de flux. De plus, contrairement à ce qui est possible pour les espèces, une perquisition ou une fouille ne permet pas de détecter qu'un individu dissimule des montants importants sous forme de cryptoactifs. En outre, il n'existe pas d'équivalent à un service tel que le *Lightning Network* pour les espèces.

Par ailleurs, alors que les États membres de l'Union européenne ont progressivement adopté des mesures visant à limiter l'utilisation des espèces[48], ils pourraient ne pas souhaiter faciliter l'émergence de nouveaux circuits de paiement présentant des caractéristiques comparables.

Enfin, favoriser le recours aux tiers de confiance que sont les CASP serait cohérent avec le mouvement de recentralisation qu'impose le respect d'autres dispositions du droit : prestataires de services de confiance pour la certification des signatures électroniques (*cf.* section 3 de l'annexe IV), intermédiaires à l'utilisation des *blockchains* pour éviter l'inscription définitive de données personnelles (*cf.* section 4 *infra*).

**La mission a donc réfléchi à une interdiction des transferts depuis des CASP vers des portefeuilles non-hébergés par des CASP**, comme le proposaient les députés Paul Tang et Aurore Lalucq, **exception faite des transferts en-dessous d'un certain seuil** (par exemple, 1 000 € par analogie avec les espèces).

**Cependant, une telle règle présenterait le défaut d'imposer aux utilisateurs de placer leurs cryptoactifs auprès d'un CASP**, puisqu'ils ne pourraient pas les sortir du secteur régulé pour les placer sur un portefeuille autohébergé et *non custodial*. Autrement dit, une telle solution interdirait aux utilisateurs des *blockchains* de conserver eux-mêmes leurs cryptoactifs si la valeur excède le seuil de 1 000 €, y compris dans le but légitime de se protéger contre la faillite d'un conservateur tiers[49] ou contre des failles de sécurité chez celui-ci. Un tel régime serait donc significativement plus restrictif que pour les espèces. En outre, il renforcerait la concentration du marché autour des CASP déjà existants.

L'arbitrage entre la proposition n° 9.A et cette solution paraît à première vue relever d'un choix entre lutte contre le blanchiment et liberté laissée aux utilisateurs d'assurer eux-mêmes la conservation de leurs cryptoactifs. Toutefois, ces deux objectifs pourraient être simultanément poursuivis par le développement de solutions d'hébergement de portefeuille sans conservation. Avec une telle solution, les prestataires d'hébergement seraient chargés de vérifier l'identité des clients (à l'instar des portefeuilles autohébergés à identité vérifiée de la proposition n° 9.A), ainsi que de respecter la *travel rule* et de bloquer les transferts de cryptoactifs hors du secteur régulé, mais ils ne détiendraient pas eux-mêmes les clefs. La possibilité technique d'un tel fonctionnement est discutée en encadré 4. De tels prestataires d'hébergement sans conservation pourraient être intégrés au secteur régulé et donc assimilés à des CASP. Ils permettraient donc aux utilisateurs de conserver leurs cryptoactifs tout en rendant possible le traçage des transactions.

**<u>Proposition n° 9.B</u> : Si la proposition n° 9.A est jugée insuffisante en matière de LCB-FT, envisager d'interdire aux CASP de réaliser ou d'accepter des transactions de cryptoactifs depuis ou vers un portefeuille autohébergé pour un montant supérieur à 1 000 €. Pour l'application de cette règle, créer un statut pour les hébergeurs de portefeuille sans conservation (*non-custodial hosted wallets*) assimilé à celui des CASP.**

[48] Par exemple, la fin de l'émission des billets de 500 € en 2019 ou l'adoption du règlement relatif aux contrôles de l'argent liquide entrant ou sortant de l'Union européenne en 2018.

[49] Risque illustré en particulier par la faillite de l'entreprise FTX en novembre 2022.

**Encadré 4 : Possibilités d'hébergement de portefeuilles sans conservation**

Un portefeuille sur une *blockchain* peut être hébergé par un CASP ou autohébergé, avec ou sans conservation :

- la *conservation* se rapporte à la maîtrise des clefs et donc à la *possession* des cryptoactifs sous-jacents (*cf.* encadré 1 de l'annexe I) ;
- l'*hébergement par un CASP* se rapporte au fait que celui-ci ouvre le compte, vérifie l'identité du client et soit en mesure d'assurer le respect des obligations au titre de la LCB-FT.

Un portefeuille non-hébergé par un CASP peut être conservé par son propriétaire lui-même (solution de type *Ledger* ou *Metamask*) ou par un tiers (par exemple, les clefs peuvent être conservées par un opérateur de jeu). Un portefeuille hébergé par un CASP sans que celui-ci assure également la conservation paraît en revanche plus complexe à concevoir : l'hébergeur, pour respecter ses obligations au titre de la LCB-FT, doit être en mesure de bloquer les transactions non conformes (par exemple, transactions n'étant pas accompagnées des informations exigées par la *travel rule*, ou transactions de plus de 1 000 € n'émanant pas de CASP si la proposition 9.B de la mission est adoptée) ce qui suppose, à première vue, qu'il conserve les cryptoactifs.

Des solutions d'hébergement sans conservation peuvent néanmoins être conçues en utilisant des *smart contracts*. Un exemple de solution pouvant être envisagée est le suivant :

- l'hébergeur vérifie l'identité de son client (*customer due diligence*) ;
- les cryptoactifs sont placés dans un programme autonome (*smart contract*, *cf.* annexe II), programmé pour que seul le client puisse autoriser des transactions sortantes. C'est donc bien le client qui maîtrise ses cryptoactifs : une faillite ou une erreur de l'hébergeur est sans conséquence pour la sécurité de ses cryptoactifs ;
- en revanche, le *smart contract* est programmé de façon à ce que seules des transactions vers des portefeuilles hébergés (par un CASP ou par d'autres solutions d'hébergement sans conservation) puissent être exécutées. Ces portefeuilles hébergés peuvent être identifiés par des jetons *ad hoc* remis par les hébergeurs et révocables en cas de corruption du portefeuille.

## 4. Les *blockchains* posent des problèmes majeurs en matière de données personnelles dont la résolution repose sur une centralisation des traitements

Le droit de la protection des données personnelles fait l'objet d'une harmonisation européenne par le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, dit « règlement général sur la protection des données » (ci-après RGPD).

### 4.1. Du fait de leur décentralisation, les *blockchains* ne permettent que très difficilement de respecter les exigences liées à la protection des données personnelles, en particulier lorsque leur utilisation est commerciale

#### 4.1.1. Les données figurant dans les *blockchains* peuvent être des données personnelles diffusées publiquement de façon irréversible

Les *blockchains* constituent des registres de données, en particulier de données de transactions associées à une cryptomonnaie de chaîne ou à des jetons (*cf.* annexe I). Ce registre est distribué : son contenu est partagé entre plusieurs acteurs ; pour les principales *blockchains* grand public (*Bitcoin*, *Ethereum*, *Ripple*, *Monero*, *etc.*), une copie peut être obtenue par toute personne qui le souhaite.

**Une difficulté réside dans le fait que les données figurant sur la *blockchain* constituent, le plus souvent, des données personnelles.**

Les données personnelles sont en effet définies par le RGPD comme « *toute information se rapportant à une personne physique identifiée ou identifiable* », sachant qu'« *est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement* ».

Or, sur la majorité des *blockchains* grand public, les transactions sont associées à une adresse de portefeuille, qui constitue un pseudonyme. Les données des transactions ne sont donc pas anonymes : chaque transaction se réfère à un individu précis, identifié par son adresse. Des croisements de données inscrites sur la *blockchain* ou de certaines de ces données avec des données issues d'autres sources peuvent par ailleurs permettre des réidentifications *via* des profilages[50]. Une fois un individu identifié, il est possible de connaître l'ensemble de son historique de transactions ainsi éventuellement que son solde et donc de déduire des informations sur sa vie privée.

Ce n'est que si des moyens sont déployés de façon à ce que les données inscrites sur une *blockchain* ne se rapportent pas à une personne physique identifiée ou identifiable que ces mêmes données cessent d'être des données personnelles. Par exemple, avec une technologie telle que les *privacy coins*, qui reposent sur des comptes à usage unique pour chaque transaction reçue et qui permettent de brouiller le compte à l'origine d'une transaction (*cf.* 3.1.2), les transactions ne se rapportent pas à des personnes physiques identifiées ou identifiables.

**Les données personnelles sont ensuite inscrites dans le registre de façon publique, irréversible et inaltérable.** Par conception de l'algorithme de consensus, les écritures passées dans le registre ne peuvent pas être modifiées. En outre, le registre distribué peut être obtenu par toute personne qui en fait la demande.

Certes, des mécanismes d'annulation de transactions ou de suppressions d'objets numériques peuvent être prévus — par exemple, un jeton peut être « brûlé », c'est-à-dire supprimé de la circulation en étant transféré vers un portefeuille dont personne ne détient la clef privée — mais ces opérations viennent s'ajouter à celles qui figuraient auparavant dans le registre. Les transactions ayant été inscrites sur la *blockchain*, quelle que soit leur nature, deviennent publiques de façon irréversible.

**Le fait que des données personnelles, dont certaines peuvent présenter une sensibilité particulière (transactions financières), soient rendues publiques de façon irréversible représente un risque élevé pour les utilisateurs**, quand bien même ceux-ci ont consenti à ce que leurs données personnelles soient ainsi publiées définitivement au moment où ils les ont inscrites sur la *blockchain*. Ce risque est aggravé par le fait que les données sont présentes dans un registre informatisé, donc facilement exploitables par des traitements algorithmiques, et qu'elles sont partagées par l'ensemble des nœuds de validation à travers le monde, incluant donc ceux qui sont établis hors de l'Union européenne.

### 4.1.2. Les jetons à usage commercial sont parfois sources de risques supplémentaires pour la vie privée

Les problématiques exposées en section 4.1.1 ont trait à l'ensemble des usages des *blockchains.* Toutefois, le développement des cryptoactifs à des fins commerciales est source de deux difficultés supplémentaires par rapport aux usages comme produits d'investissement.

[50] Supposons par exemple qu'une association accepte l'encaissement des cotisations par des transactions en bitcoins sur une adresse de portefeuille A. Si une transaction est inscrite sur *Bitcoin* depuis une adresse B vers l'adresse A pour un montant correspondant à celui de la cotisation annuelle quelque jour après l'appel à cotisation, alors il est possible de présumer avec une forte probabilité que l'adresse B est détenue par un membre adhérent à cette association.

D'une part, il est associé à une hausse du volume de données personnelles inscrites dans les *blockchains*. Cette hausse s'explique par :

- une augmentation du nombre d'utilisateurs potentiels ;
- la présence de davantage de données associées à chaque transaction. En effet, des transactions purement financières ne rendent publics que l'identifiant de portefeuille des parties et le montant : des croisements supplémentaires sont nécessaires pour connaître l'objet de la transaction et l'identité des parties. En revanche, pour les cryptoactifs à usage commercial, l'objet de la transaction est un jeton inscrit dans la chaîne et est donc public.

D'autre part, **l'objet même de certains cryptoactifs destinés à un usage commercial est la collecte de données personnelles sur les utilisateurs.** Plusieurs jetons destinés à cet objet sont présentés en section 3 de l'annexe III. Certaines entreprises rencontrées par la mission proposent par exemple des jetons destinés à représenter publiquement la possession de certains biens afin de permettre à l'entreprise ayant commercialisé ce bien de rester en contact avec l'utilisateur à des fins de prospection commerciale et ont fait part de leur intérêt à pouvoir, à l'avenir, réaliser des ciblages sur le fondement du fait qu'un utilisateur détienne plusieurs jetons distincts.

## 4.2. Indépendamment de l'identification des responsables de traitement et des sous-traitants, les *blockchains* ne permettent techniquement pas de respecter les droits des personnes concernées

Le règlement général sur la protection des données (RGPD) vise à protéger les personnes physiques à l'égard des traitements de leurs données personnelles. À cette fin, il confère aux personnes physiques identifiées ou identifiables un certain nombre de droits vis-à-vis de leurs données et de leur traitement, par exemple :

- un droit d'information sur les données personnelles collectées, sur les traitements dont elles font l'objet et sur leur durée de conservation (article 13 du RGPD). Lorsque le traitement de données est fondé sur le consentement de l'utilisateur, cette information doit être fournie au moment du recueil du consentement ;
- un droit à la limitation des traitements et d'opposition à ceux-ci ;
- un droit d'accès aux données traitées et à la portabilité de celles-ci ;
- un droit à la rectification et l'effacement des données, ce dernier étant parfois qualifié de « droit à l'oubli » ;
- un droit à ne pas faire l'objet d'une prise de décision sur le fondement d'un traitement automatisé.

Néanmoins, ces droits ne sont opposables qu'au responsable du traitement automatisé de données, défini par l'article 4(7) du RGPD comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* ».

La mise en œuvre de certains de ces droits vis-à-vis des données inscrites sur une *blockchain* n'est source d'aucune difficulté. C'est le cas en particulier du droit d'accès et du droit à la portabilité des données.

La mise en œuvre d'autres droits (droit à ne pas faire l'objet d'une prise de décision automatisée et droit à l'information) est indépendante de l'inscription des données sur une *blockchain* ou sur un autre support. Toutefois, dans la pratique, la mission relève que la mise en œuvre du droit à l'information est insatisfaisante. Les utilisateurs sont, en effet, rarement avertis du fait que leurs données personnelles seront conservées sur la *blockchain*, sans limite de durée, et seront accessibles publiquement.

En revanche, la mise en œuvre du droit de rectification et d'effacement des données et du droit de retrait du consentement est impossible pour des données inscrites sur une *blockchain* (*cf.* 4.2.3). *A fortiori*, les utilisateurs ne sont pas informés de cette impossibilité de faire valoir leurs droits, ce qui vicie leur consentement.

### 4.2.1. Contrairement aux participants, les mineurs ne peuvent pas être qualifiés de responsables de traitement

En septembre 2018, la Commission nationale de l'informatique et des libertés (CNIL) a publié une communication intitulée *Blockchain : premiers éléments d'analyse de la CNIL* dont l'objet est de préciser le droit applicable aux données personnelles figurant sur les *blockchains*. Cette analyse n'a pas été mise à jour depuis sa publication.

De cette analyse, il ressort qu'**une *blockchain* ne constitue pas en soi un traitement, mais seulement une technologie permettant la mise en œuvre de traitements**. Ainsi, les concepteurs ou développeurs des *blockchains* ne sont pas responsables de traitement.

Les participants, c'est-à-dire les personnes qui réalisent les inscriptions sur la *blockchain* en envoyant un ordre de transaction aux mineurs, sont responsables de traitement. Cependant, l'article 2(2)(c) du règlement exclut de son champ d'application les traitements réalisés par des personnes physiques pour des fins strictement personnelles ou domestiques. Le participant n'est donc responsable de traitement que s'il est une personne morale ou une personne physique agissant dans le cas d'une activité professionnelle.

En revanche, la CNIL estime que les nœuds chargés de la validation des transactions (mineurs et *stakers*, *cf.* annexe I) « *se limitent à la validation des transactions que lui soumettent les participants et n'interviennent pas sur l'objet de ces transactions : ils ne déterminent donc pas les finalités et les moyens à mettre en œuvre* ». Bien que les nœuds réalisent des traitements de données personnelles, le fait qu'ils n'en déterminent ni la finalité ni les moyens exclut la qualification de responsables de traitement.

### 4.2.2. Les mineurs et développeurs de *smart contracts* pourraient être qualifiés de sous-traitants

Néanmoins, comme ces nœuds sont chargés de traiter des données à caractère personnel, la CNIL estime qu'« *il est possible de considérer dans certains cas les mineurs comme des sous-traitants au sens du RGPD* ». Une telle analyse s'applique également aux autres catégories de nœuds de validation (tels que les *stakers* sur *Ethereum)*. En particulier, sur certaines *blockchains* (dont *Bitcoin* et *Ethereum*), les nœuds de validation reçoivent des frais de transaction versés par les participants à l'origine des écritures sur la *blockchain*, ce qui constitue un indice d'une relation de sous-traitance.

La CNIL estime par ailleurs que les développeurs de programmes autonomes sur *blockchains* (« *smart contracts* ») traitent des données à caractère personnel pour le compte des responsables de traitement et doivent donc être qualifiés de sous-traitants.

**La qualification de sous-traitant à donner aux mineurs constitue cependant un sujet de dissensus au sein du comité européen de protection des données** (CEPD, réunion des homologues de la CNIL dans les États membres de l'Union européenne). Dans son analyse de 2018, la CNIL encourage toutefois les mineurs à « *avoir recours à des solutions innovantes leur permettant d'assurer une conformité avec les obligations que fait peser le RGPD sur le sous-traitant* ». Selon les interlocuteurs rencontrés par la mission au sein de la CNIL, ce sujet de désaccord d'interprétation sur la qualification de sous-traitants pour les nœuds de validation constituerait la principale cause de l'absence de mise à jour des analyses de la CNIL depuis 2018.

#### 4.2.3. En tout état de cause, l'inscription de données personnelles directement dans une *blockchain* est incompatible avec les exigences du RGPD

Les articles 24 et 28 définissent certaines obligations générales applicables aux responsables du traitement et à ses sous-traitants. Ainsi, il appartient au responsable du traitement de mettre en œuvre des mesures appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au RGPD. Le sous-traitant doit également mettre en œuvre de tels traitements et garantir les droits de la personne concernée.

**Ainsi, compte tenu de l'impossibilité technique de mettre en œuvre les droits de rectification et de suppression, aucun responsable de traitement ou de sous-traitant de données personnelles qui inscrirait celles-ci directement dans une *blockchain* n'est en mesure de satisfaire aux exigences du RGPD.**

Autrement dit, la compatibilité d'un traitement de données personnelles sur une *blockchain* avec le RGPD suppose :

- soit que le traitement soit réalisé par une personne physique dans le cadre d'une activité strictement personnelle ou domestique[51] (exception domestique). Néanmoins, les personnes concernées par les données personnelles qu'elles traitent pourront être lésées par ce traitement sans avoir la possibilité de faire valoir leurs droits ;
- soit que les seules données personnelles inscrites dans la *blockchain* puissent être supprimées ou rendues anonymes par le responsable de traitement. Le traitement doit donc être conçu de façon à ce que jamais une donnée personnelle ne soit directement inscrite dans la *blockchain* (*privacy by design*).

**Néanmoins, il reste impossible, dans le cas où ces exigences n'ont pas été respectées, de forcer l'application du droit à rectification ou suppression des données personnelles qui ont été inscrites dans la *blockchain*.**

### 4.3. Le respect du principe de *privacy by design* et des obligations de lutte antiblanchiment repose sur une nécessaire recentralisation des données, qui limite l'utilité des *blockchains*

Afin d'éviter que des données personnelles ne soient inscrites dans la *blockchain*, un utilisateur dispose de plusieurs possibilités :

- il peut, d'une part, définir un protocole permettant de ne pas inscrire dans la *blockchain* les données elles-mêmes, mais un « engagement cryptographique », c'est-à-dire une preuve d'existence des données permettant à une personne qui les détient de vérifier leur authenticité, dont le lien avec les données elles-mêmes peut être supprimé (*cf.* encadré 5) ;
- il peut, d'autre part, recourir à des technologies permettent de rendre réellement anonymes les transactions, c'est-à-dire d'empêcher que les écritures figurant dans la *blockchain* se réfèrent à des individus uniques : il s'agit en particulier des *privacy coins*, qui comportent par conception des fonctions d'anonymisation, ou de certaines technologies dites « de seconde couche ». **Ces technologies posent cependant des difficultés substantielles en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, qui ne peuvent être résolues qu'en assurant qu'un tiers conserve les données à fin d'exploitation par les services d'enquête.** C'est notamment la raison de l'assujettissement des CASP au règlement unique sur la lutte anti-blanchiment et aux obligations de connaissance de leur clientèle et de l'obligation d'accompagner les transferts de cryptoactifs de certaines données personnelles (*cf.* 3.2).

[51] Cf. article 2(2)(c) du RGPD.

Ainsi, le respect conjoint de la vie privée des personnes concernées par les données personnelles et des exigences de la LCB-FT suppose soit d'être en mesure de maîtriser strictement les données personnelles inscrites sur la *blockchain* — ce qui est complexe pour un utilisateur non averti — soit de recourir à des intermédiaires centralisés. Dans le cas des utilisations des *blockchains* à des fins commerciales, c'est le plus souvent cette solution qui est mise en œuvre : les entreprises rencontrées par la mission ont ainsi majoritairement fait le choix de n'inscrire sur le registre que des engagements cryptographiques et de conserver les données personnelles claires dans des bases de données privées. **L'intérêt de l'utilisation de *blockchains* dans un contexte centralisé est toutefois contestable, exception faite de considérations d'interopérabilité (*cf.* section 4 de l'annexe I).**

**Aussi, dans sa publication de septembre 2018, la CNIL recommande, si les propriétés d'une *blockchain* ne sont pas nécessaires pour atteindre l'objectif recherché par le traitement, de privilégier d'autres solutions permettant d'assurer une entière conformité au RGPD**, exception faite des cas dans lesquels l'étude d'impact démontre qu'il est acceptable ou obligatoire de rendre publiquement accessibles sans limitation de durée certaines informations.

**Encadré 5 : Un exemple d'utilisation d'une *blockchain* permettant l'exercice du droit de suppression de données personnelles**

Une utilisation d'une *blockchain* pour prouver l'existence et la connaissance d'une donnée personnelle compatible avec les exigences du RGPD peut par exemple consister en l'utilisation d'un engagement cryptographique, reposant sur l'utilisation d'une fonction de hachage cryptographique (*cf.* section 1.2 de l'annexe I).

Supposons qu'une personne souhaite faire figurer dans une *blockchain* la preuve d'une donnée personnelle, par exemple la chaîne de caractère « *Alice Lambert = 01 23 45 67 89* ». Le responsable de traitement choisit une chaîne de caractères appelée « *sel* », en principe de façon aléatoire (par exemple « *Dr05@%Wt5EWQ* »). Il concatène les chaînes de caractère et calcule leur *hash* (*cf.* section 1.2 de l'annexe I), c'est-à-dire qu'il réalise l'opération :

```
sha256("Dr05@%Wt5EWQAlice Lambert = 01 23 45 67 89")
```

Son résultat est une donnée dont la représentation hexadécimale est un *hash* `0x895728f758a1`… Ce *hash* peut être inscrit dans la *blockchain*.

Tant que le responsable du traitement conserve une trace du « sel », toute personne peut confirmer que les données qu'elle détient correspondent bien à celles qui ont été inscrites. En effet, il lui suffit de demander au responsable du traitement de réaliser le même calcul et de confirmer que le résultat est bien `0x895728f758a1`… pour obtenir une telle confirmation.

Si la personne objet de la donnée personnelle souhaite obtenir effacement, il suffit que le responsable du traitement détruise chaque copie qu'il détient du « sel ». En effet, sans celui-ci, il est impossible de retrouver le sens à donner à l'inscription `0x895728f758a1`… qui figure dans le registre.

La mission ne peut aller plus loin que ce constat d'incompatibilité entre l'utilisation grand public des *blockchains* et une partie des droits protégés par le RGPD. **Elle ne peut qu'appeler de ses vœux une clarification de l'effectivité des droits reconnus par le RGPD quant aux données inscrites sur des *blockchains*** : une harmonisation de la position des régulateurs européens doit permettre soit de tirer les conséquences de l'incompatibilité des traitements de données sur *blockchain* avec le droit, soit de conduire à une modification de ce dernier. Une telle clarification est nécessaire afin de limiter l'insécurité juridique entourant l'utilisation des *blockchains* en matière de données personnelles, tant pour les responsables de traitement que pour les personnes concernées par ces données.

# ANNEXE VI

# La fiscalité des jetons à vocation commerciale

# SOMMAIRE

**Le traitement fiscal des jetons à vocation commerciale (JVC), parmi lesquels la plupart des NFT, demeure incertain**. **Cette incertitude provient de l'absence de qualification juridique des JVC, qui, en l'absence de jurisprudence, empêche de déterminer précisément le régime fiscal à appliquer.** Cette insécurité juridique constitue un frein au développement des cryptoactifs dans l'économie française car les acteurs concernés, au premier rang desquels les entreprises souhaitant intégrer les cryptoactifs dans leur activité, ne savent pas quelles hypothèses fiscales prendre en compte dans la conception de leur modèle économique et prennent un risque de requalification.

La loi PACTE a instauré un régime fiscal précis pour les actifs numériques, qui incluent notamment les cryptomonnaies. L'inclusion ou non des JVC dans ces actifs numériques reste en débat (*cf.* section 2). Dès lors, il n'existe pas de régime spécifique pensé pour les JVC.

**Trancher en faveur d'une inclusion générique des JVC dans le régime des actifs numériques a pour avantage principal la simplicité. Néanmoins, pour les raisons exposées ci-dessous, imposer à tous les JVC, quelle que soit la contrepartie, un traitement fiscal homogène ne semble pas recommandable d'après la mission**. Par ailleurs, le régime des actifs numériques est lui-même critiqué par les acteurs du secteur pour sa complexité. En effet, en tant que régime fondé sur l'imposition de la plus-value, il est adapté à une logique de placement : le contribuable doit déclarer les transactions qu'il effectue en cryptomonnaies ainsi que les plus-values réalisées sur la base d'une valeur moyenne de portefeuille afin d'être imposé sur cette plus-value. Dès lors que le contribuable utilise les cryptomonnaies non pas comme un instrument de placement financier mais comme une monnaie d'échange, lors de transactions nombreuses et de faibles montants, avec des conversions en monnaie *fiat* très fréquentes, le régime devient complexe à respecter. Sans pouvoir se prononcer sur le régime idéal qu'il s'agirait de mettre en place, la mission recommande le lancement d'une réflexion, qui pourrait inclure les acteurs du secteur, sur l'ajustement de ce régime, qui pourrait comporter un avantage fiscal lié à la détention longue des actifs, comme c'est le cas au Portugal ou en Allemagne.

**Dans le cas où l'inclusion dans le régime des actifs numériques ne serait pas admise, la création d'un régime propre aux JVC ne constituerait pas pour autant une solution préférable**. **En effet, les JVC constituent des outils techniques utilisés dans des cas d'usages variés** (*cf.* annexe III) et qui sont associés à des actifs sous-jacents très hétérogènes. Ainsi, il n'est pas évident que la meilleure manière de fiscaliser les JVC soit de concevoir un régime sur la base de la technologie utilisée, puisque ce régime ne pourrait pas, par définition, être adapté à chaque cas d'usage.

**La mission se prononce donc plutôt en faveur d'une réflexion sur la mise en place d'un régime qui soit fonction des sous-jacents et non de la technologie utilisée.** Ainsi, un NFT artistique pourrait bénéficier de la fiscalité relative aux droits sur les œuvres d'art et un NFT représentant une épée dans un jeu vidéo serait fiscalisé comme une prestation de service électronique. Cette logique reviendrait à considérer le jeton comme fiscalement transparent et à fiscaliser son actif sous-jacent. C'est d'ailleurs le raisonnement qui prévaut déjà dans l'assimilation des *security tokens* à des instruments financiers, laquelle emporte des conséquences fiscales (exonération de la TVA, par exemple) : dans ce cas, c'est bien la contrepartie qui l'emporte sur la technologie.

# 1. En matière de fiscalité des entreprises, les jetons à vocation commerciale ne font pas l'objet de règles spécifiques

## 1.1. Le plan comptable général a été révisé pour prendre en compte les jetons, dont font partie les JVC

Par les règlements 2018-07 du 10 décembre 2018 et 2020-05 du 24 juillet 2020, l'Autorité des normes comptables (ANC) a modifié le plan comptable général (PCG) afin d'y intégrer la comptabilisation des jetons, à la suite de la loi PACTE.

Ainsi, une section 9 consacrée aux jetons a été ajoutée au chapitre 1 du titre VI du livre II. Les règles de comptabilisation adoptent la logique prévalant en matière de réglementation financière et de fiscalité : les jetons sont comptabilisés différemment selon qu'ils présentent les caractéristiques d'instruments financiers ou non.

En cas d'émission de jetons, « *les jetons ne présentant pas les caractéristiques de titres financiers, de contrats financiers ou de bons de caisse sont comptabilisés selon les droits et obligations attachés :*

- *si les jetons présentent les caractéristiques d'une dette remboursable, même à titre temporaire, ils sont comptabilisés en emprunts et dettes assimilées, conformément aux règles de l'article 941-16 ;*
- *si les jetons sont représentatifs de prestations restant à réaliser ou de biens restant à livrer, ils sont comptabilisés en produits constatés d'avance, selon les articles 323-9 et 619-7 ;*
- *s'il n'existe pas d'obligations explicites ou implicites vis-à-vis des souscripteurs et détenteurs de jetons, les sommes collectées sont considérées comme définitivement acquises par l'émetteur et sont comptabilisées en produits, conformément à l'article 512-1* »[1].

En cas de détention de jetons, « *lorsque l'entité détient, par souscription ou acquisition, des jetons ne présentant pas les caractéristiques de titres financiers, de contrats financiers ou de bons de caisse, en vue d'utiliser les services ou les biens associés, et qu'il en est attendu une utilisation au-delà de l'exercice en cours,* ***ces jetons constituent des immobilisations incorporelles****, amorties et dépréciées selon les articles 214-1 à 214-21. Les jetons comptabilisés en immobilisation incorporelle de durée d'utilisation non définie peuvent être transférés à titre définitif en jetons détenus tels que décrits à l'article 619-12, lorsque l'usage attendu des services ou des biens associés n'existe plus* »[2]. Les « jetons détenus » sont comptabilisés au compte 522.

Le PCG ne fait pas mention des NFT, qui ne font donc pas l'objet d'un traitement spécifique et sont, a priori, considérés comme des jetons.

## 1.2. En matière d'impôt sur les sociétés, les JVC ne font l'objet d'aucune règle spécifique

Les JVC ne font l'objet, en matière d'impôt sur les sociétés (IS), d'aucun régime particulier : ce sont les règles de droit commun qui s'appliquent.

La vente de JVC émis par des sociétés soumises à l'IS donne lieu à des produits, qui viennent abonder le résultat imposable.

---

[1] Article 619-4 du PCG.

[2] Article 619-11 du PCG.

Lorsque les JVC sont acquis puis revendus, ceux-ci sont comptabilisés comme des immobilisations incorporelles (*cf.* dispositions du PCG ci-dessus). Les plus-values sur cryptoactifs ne font pas l'objet de régime fiscal spécifique, contrairement aux particuliers (*cf.* section 3.1) et obéissent aux règles de la fiscalité des plus-values professionnelles pour les sociétés soumises à l'IS (un autre régime existe pour les entreprises soumises à l'impôt sur le revenu). Les plus-values professionnelles nettes à long terme[3] sont taxées au taux d'IS de 15 % (article 219 du CGI). Les plus-values de court terme sont intégrées au résultat imposable, soumis au taux normal de l'IS, fixé par l'article 219 du CGI à 25 %. Contrairement aux particuliers, une cession de cryptoactifs contre d'autres cryptoactifs (par exemple, un NFT artistique contre des bitcoins) constitue un fait générateur pour l'imposition des plus-values.

## 2. L'application du régime de TVA à la vente de JVC soulève plusieurs problèmes, notamment en matière de territorialité

### 2.1. Le régime de TVA applicable aux JVC dépend d'une analyse au cas par cas et suppose la connaissance du pays de résidence des clients

Les jetons sont parfois utilisés par les institutions et les entreprises à titre gratuit, que ce soit pour les incorporer dans un système interne de logistique ou de gestion des relations aux clients (*cf.* annexe III sur les cas d'usage). Néanmoins, dans de nombreux cas d'usage, les JVC sont vendus à des clients (dans le secteur du jeu, notamment, ou des biens de luxe). Dès lors, la question de l'assujettissement à la TVA se pose[4]. En effet, l'article 256 du CGI dispose que « *sont soumises à la taxe sur la valeur ajoutée les livraisons de biens et les prestations de services effectuées à titre onéreux par un assujetti agissant en tant que tel* ». Pour rappel, une prestation de service est définie par l'article 24 de la directive 2006/112/CE du Conseil relative au système commun de TVA (désignée par l'expression « directive TVA » par la suite) comme « *toute opération qui ne constitue pas une livraison de biens* ».

La jurisprudence de la Cour de justice de l'Union européenne (CJUE) a précisé que la notion de prestation de services effectuée à titre onéreux supposait l'existence d'un lien direct entre le service rendu et la contre-valeur reçue (CJUE, 8 mars 1988, n° 102/86, *Apple and Pear Development Council*). L'existence d'un aléa entre l'acquisition du jeton et l'éventuelle contrepartie associée à sa détention rompt ce lient direct et justifie, selon la doctrine, qu'une émission de jetons dans le cadre d'une offre au public de jetons ne soit pas soumise à la TVA (*cf.* rescrit BOI-RES-TVA-000054[5]). À la différence des offres au public de jetons, la vente de JVC a, *a priori*, pour principe de ne pas rendre aléatoire la fourniture de la contrepartie et, au contraire, de procurer un droit de « propriété » reconnu sur le bien ou le service sous-jacent (*cf.* annexe III).

[3] En vertu de l'article 39 duodecies du CGI, une plus-value est considérée comme à court terme si l'actif est cédé moins de deux ans après son acquisition et à long terme si l'actif est cédé plus de deux ans après son acquisition.

[4] Dans la suite de cette partie, nous nous situons dans le cas où le vendeur du jeton est une entreprise assujettie à la TVA. La vente d'un jeton par un particulier ne serait *a priori* pas soumise à la TVA, sauf si cette vente est qualifiée d'activité économique (notamment, si cette vente initiale donne droit à des *royalties* à chaque revente ultérieure). Le *working paper* du Comité TVA considère néanmoins que ces royalties *auraient* plus de chances d'être qualifiées de droits de revente, non soumis à TVA, plutôt que de droits d'utilisation successive (*cf.* p. 14 du *working paper)*.

[5] Rescrit « RES - Taxe sur la valeur ajoutée - Champ d'application et territorialité - Assujettissement et base d'imposition d'une offre au public de jetons » du 9 mars 2021.

Si un jeton est un *security token* et constitue un instrument financier, celui-ci est exonéré de TVA en vertu du f de l'article 135 de la directive TVA, qui exonère « *les opérations, y compris la négociation mais à l'exception de la garde et de la gestion, portant sur les actions, les parts de sociétés ou d'associations, les obligations et les autres titres* ». De même, les opérations d'échange de cryptomonnaies sont exonérées sur le fondement du e de l'article 135 de la directive, qui vise les opérations portant sur les devises[6].

Lorsque le jeton est à vocation commerciale (le plus souvent un *utility token* ou un jeton artistique), l'ensemble de l'opération économique doit être analysé pour déterminer les conditions d'assujettissement à la TVA, dans une démarche de cas par cas.

L'administration fiscale française n'a pas émis de doctrine faisant état de règles spécifiques appliquées à la taxation à la TVA des JVC : le droit commun s'applique. Le *working paper* n° 1060 du Comité TVA, daté du 21 février 2023, pose les bases d'une analyse du traitement fiscal à appliquer aux NFT, dans le but de faire converger les positions des administrations nationales — la mission relève que des analyses similaires pourraient être menées pour les autres types de jetons à vocation commerciale. Le Comité TVA considère que les NFT peuvent recevoir les qualifications suivantes :

- titres de propriété : dans ce cas, la taxation TVA à appliquer est celle de l'actif sous-jacent ;
- bons, à usage unique ou à usage multiple (*cf. infra* pour la fiscalité des bons) ;
- offres composites (entre un jeton numérique et un actif sous-jacent) : dans ce cas, la fiscalité applicable est celle de l'élément principal (*vs* l'élément accessoire) ;
- services électroniques (*cf. infra*).

Le *working paper* confirme donc qu'une appréciation au cas par cas est nécessaire pour déterminer le traitement fiscal à appliquer.

Lorsqu'ils donnent droit à la livraison d'un bien ou d'un service[7], les jetons peuvent être assimilés à des bons, définis à l'article 256 ter du CGI : « *Est considéré comme un bon tout instrument assorti d'une obligation de l'accepter comme contrepartie totale ou partielle d'une livraison de biens ou d'une prestation de services et pour lequel les biens à livrer ou les services à fournir ou l'identité de leurs fournisseurs ou prestataires potentiels sont indiqués soit sur l'instrument même, soit dans la documentation correspondante, notamment dans les conditions générales d'utilisation de cet instrument* ».

Le régime fiscal des bons, issu de la directive 2016/1065 du Conseil du 27 juin 2016, dépend du type de bons, selon qu'ils sont à usage unique ou à usage multiple :

- dans le cas d'un bon à usage unique (défini à l'article 256 ter du CGI[8]), tout transfert « *est considéré comme une livraison des biens ou une prestation des services à laquelle le bon se rapporte. La remise matérielle des biens ou la prestation effective des services en échange d'un bon à usage unique accepté en contrepartie totale ou partielle par le fournisseur ou le prestataire n'est pas considérée comme une opération distincte* »[9]. La vente du bon est donc soumise à la TVA du bien ou service rattaché au bon ;

---

[6] *Cf.* CJUE, 22 octobre 2015, Skatteverket c/ David Hedqvist, C-264/14.

[7] Cette condition suppose que les droits associés à la détention du jeton soient clairement énoncés lors de l'acquisition. Cette question renvoie à la problématique de la définition des droits associés aux jetons, traitée en section 2 de l'annexe IV.

[8] « *Est considéré comme un bon à usage unique un bon* […] *pour lequel le lieu de la livraison des biens ou de la prestation des services à laquelle le bon se rapporte et la taxe sur la valeur ajoutée due sur ces biens ou services sont connus au moment de l'émission du bon.* »

[9] Article 256 ter du CGI.

- dans le cas d'un bon à usage multiple, le transfert du bon n'est pas soumis à la TVA : c'est la « *remise matérielle de biens ou la prestation effective de services* » qui y est soumise, au taux associé aux biens ou aux services en question.

La plupart du temps, les JVC sont associés à la livraison d'un service, plus précisément d'une prestation de services électroniques (comme l'accès à un jeu en ligne), définis à l'article 7 du règlement d'exécution (UE) n° 282/2011 du Conseil du 15 mars 2011 comme les « *services fournis sur l'internet ou sur un réseau électronique et dont la nature rend la prestation largement automatisée, accompagnée d'une intervention humaine minimale, et impossible à assurer en l'absence de technologie de l'information* ». L'article 98 C de l'annexe III du CGI donne notamment pour exemple de services fournis par voie électronique la « *fourniture d'images, de textes et d'informations et la mise à disposition de bases de données* ».

La taxation des prestations de service est régie par un principe de différenciation, selon que le client est un assujetti (cas du « *business to business* ») ou un non-assujetti (cas du « *business to customer* »):

- lorsque le client est un assujetti, c'est le principe de destination qui s'applique : le lieu de la prestation (qui détermine le taux de TVA applicable) est « *l'endroit où l'assujetti a établi le siège de son activité économique* » (article 44 de la directive TVA) ;
- lorsque le client est un non assujetti, c'est le principe d'origine qui s'applique : le lieu de la prestation est « *l'endroit où le prestataire a établi le siège de son activité économique* » (article 45 de la directive TVA).

Néanmoins, les réformes de la directive TVA (directive du 12 février 2008, directive du 5 avril 2022) ont prévu des exceptions au principe d'origine dans le cas du « *B to C* ». Pour certains types de services (prestations de télécommunications, services de télévision et de radiodiffusion et services fournis par voie électronique), c'est le principe de destination qui s'applique (*cf.* article 58 de la directive TVA). Ainsi, en considérant le cas d'un prestataire français livrant un service électronique à une personne non assujettie :

- si le consommateur est établi en France, le lieu de la prestation de service électronique est réputé situé en France et c'est le taux français qui s'applique (*cf.* article 259 D du CGI) ;
- si le consommateur est établi dans un autre État membre de l'Union européenne :
  - si de plus « *la valeur totale de ces prestations ainsi que des ventes à distance intracommunautaires de biens effectuées par cet assujetti n'a pas excédé, pendant l'année civile en cours au moment de la prestation ou de la vente à distance intracommunautaire de biens et pendant l'année civile précédente, le seuil de 10 000 € hors taxe sur la valeur ajoutée* », alors c'est le taux français qui s'applique (*cf.* II.1. de l'article 259 D du CGI) ;
  - si au contraire le seuil mentionné au point précédent est dépassé, alors c'est le taux du pays du consommateur qui s'applique[10] et le prestataire peut avoir recours au dispositif de guichet unique européen « *one stop shop* » (OSS)[11] pour déclarer ses opérations et payer la TVA due aux différents États membres ;
- si le consommateur n'est pas établi dans l'Union européenne, le lieu de la prestation est réputé ne pas se situer en France et la transaction n'est pas imposable en France (article 259 B du CGI).

[10] L'alinéa 2 du II.1 de l'article 259 D du CGI dispose que, une fois ce seuil dépassé, les dispositions du premier alinéa cessent de s'appliquer, ce qui signifie que le lieu de la prestation de service n'est plus réputé situé en France. L'article 58 de la directive TVA dispose alors qu'il est réputé situé dans l'État membre où est situé le preneur.

[11] Prévu dans le droit français à l'article 298 sexdecies G du CGI.

**Tableau 1 : Synthèse des lieux d'imposition à la TVA selon les situations, lorsque le prestataire de service électronique est établi en France**

| Lieu d'établissement du prestataire de service électronique | Lieu d'établissement du preneur non assujetti | Lieu d'imposition |
|---|---|---|
| France | France | France |
| | Autre État membre | France si ventes ≤ 10 k€ par an<br>État membre si ventes > 10 k€ par an |
| | Pays tiers | Pays tiers |

*Source : Mission, sur la base du CGI.*

Ce critère de territorialité pose problème pour les ventes de jetons dans la mesure où les transactions sur les *blockchains* ne permettent pas de connaître l'identité et, *a fortiori*, l'adresse des acquéreurs. Ce problème n'est pas mentionné par le *working paper* du Comité TVA.

Or, la connaissance par le prestataire du lieu d'établissement du preneur est une obligation, matérialisée par la déclaration TVA (prévue à l'article 287 du CGI), nécessaire au bon acquittement de la taxe. Le règlement d'exécution n° 282/2011 prévoit également, pour l'application de l'article 58 de la directive TVA, que « *le preneur est établi, à son domicile ou à sa résidence habituelle au lieu identifié comme tel par le prestataire sur la base de deux éléments de preuve non contradictoires visés à l'article 24 septies* » (article 24 ter). Ces éléments de preuve sont :

- *« l'adresse de facturation du preneur ;*
- *l'adresse IP (protocole internet) du dispositif utilisé par le preneur ou toute autre méthode de géolocalisation ;*
- *les coordonnées bancaires, telles que le lieu où est tenu le compte bancaire utilisé pour le paiement ou l'adresse de facturation du preneur connue par la banque ;*
- *le code mobile national (MCC) de l'identité internationale de l'abonné mobile (IMSI) enregistré sur la carte SIM (module d'identité de l'abonné) utilisée par le preneur ;*
- *la localisation de la ligne fixe du preneur par l'intermédiaire de laquelle le service lui est fourni ;*
- *d'autres informations commerciales pertinentes. »*

**Le problème de la territorialité des opérations de vente de JVC n'est donc à ce jour pas réglé**. L'adresse IP pourrait constituer un élément de preuve si le client doit passer par un site internet qui fournit cette information au prestataire, mais il ne serait pas suffisant à lui seul. En l'absence de donnée sûre quant à l'adresse d'un client, les entreprises rencontrées par la mission tendent à appliquer, par défaut, le taux français, mais ce pis-aller ne les place pas en situation de conformité.

La circonstance selon laquelle une transaction a lieu *via* une *blockchain* qui ne nécessite pas la connaissance de l'identité de l'acheteur ne dispense pas les entreprises du respect de leurs obligations en matière de TVA. Dès lors, toute vente de jetons à vocation commerciale devrait être, *a priori*, accompagnée d'une procédure d'identification du pays de résidence du client. Il reste à déterminer quelles modalités de collecte de cette information sont jugées suffisantes par l'administration fiscale. Cet enjeu est propre à toute prestation de service électronique et non pas spécifique aux ventes de jetons.

## 2.2. Les œuvres d'art bénéficient de régimes de TVA particuliers

Les œuvres d'art bénéficient d'un régime spécial de TVA à plusieurs titres :

- des taux réduits de TVA sont applicables à la vente d'une œuvre d'art :
  - le taux réduit de 10 %, prévu par l'article 278 septies du CGI, est applicable lors d'une vente par une personne ayant utilisé l'œuvre pour ses besoins d'exploitation (le BOFIP[12] donne l'exemple d'entreprises ayant acquis une œuvre dans le cadre du mécénat). L'entreprise doit avoir comptabilisé l'œuvre dans ses immobilisations et non dans ses stocks (elle serait alors considérée comme assujetti-revendeur et non comme assujetti-utilisateur) ;
  - le taux réduit de 5,5 % est applicable dans les situations suivantes (*cf.* I de l'article 278-0 bis du CGI) :
    - « *les importations d'œuvres d'art, d'objets de collection ou d'antiquité, ainsi que sur les acquisitions intracommunautaires, effectuées par un assujetti ou une personne morale non assujettie, d'œuvres d'art, d'objets de collection ou d'antiquité qu'ils ont importés sur le territoire d'un autre État membre de l'Union européenne* » ;
    - « *les acquisitions intracommunautaires d'œuvres d'art qui ont fait l'objet d'une livraison dans un autre État membre par d'autres assujettis que des assujettis revendeurs* » ;
    - « *les livraisons d'œuvres d'art effectuées par leur auteur ou ses ayants droit* ». Le BOFIP rappelle que « *les auteurs des œuvres de l'esprit agissant à titre indépendant soumettent à la TVA les livraisons de biens qu'ils réalisent à titre onéreux* », en vertu de l'article 256 A du CGI ;
- le régime spécial de la marge, prévu par les articles 311 à 325 de la directive TVA, transposé à l'article 297 A du CGI, prévoit qu'un assujetti-revendeur d'œuvres d'art peut décider de soumettre à la TVA, lors d'une livraison, seulement la marge bénéficiaire, c'est-à-dire la différence entre le prix de vente et le prix d'achat[13]. En application de l'article 297 B, le taux de TVA alors appliqué peut être le taux réduit prévu par l'article 278 septies ou 278-0 bis du CGI (*cf. supra*). Les galeries d'art, par exemple, sont des assujettis-revendeurs et peuvent proposer à la vente des NFT ;
- les cessions de droits patrimoniaux[14] portants sur des œuvres d'art, en tant qu'œuvres de l'esprit (pour les définitions, se reporter à la section 4), sont taxées au taux intermédiaire de 10 %, en vertu du g de l'article 279 du CGI[15]. **La question de la compatibilité de cet article avec la directive TVA ne sera pas tranchée dans ce rapport mais mérite néanmoins d'être soulevée**, dans la mesure où il y est fait référence aux « œuvres de l'esprit », terme qui, en droit français, a une acception plus large que celui d'« objets d'art », défini dans la directive TVA.

---

[12] *Cf.* BOFiP BOI-TVA-SECT-90-40 du 4 mars 2015, « TVA - Régimes sectoriels - Dispositions particulières applicables aux œuvres d'art, objets de collection ou d'antiquité ».

[13] Pour plus de détails sur ce régime et sur le calcul de la marge, *cf.* BOFIP BOI-TVA-SECT-90-20-20 du 13 août 2021, « TVA - Régimes sectoriels - Biens d'occasion, œuvres d'art, objets de collection ou d'antiquité - Principes d'imposition - Biens livrés par des assujettis-revendeurs ».

[14] Pour rappel, les droits d'auteur comprennent les droits moraux, qui sont perpétuels et inaliénables, et les droits patrimoniaux (par exemple, droit de reproduction, droit de traduction ou droit de suite), qui sont cessibles par un contrat de cession de droits. Pour plus de précisions, *cf.* section 4 de l'annexe IV, en particulier encadré 4.

[15] « *Les cessions des droits patrimoniaux reconnus par la loi aux auteurs des œuvres de l'esprit et aux artistes-interprètes ainsi que de tous droits portant sur les œuvres cinématographiques et sur les livres* ».

**Ainsi, la qualification d'œuvre d'art pour les NFT artistiques aurait des conséquences fiscales importantes, notamment pour les artistes vendeurs et pour les galeries, les ventes d'œuvres d'art bénéficiant de taux de TVA réduits.**

La question de cette qualification, qui emporte d'autres conséquences fiscales, est traitée en section 4.

## 3. En matière de fiscalité des particuliers, le régime des actifs numériques existe, mais la mission recommande un traitement fiscal au cas par cas, selon le sous-jacent

L'article 516 du Code civil dispose que « *tous les biens sont meubles ou immeubles* ». Au sein des biens meubles, quatre catégories de biens doivent être distinguées, car elles relèvent chacune d'un régime fiscal différent[16] :

- les métaux précieux, les bijoux et les objets d'art, de collection ou d'antiquité (*cf.* article 150 VI du CGI) ;
- les valeurs mobilières et les droits sociaux (*cf.* article 150-0 A du CGI) ;
- les actifs numériques (*cf.* article 150 VH bis du CGI) ;
- les autres biens meubles (*cf.* article 150 UA du CGI).

Le régime fiscal des « autres biens meubles » est ainsi le régime de droit commun : tout bien meuble y est soumis à moins d'être considéré comme une œuvre d'art, une valeur mobilière ou un actif numérique. Les jetons à vocation commerciale, parmi lesquels les jetons non fongibles n'étant pas définis dans le droit français, leur qualification juridique et fiscale reste indéterminée. Dans la mesure où les jetons à vocation commerciale ne sont pas des valeurs mobilières, trois régimes fiscaux restent envisageables en ce qui concerne les transactions portant sur des JVC et effectuées par des particuliers :

- le régime des actifs numériques ;
- le régime des plus-values sur biens meubles incorporels ;
- le régime des œuvres d'art, qui pourrait trouver à s'appliquer pour les NFT artistiques.

En l'absence de définition des JVC dans le droit français, les acteurs économiques qui les manient considèrent qu'ils souffrent d'une certaine insécurité juridique et prennent un risque fiscal en optant pour un régime fiscal ou pour un autre.

L'administration fiscale considère, elle, que les JVC, parmi lesquels les NFT, constituent des actifs numériques et sont donc régis par le même régime fiscal que les autres cryptoactifs[17].

---

[16] *Cf.* doctrine exposée dans le BOFiP BOI-RPPM-PVBMC.

[17] En ce qui concerne les NFT, cette position est exposée dans une note interne de la Direction générale des finances publiques, annexe à la note 2022/16725, mise à jour en février 2023. Cette note indique que « *l'inclusion ou non des NFT dans le champ d'application de l'article L.54-10-1 du CoMoFi (et partant de l'article 150 VH bis du CGI) fait débat* » mais qu'« *en principe les NFT entrent dans le champ d'application de l'article L.54-10-1 du Code monétaire et financier (CoMoFi) qui inclut parmi les actifs numériques les jetons. […]Dès lors que le caractère fongible ou non-fongible des jetons n'est pas un critère de définition, au regard du texte légal précité, des actifs numériques, il y a lieu de considérer que le NFT est bien un actif numérique* ».

Une députée, M^me^ Véronique Louwagie (LR), a posé une question écrite au gouvernement le 25 janvier 2022 (question n° 43760) au sujet de la fiscalité des NFT, notamment au regard du régime fiscal des œuvres d'art. Cette question n'a pas obtenu de réponse avant la fin de la législature en juin 2022 et a été retirée.

## 3.1. Un régime fiscal spécialement consacré aux actifs numériques a été instauré en 2019

### 3.1.1. En vertu de la définition des actifs numériques du code monétaire et financier, les JVC devraient être considérés comme des actifs numériques et, dès lors, être soumis au régime fiscal spécial

L'article 41 de la loi n° 2018-1317 du 28 décembre 2018 de finances pour 2019 a créé, en modifiant le code général des impôts (CGI), un régime fiscal propre aux cryptoactifs. Ainsi, l'article 150 VH bis du CGI, modifié par la loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises (PACTE), prévoit la fiscalisation des plus-values réalisées à l'occasion de la cession d'actifs numériques, à un taux fixé à l'article 200 C du CGI, lui aussi créé par la loi de finances pour 2019.

Le périmètre d'application de ce régime suppose de définir préalablement les « actifs numériques » concernés. Ces derniers sont définis par l'article L. 54-10-1 du code monétaire et financier (CMF) comme :

« *1° Les jetons mentionnés à l'article L. 552-2, à l'exclusion de ceux remplissant les caractéristiques des instruments financiers mentionnés à l'article L. 211-1 et des bons de caisse mentionnés à l'article L. 223-1 ;*

*2° Toute représentation numérique d'une valeur qui n'est pas émise ou garantie par une banque centrale ou par une autorité publique, qui n'est pas nécessairement attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d'une monnaie, mais qui est acceptée par des personnes physiques ou morales comme un moyen d'échange et qui peut être transférée, stockée ou échangée électroniquement.* »

Les jetons mentionnés à l'article L. 552-2 du CMF sont définis de la manière suivante : « *Au sens du présent chapitre, constitue un jeton tout* ***bien incorporel représentant, sous forme numérique, un ou plusieurs droits pouvant être émis, inscrits, conservés ou transférés au moyen d'un dispositif d'enregistrement électronique partagé permettant d'identifier, directement ou indirectement, le propriétaire dudit bien.*** ».

Les instruments financiers, définis à l'article L. 211-1 du CMF, regroupent les titres financiers (titres de capital émis par les sociétés par actions, titres de créance, parts ou actions d'organismes de placement collectif) et les contrats financiers, aussi appelés instruments financiers à terme.

Les cryptomonnaies rentrent dans la définition des actifs numériques en tant que représentation numérique d'une valeur qui n'est pas émise ou garantie par une banque centrale, acceptée par des personnes physiques ou morales comme un moyen d'échange et qui peut être transférée, stockée ou échangée électroniquement.

**Les jetons à vocation commerciale constituent des jetons, qui, *a priori*, rentrent dans la définition de l'article L. 552-2 du CMF et seraient ainsi régis par l'article L. 54-10-1 du CMF**. Le cas des jetons utilitaires (*utility tokens*), par exemple des NFT donnant droit à un bien (la livraison d'un vinyle, par exemple) ou à un service (accès à un événement payant, programme de garantie), laisse peu de place au doute. Le cas des jetons n'étant associés à aucun droit, comme c'est le cas des NFT purement artistiques (c'est-à-dire des NFT se contentant de pointer vers des fichiers numériques d'œuvres d'art), est plus ambigu dans la mesure où ces jetons ne remplissent pas la condition de « *représent[er] sous forme numérique,* ***un ou plusieurs droits*** *pouvant être émis, inscrits, conservés ou transférés au moyen d'un dispositif d'enregistrement électronique partagé* », inscrite dans la définition de l'article L. 552-2 du CMF. La mission considère néanmoins que le cas des jetons dépourvus de tous droits associés devrait tendre à disparaître : elle recommande que tout achat de JVC soit accompagné d'une mention claire des droits qui sont associés au jeton acquis (*cf.* sections 2 et 4 de l'annexe IV). Si cette recommandation était suivie, tout JVC serait théoriquement considéré comme un jeton au sens de l'article L. 552-2 du CMF. Seule resterait incertaine la situation des jetons « nus », c'est-à-dire dépourvus de tout droit associé.

### 3.1.2. Le régime fiscal des actifs numériques prévoit une taxation des plus-values au prélèvement forfaitaire unique sauf en cas d'échange entre actifs numériques

**Le régime fiscal posé par l'article 150 VH bis du CGI prévoit la fiscalisation à l'impôt sur le revenu (IR) des plus-values** « *réalisées par les personnes physiques domiciliées fiscalement en France […] lors d'une cession à titre onéreux d'actifs numériques* ».

**Le calcul de l'impôt dû suppose de calculer la plus-value réalisée**. Le BOFIP (*cf.* BOI-RPPM-PVBMC-30-20[18]) précise comment doit être calculée la plus-value, selon une approche de portefeuille, par année calendaire : « *la plus ou moins-value brute est égale à la différence entre, d'une part, le prix de cession et, d'autre part, le produit du prix total d'acquisition de l'ensemble du portefeuille d'actifs numériques par le quotient du prix de cession sur la valeur globale de ce portefeuille* ». Toutes les valeurs doivent être converties en euros par application du taux de change à la date de chaque opération. La plus-value imposable est nette des moins-values : « *les moins-values brutes subies au cours d'une année d'imposition au titre des cessions d'actifs numériques ou droits s'y rapportant sont imputées exclusivement sur les plus-values brutes de même nature réalisées par le redevable (foyer fiscal) au titre de cette même année* ».

Les plus-values issues des actifs numériques sont, du fait de leur imposition à l'IR, soumises aux prélèvements sociaux. En effet, l'article L. 136-6 du code de la sécurité sociale prévoit que les « *plus-values, gains en capital et profits soumis à l'impôt sur le revenu* » sont soumis à la contribution sociale généralisée (CSG), dont le taux est fixé par l'article L. 136-8 du même code à 9,2 %. L'article 15 de l'ordonnance n° 96-50 du 24 janvier 1996 relative au remboursement de la dette sociale a par ailleurs instauré la contribution pour le remboursement de la dette sociale (CRDS), « *assise sur les revenus du patrimoine désignés aux I et I bis de l'article L. 136-6 du code de la sécurité sociale* », dont le taux est fixé par l'article 19 de la même ordonnance à 0,5 %. Enfin, la loi n° 2018-1203 du 22 décembre 2018 de financement de la sécurité sociale pour 2019 a instauré, à l'article 235 ter du CGI, un « *prélèvement de solidarité sur les revenus du patrimoine mentionnés à l'article L. 136-6 du code de la sécurité sociale* », dont le taux est de 7,5 %. Les plus-values issues des cessions d'actifs numériques sont donc soumises aux prélèvements sociaux à hauteur de 17,2 %.

[18] BOFiP BOI-RPPM-PVBMC-30-20 du 2 septembre 2019, « RPPM - Plus-values sur biens meubles et taxe forfaitaire sur les objets précieux - Cession d'actifs numériques à titre occasionnel - Base d'imposition ».

**En matière d'IR, l'article 200 C du CGI fixe le taux d'imposition des plus-values réalisées à un niveau forfaitaire de 12,8 %, ce qui porte le total de l'impôt pesant sur ces plus-values à 30 %.** L'article 79 de la loi n° 2021-1900 du 30 décembre 2021 de finances pour 2022 a modifié l'article 200 C du CGI pour ajouter la possibilité, pour le contribuable, d'opter de manière irrévocable pour une fiscalisation selon le barème progressif de l'IR à compter du 1er janvier 2023[19].

Le II de l'article 200 C du CGI prévoit deux exceptions :

- les cessions ne dépassant pas 305 € par an sont exonérées ;
- les « *opérations d'échange sans soulte entre actifs numériques* » sont exonérées. Ainsi, tant que les cryptomonnaies sont échangées contre d'autres actifs numériques, la plus-value est placée en sursis d'imposition et n'est taxée que lorsque les actifs numériques acquis sont eux-mêmes cédés.

Le BOFIP précise ainsi que les opérations imposables sont « *les cessions à titre onéreux d'actifs numériques ou de droits s'y rapportant, réalisées à compter du 1er janvier 2019, en contrepartie :*

- *de monnaie ayant cours légal ;*
- *de l'échange d'un bien autre qu'un actif numérique ;*
- *de l'échange avec soulte d'un actif numérique ;*
- *d'un service.* »

La question de la qualification juridique et fiscale des JVC est donc déterminante : si ces jetons sont considérés comme des actifs numériques, alors l'acquisition d'un JVC ne donne pas lieu à fiscalisation de la plus-value réalisée sur les actifs numériques utilisés pour l'acquisition (cryptomonnaies), alors que si les JVC ne sont pas considérés comme des actifs numériques, il y a bien échange entre des actifs numériques (cryptomonnaies) et d'autres biens, donc il y a fiscalisation des plus-values réalisées sur les cryptomonnaies. **Or, l'acquisition d'un JVC ouvrant droit à un bien ou à un service (par exemple une place de concert) pourrait être considérée comme équivalente à l'acquisition de ce bien ou de ce service et donc, donner lieu à fiscalisation de la plus-value.**

Si les JVC étaient considérés comme des actifs numériques, les cas où leur cession serait imposée seraient *a priori* rares. En effet, les JVC sont le plus souvent acquis et cédés contre des cryptomonnaies. Seule une cession « *off chain* », contre une somme de monnaie ayant cours légal sur la base d'un contrat de cession prévoyant le transfert du JVC sur la *blockchain* (sans contrepartie en cryptomonnaie), donnerait lieu à fiscalisation de la plus-value. En cas de cession contre des cryptomonnaies, la plus-value réalisée sur le JVC ne serait imposée qu'au moment de la conversion des cryptomonnaies en monnaie *fiat* (ou au moment de la cession de ces cryptomonnaies contre un bien ou un service).

[19] « *Par dérogation au premier alinéa du présent article, sur option expresse et irrévocable du contribuable, les plus-values mentionnées au même premier alinéa sont retenues dans l'assiette du revenu net global défini à l'article 158. Cette option globale est exercée lors du dépôt de la déclaration prévue à l'article 170, et au plus tard avant l'expiration de la date limite de déclaration.* »

**Encadré 1 : Les régimes fiscaux des cryptoactifs dans le monde**

La France fait office de pionnière en ayant établi, dès 2019, un régime fiscal propre aux cryptoactifs, appelés actifs numériques dans la loi PACTE. Les JVC (incluant les NFT) sont, *a priori*, englobés dans les actifs numériques et ne font pas l'objet d'un traitement spécifique. C'est également le cas dans les autres pays disposant d'écosystèmes Web 3.0 :

- au Portugal, les plus-values réalisées sur des cryptoactifs par des particuliers sont taxées depuis 2023 à un taux de 28 % (ou au taux d'imposition sur le revenu individuel, par consolidation dans le revenu imposable). Avant cette date, le Portugal était considéré comme un « paradis fiscal » pour les cryptoactifs car ceux-ci, considérés comme des moyens de paiement, étaient exemptés de toute imposition. L'exemption demeure aujourd'hui pour les cryptoactifs détenus depuis plus d'un an ;
- en Suisse, le régime fiscal distingue les cryptomonnaies des cryptoactifs. Les cryptomonnaies sont touchées par l'impôt sur la fortune mais les plus-values ne sont pas taxées tant qu'elles s'inscrivent dans un investissement privé occasionnel. Les cryptoactifs comprennent les jetons d'investissement, soumis au régime fiscal des instruments financiers, et les jetons utilitaires (considérés comme des « rapports de mandat »), qui obéissent au même régime que les cryptomonnaies ;
- aux États-Unis, le traitement fiscal des cryptoactifs repose sur une série de directives publiées en 2014 par l'*Internal Revenue Service* (IRS) et sur des dispositions législatives adoptées en 2021. Les plus-values réalisées sur des cryptoactifs par des particuliers sont assimilées à des plus-values sur valeurs mobilières et sont taxées à l'impôt sur le revenu pour les actifs détenus depuis moins d'un an et un barème progressif allant de 0 % à 20 % pour les plus-values de long terme. Les NFT sont aussi considérés comme des valeurs mobilières, sauf quand ils constituent des biens de collection, pour lesquels la plus-value est soumise à un taux plus élevé de 28 % ;
- en Israël, les cryptoactifs sont assimilés à des valeurs mobilières, dont les plus-values sont taxées à un barème allant de 25 % à 30 %. Les NFT ne font pas l'objet d'un traitement spécifique ;
- à Singapour, les cryptoactifs sont considérés comme des valeurs mobilières. Les gains en capital, sur les cryptoactifs comme sur les actifs financiers traditionnels, sont soumis à une imposition nulle dans ce pays.

*Source : Enquête menée auprès des services économiques des ambassades de France au Portugal, en Suisse, aux États-Unis, en Israël et à Singapour.*

### 3.1.3. La mission recommande d'appliquer aux JVC le régime fiscal de leur sous-jacent et de ne pas généraliser le régime des actifs numériques à tous les JVC

L'intégration des JVC dans le régime des actifs numériques présente un avantage majeur, celui de la simplicité : tous les jetons reçoivent le même traitement fiscal, aucune analyse du contenu du jeton n'est nécessaire[20]. Par ailleurs, pour les détenteurs de JVC, le régime est avantageux à plusieurs titres : le taux d'IR est plus faible que celui du régime des biens meubles (*cf.* 3.2), les éventuelles moins-values réalisées sur des JVC peuvent venir en déduction de plus-values réalisées sur d'autres types d'actifs numériques (ou inversement) et les plus-values réalisées sur les JVC ne sont pas fiscalisées tant que les cryptomonnaies reçues à la vente ne sont pas converties en monnaie *fiat*.

[20] Une analyse est néanmoins nécessaire pour déterminer si les jetons peuvent être qualifiés d'instruments financiers, valeurs mobilières ou bons de caisse, dès lors que ces qualifications écartent celle d'actif numérique.

Néanmoins, ce traitement fiscal présente l'inconvénient de faire reposer le régime fiscal non sur la nature de l'objet, mais sur la forme de son support. En effet, de nombreux JVC sont liés à des objets, *a priori* immatériels, sans lesquels les jetons seraient dépourvus de valeur. Ces objets sont soumis au régime des actifs numériques pour le simple fait de leur support (le jeton), alors qu'ils connaîtraient une autre fiscalité en présence d'un autre support. Par exemple, une place de concert a, *a priori*, la même valeur et comporte les mêmes droits, qu'elle prenne la forme d'un billet papier, d'un billet numérique (code-barres dans un courriel, par exemple) ou d'un NFT. Pourtant, ce dernier support emportera une fiscalité spécifique.

**Pour cette raison, la mission recommande de passer à une logique de détermination du régime fiscal applicable selon le sous-jacent du JVC. Dès lors qu'un jeton serait associé à un bien meuble, corporel ou incorporel, son régime fiscal serait celui des biens meubles (*cf.* 3.2), sauf à ce que le bien en question soit régi par un régime spécial, comme celui des objets précieux et œuvres d'art (*cf.* 3.3).**

Une telle solution permettrait d'appliquer le régime fiscal le plus adapté au sous-jacent du jeton, ce qui impliquerait cependant un travail d'analyse au cas par cas et supposerait l'émergence d'une jurisprudence suffisante pour parvenir à établir une architecture globale claire d'imposition des jetons.

Les modalités de passage du régime fiscal actuel au régime fiscal cible de la mission restent à définir. La doctrine fiscale peut rendre publique cette nouvelle pratique afin de donner davantage de sécurité juridique aux acteurs économiques manipulant des JVC. La question de la nécessité de modifier le droit demeure. En effet, la majorité des JVC entrent dans la définition des actifs numériques ; il serait donc contestable, du point de la lettre du droit fiscal, de ne pas leur appliquer le régime fiscal spécifiquement prévu pour les actifs numériques. Il faudrait donc que l'identification d'un actif accessoire (l'actif numérique) et d'un actif principal (le sous-jacent) suffise à justifier un tel écart par rapport au droit pour ne pas avoir à modifier le droit.

La requalification des JVC en vue de leur traitement fiscal se posera, dans tous les cas, au moment de l'entrée en application du règlement européen MiCA (*cf.* annexe V) dans la mesure où celui-ci repose sur des définitions qui ne sont pas celles retenues par le droit français pour le régime des actifs numériques. Le cas particulier des JVC n'est pas traité par le droit interne puisque ces jetons étaient très peu développés au moment du vote de la loi PACTE qui a établi le régime des actifs numériques. Les JVC rentrent dans une définition, donc dans un régime juridique et fiscal, qui n'a pas été pensée pour eux. En revanche, les JVC sont pris en compte dans le règlement MiCA : les jetons non fongibles sont exclus du périmètre du règlement et les jetons utilitaires permettant l'accès à un bien existant ou à un service opérationnel sont soumis à une réglementation allégée (*cf.* section 2.1 de l'annexe V). L'importation des définitions issues du droit européen dans le droit français impliquera nécessairement une refonte du régime fiscal associé aux actifs numériques. Elle pourrait donc constituer une occasion opportune pour clarifier le régime appliqué aux JVC.

**<u>Proposition n° 3</u> : Appliquer aux plus-values réalisées sur jetons utilitaires le régime fiscal de leur sous-jacent, c'est-à-dire celui des biens meubles, et non le régime prévu pour les actifs numériques par l'article 150 VH bis du CGI.**

## 3.2. Le régime fiscal des biens meubles prévoit la taxation des plus-values à un taux de 36,2 %, avec un abattement lié à la durée de détention

Si les JVC ne sont pas considérés comme des actifs numériques (*cf.* 3.1), les plus-values liées à leur cession relèvent du régime des biens meubles incorporels. Le Conseil d'État avait qualifié le bitcoin, avant que le régime des actifs numériques ne soit instauré, de bien meuble incorporel et avait tranché en faveur du régime d'imposition afférent dans une décision de 2018[21].

L'article 150 UA du CGI prévoit un régime de fiscalisation à l'impôt sur le revenu (IR) des plus-values sur les cessions à titre onéreux de biens meubles, réalisées par des personnes physiques, domiciliées en France.

Le même article prévoit les exonérations suivantes :

- les meubles meublants, appareils ménagers et voitures automobiles, sauf s'ils constituent des objets d'art, de collection ou d'antiquité pour lesquels l'option prévue à l'article 150 VL du CGI a été exercée ;
- les actifs numériques (*cf.* 2.2) ;
- les cessions d'un montant inférieur à 5 000 €.

**Les plus-values sont imposées à l'IR selon un taux forfaitaire de 19 %, déterminé par l'article 200 B du CGI.**

Comme les plus-values sur actifs numériques, les plus-values issues des biens meubles sont, du fait de leur imposition à l'IR, soumises aux prélèvements sociaux (*cf*. 3.1.2). **Les prélèvements sociaux auxquels sont soumises les plus-values sur biens meubles s'élèvent donc à 17,2 %, ce qui porte le taux d'imposition total sur ces plus-values à 36,2 %.**

L'article 150 VC du CGI prévoit un abattement de 5 % sur la plus-value brute pour chaque année de détention du bien, au-delà de la deuxième année. L'article 150 VD du CGI précise que les moins-values ne sont pas prises en compte.

Il est à noter que si les JVC sont considérés comme des biens meubles et non comme des actifs numériques, chaque acquisition de JVC avec des cryptomonnaies devra donner lieu à fiscalisation des plus-values réalisées sur ces cryptomonnaies (*cf*. 3.1.2).

## 3.3. Le régime fiscal des œuvres d'art prévoit une taxation à hauteur de 6,5 % du prix de cession

Si le régime fiscal appliqué aux JVC dépend du sous-jacent, alors la question de l'applicabilité du régime fiscal des œuvres d'art se pose, au vu de l'émergence d'un cas d'usage artistique des NFT (*cf.* annexe III).

Le régime fiscal des cessions de métaux précieux, bijoux et objets d'art, de collection ou d'antiquité a été codifié aux articles 150 VI à 150 VM du CGI. Nous bornons notre présentation au cas des objets d'art et de collection, qui sont les seuls auxquels pourraient être assimilés les NFT.

Les cessions d'une valeur inférieure à 5 000 € sont exonérées (art. 150 VJ du CGI). Lorsque la cession n'est pas exonérée, une taxe forfaitaire s'élevant à 6 % du prix de cession est prévue (article 150 VK du CGI).

[21] CE, 26 avril 2018, n° 417809, 418030, 418031, 418032 et 418033, *M. G. e. a.*

À la condition de pouvoir justifier de la date et du prix d'acquisition du bien (afin de pouvoir calculer l'abattement) ou de justifier que le bien est détenu depuis plus de vingt-deux ans, le vendeur peut, en vertu de l'article 150 VL du CGI, opter pour le régime fiscal des cessions de biens meubles de l'article 150 UA du CGI (*cf. supra*).

Par ailleurs, les ventes d'objets d'art sont soumises à la CRDS, en vertu de l'article 17 de l'ordonnance n° 96-50 du 24 janvier 1996 relative au remboursement de la dette sociale. Le taux, fixé par l'article 19 de la même ordonnance, est de 0,5 % et porte sur la même assiette que la taxe forfaitaire.

**Au total, le taux d'imposition des cessions d'objets d'art s'élève donc à 6,5 % du prix de cession**.

L'applicabilité du régime fiscal des œuvres d'art aux NFT est étudiée en section 4.

**Tableau 2 : Comparaison des régimes fiscaux possibles pour les JVC**

| Régime fiscal | Fiscalisation des PV[22] sur les cryptomonnaies utilisées pour l'acquisition du JVC | Fiscalité sur la PV lors de la cession du JVC |
|---|---|---|
| Biens meubles incorporels | Oui[23] (30 %) | 36,2 % de la PV - abattement |
| Actifs numériques | Non | 0 % si la cession se fait contre un autre actif numérique<br>30 % de la PV si la cession se fait contre autre chose |
| Œuvres d'art | Oui[23] | 6,5 % du prix de vente |

*Source : Mission, sur la base du CGI.*

## 4. Les NFT ne pouvant pas être qualifiés d'œuvres d'art, l'application des dispositions fiscales propres à l'art est très limitée

**Les œuvres d'art bénéficiant de régimes fiscaux spécifiques, tant en matière de TVA (*cf.* 2.2) que d'imposition des plus-values pour les particuliers (*cf.* 3.3), la qualification d'œuvres d'art pour des NFT emporte des conséquences fiscales importantes pour leurs détenteurs**.

**La notion d'œuvre d'art n'est pas précisément définie dans le droit français**. Les œuvres d'art, au sens courant du terme, font partie des œuvres de l'esprit protégées par le code de la propriété intellectuelle. Ainsi, l'article L. 112-2 dudit code dispose que « *Sont considérés notamment comme œuvres de l'esprit au sens du présent code :*

*[…]*

*7° Les œuvres de dessin, de peinture, d'architecture, de sculpture, de gravure, de lithographie ;*

*8° Les œuvres graphiques et typographiques ;*

*9° Les œuvres photographiques et celles réalisées à l'aide de techniques analogues à la photographie* ».

[22] Plus-value.

[23] Application du prélèvement forfaitaire unique (30 % des plus-values).

Néanmoins, cette liste n'est pas limitative et la définition des œuvres de l'esprit reste très ouverte, comme l'indiquent les articles L. 111-1 (« *L'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous* ») et L. 111-2 (« *Les dispositions du présent code protègent les droits des auteurs sur toutes les œuvres de l'esprit, quels qu'en soient le genre, la forme d'expression, le mérite ou la destination* »). Les deux seuls critères contribuant à définir une œuvre de l'esprit sont ceux de l'originalité (au sens de création qui traduit des « *choix esthétiques traduisant la personnalité de l'auteur* »[24]) et de forme (la conception de l'auteur doit être réalisée, c'est-à-dire prendre forme).

**La loi fiscale a donc précisé la définition des œuvres d'art auxquelles elle comptait accorder des dérogations**.

En matière de TVA, la définition des œuvres d'art comprise à l'article 98 A de l'annexe III du CGI, transposant la directive européenne sur la TVA, est constituée d'une liste limitative, qui inclut notamment les « *tableaux, collages et tableautins similaires, peintures et dessins, entièrement exécutés à la main par l'artiste* », mais qui n'inclut pas les œuvres numériques[25].

**La définition d'une œuvre d'art en matière de TVA, contrainte par la directive TVA, peut néanmoins différer de la définition retenue en matière d'impôt sur le revenu.** Le BOFIP précise que parmi les objets d'art visés par l'article 150 VI du CGI (régime des plus-values) se trouvent les « *œuvres d'art audiovisuelles sur support analogique ou numérique, ainsi que les biens mobiliers constitutifs de l'installation dans laquelle ils s'intègrent lorsqu'ils font l'objet d'une facturation globale, sous réserve que le tirage de celles-ci soit contrôlé par l'artiste ou ses ayants-droit et limité au plus à douze exemplaires, et qu'elles soient signées et numérotées par l'artiste ou, à défaut, accompagnées d'un certificat d'authenticité signé par lui* »[26]. La définition des œuvres d'art en matière d'IR est donc plus large que celle qui est retenue en matière de TVA. Il reste à savoir si les NFT peuvent entrer dans cette définition, comme le soutiennent leurs promoteurs, qui voient en eux des œuvres d'art audiovisuelles sur support numérique.

Comme le note le rapport du Conseil supérieur de la propriété littéraire et artistique (CSPLA) sur les jetons non fongibles[27], cette vision relève d'un raccourci puisqu'il faut différencier le NFT, inscription dans la mémoire d'un *smart contract* d'un lien vers un fichier numérique et d'une adresse de portefeuille, du fichier numérique vers lequel pointe ce lien, une image le plus souvent. Ni le bien incorporel que constitue le jeton, ni le code informatique ne peut être qualifié d'œuvre d'art. Seul le fichier ressource pourrait éventuellement être qualifié d'œuvre d'art dans la mesure où l'image remplit le critère de création originale.

**Cependant, cette qualification est, dans l'état actuel du droit fiscal, impossible en matière de TVA** dans la mesure où la définition des œuvres d'art présente à l'article 98 A de l'annexe III du CGI exclut les œuvres numériques, caractéristique intrinsèque des NFT.

---

[24] Arrêt de la première chambre civile de la Cour de cassation, 13 novembre 2008, n° 06-19.021.

[25] Seules les photographies *tokenisées* sous forme de NFT pourraient éventuellement rentrer dans le cadre de cette définition, puisqu'elle inclut les « *photographies prises par l'artiste, tirées par lui ou sous son contrôle, signées et numérotées dans la limite de trente exemplaires, tous formats et supports confondus* ».

[26] *Cf.* BOI-RPPM-PVBMC-20-10 du 31 décembre 2018, « RPPM - Plus-values sur biens meubles et taxe forfaitaire sur les objets précieux - Taxe forfaitaire sur les objets précieux - Application de plein droit de la taxe forfaitaire », § 40.

[27] Rapport de la mission sur les jetons non fongibles, « Sécuriser le cadre juridique pour libérer les usages », 2022.

**Le caractère duplicable à l'infini des images numériques semble également irréconciliable avec la définition d'œuvre d'art en matière d'IR** puisqu'une image ne peut satisfaire le critère d'un tirage limité à douze exemplaires maximum. Il n'est pas possible de distinguer l'œuvre originale d'une reproduction en matière de NFT artistiques. Le NFT se borne à identifier le seul « propriétaire » légitime. La jouissance privée de l'œuvre par le « propriétaire » n'est pas différente de celle de n'importe quelle autre personne puisque l'image est facilement et gratuitement accessible en ligne. La seule exclusivité que peut emporter la détention du NFT concerne les droits associés à l'image, comme les droits d'exploitation commerciale, sous réserve que cela ait été explicitement prévu par un contrat de licence (*cf.* section 4 de l'annexe IV).

La cession d'un NFT purement artistique pourrait donc s'apparenter à une cession de droits (et non à une cession de bien) si un contrat de licence le prévoit explicitement, dans les conditions expliquées à la section 4 de l'annexe IV. Dans la mesure où l'article 279 du CGI fait référence aux cessions de « *droits patrimoniaux reconnus par la loi aux auteurs des œuvres de l'esprit* » et non aux droits relatifs à des objets d'art au sens de la directive TVA, les fichiers sous-jacents des NFT artistiques sont qualifiables d'œuvres de l'esprit et la vente de NFT pourrait donc être éligible au taux intermédiaire de TVA sur la cession de ces droits.

Si l'on part de ce principe, les NFT artistiques (associés à des droits) devraient relever du régime fiscal suivant :

- lors de la première vente, puis des reventes éventuelles, vente du NFT soumise au taux intermédiaire de TVA de 10 % sur les cessions de droits – sous réserve que ce taux réduit soit compatible avec les dispositions de la directive TVA (*cf.* 2.2) ;
- lors des reventes entre particuliers, fiscalisation des plus-values réalisées sur les cryptoactifs utilisés pour l'acquisition et application du régime fiscal des plus-values sur biens incorporels, c'est-à-dire 19 % d'IR et 17,2 % de prélèvements sociaux (*cf.* 3.2).

Un NFT artistique dépourvu de contrat et de droits associés ne pourrait pas bénéficier du taux intermédiaire de TVA. Le régime fiscal des reventes entre particuliers reste incertain. En effet, un NFT sans droits n'entre techniquement pas dans la définition des jetons du code monétaire et financier, si bien que le régime des actifs numériques ne peut être appliqué : une taxation en tant que bien incorporel semble probable.

# ANNEXE VII

# L'écosystème français du Web 3.0

# SOMMAIRE

La présente annexe vise à décrire l'écosystème Web 3.0 français et à le restituer dans son environnement international. Son champ couvre l'ensemble des acteurs Web 3.0, y compris les sociétés de finance décentralisée ou les acteurs des cryptomonnaies. En effet, il n'est pas possible statistiquement d'isoler les startups qui relèvent du champ de la mission (les jetons à vocation commerciale) de l'univers général du Web 3.0. En outre, elles reposent sur le même socle de technologies et de compétences que les autres startups du Web 3.0 et la distinction n'est pas pertinente pour apprécier la force de l'écosystème dans son ensemble.

Il convient par ailleurs de relativiser la notion d'écosystème national s'agissant de ces sociétés et de leur environnement. En effet, les équipes sont fréquemment multinationales et des sociétés très jeunes peuvent avoir des implantations variées rendues possibles par des organisations reposant sur le travail à distance. Ainsi Lisbonne regroupe une communauté de développeurs Web 3.0 très dynamique bien que le nombre de sociétés qui y sont effectivement implantées soit limité.

# 1. L'écosystème français du Web 3.0 fait partie des principaux écosystèmes mondiaux mais n'est pas leader

## 1.1. Le développement du Web 3.0 reste dynamique, à l'échelle mondiale, malgré « l'hiver crypto »

Le Web 3.0 continue de se développer, malgré un retournement des marchés à l'automne 2022. Ces technologies se diffusent et de nouveaux projets continuent de voir le jour. À titre d'indicateurs, les téléchargements de librairies de logiciels utilisées pour développer des applications Ethereum (Ether.js, Web3.js, Hardahat et Web3.py) sont en progression de 87 % en 2022 par rapport à 2021, le nombre de « *smart contracts* » déployés sur la chaine Ethereum en 2022 a été multiplié par 4 par rapport à 2021 et le nombre de « *layers 2* » en développement, par 2,5 (chiffres issus du rapport de la société Alechemy.com « Web3 development report » de janvier 2023).

Deux cents fonds spécialisés ont été levés en 2022 et ils ont réuni plus de 30 Md$ à l'échelle mondiale. L'investissement dans les startups en 2022 (31,4 Md$), n'a pas fait apparaitre d'inflexion notable par rapport à 2021 (32,6 Md$)[1].

L'Europe concentre le plus grand nombre de startups (4 000) dans le domaine du Web 3.0 devant les États-Unis (3 400) sur un total de 11 300 recensées dans le monde[2]. En revanche, les États-Unis dominent en termes de sociétés soutenues par des fonds de capital-risque et plus encore en termes de sociétés valorisées plus d'un milliard de dollars lors de leur dernière levée de fonds avec 55 « licornes » contre 14 en Europe.

Les investisseurs d'origine américaine sont très présents en Europe et représentent une part supérieure à celle des acteurs européens (40 % des financements apportés au start-ups européennes contre 32 %). Ils sont plus présents dans le domaine du Web 3.0 que dans leurs investissements en capital risque en général, en Europe. En amorçage, les fonds américains représentent, par exemple, 21 % des financements apportés aux startups européennes du Web 3.0, contre 8 % en général. Pour les séries A, ces chiffres s'élèvent à 29 et 13 %, respectivement[3]. C'est un signe de reconnaissance du dynamise de l'écosystème Web 3.0 européen mais également un point d'alerte quant au faible nombre de fonds présents en Europe spécialisés dans ce secteur.

---

[1] *State of European Crypto startups*. Deal Room et RockawayX. mars 2023

[2] State of European Crypto startups. Deal Room et RockawayX. mars 2023

[3] *State of European Crypto startups*. Deal Room et RockawayX. mars 2023

## 1.2. Les écosystèmes se développent à partir d'une compétence technologique ou d'un cadre réglementaire favorable

La mission a interrogé les services économiques des ambassades de France aux États-Unis, à Singapour, en Israël, en Suisse et au Portugal (*cf*. pièces jointes). Les réponses obtenues font apparaître une distinction entre les écosystèmes bâtis à partir d'une assise technologique et ceux qui se sont appuyés sur un cadre réglementaire.

L'écosystème des États-Unis souffre d'une situation réglementaire particulièrement confuse marquée par l'absence de réglementation fédérale, une concurrence entre régulateurs et la montée des contentieux. Cet environnement instable explique en partie la relative faiblesse des États-Unis dans le domaine du Web 3.0 par rapport à sa puissance technologique et constitue une opportunité pour les écosystèmes alternatifs.

En Europe, la Suisse a pris un ascendant significatif grâce à son cadre réglementaire. Elle s'est dotée à partir de 2020 d'un cadre complet, financier et juridique et l'écosystème bénéficie du soutien du régulateur du secteur financier (FINMA). Le canton de Zoug abrite de nombreux acteurs clés, dont les fondations qui hébergent les principales *blockchains* (notamment Ethereum, Solana, Cardana, Polkadot et la française Thezos). Le pays accueille également les deux principales « crypto banques » européennes, Sygnum et SEBA, agréées par le régulateurs et des prestataires de services essentiels (places de marché, conservation, émetteurs) pour l'écosystème crypto. Avec 1 135 entreprises[4], principalement localisées dans les cantons de Zurich et de Zoug, et 9 licornes, dont 7 développant des *blockchains*, son écosystème est très puissant en Europe.

En Asie, Singapour, à l'instar de la Suisse, souhaite faire de sa place financière l'une des plus avancées en matière de *fintechs*, tout en cherchant à trouver, dans les cryptos, le bon équilibre entre promotion du secteur et régulation de ses acteurs afin de préserver sa réputation de centre financier innovant mais responsable. L'Autorité monétaire de Singapour a introduit en 2020 un régime de licence pour les acteurs proposant des services de paiements en « *DPT* » (« *Digital Payment Tokens* », qui regroupe toutes les cryptomonnaies).

Israël, à l'inverse, n'a mis en place aucune réglementation et son écosystème se développe à partir de l'expertise israélienne dans les technologies numériques et plus spécifiquement la cryptographie. L'expertise technique dérive souvent des formations militaires suivies par les jeunes générations lors du service militaire. Avec l'Institut Weizmann, Israël possède aussi des professeurs et chercheurs ou techniciens de premier plan qui sont à l'origine de nombreuses technologies ayant rendu possible le développement de la crypto (notamment, les briques de base de la *blockchain*). Israël est le siège de plusieurs startups d'envergure mondiale, à la pointe des technologies et de l'infrastructure Web 3.0, dont trois licornes qui jouent un rôle clé dans le développement de ces technologies[5]. Son expertise en fait le siège de nombreuses équipes de développement et de prestataires techniques qui irriguent l'écosystème mondial.

## 1.3. L'écosystème français se situe au troisième rang en Europe

Bpifrance recense 787 sociétés ou projets actifs dans le secteur dans le Web 3.0 au 1er avril 2023 dont 111 startsups ayant levé des fonds auprès d'investisseurs pour un montant total levé de 2,2 milliards d'euros.

---

[4] D'après l'édition 2023 du rapport *CV VC Top 50.*

[5] Fireblocks dans la sécurité et la conservation des actifs numériques, Starkware pour le développement des « layers 2 » et la plateforme d'échanges eToro.

En complément de ces données, la French Tech a transmis à la mission les résultats d'une interrogation de la base de données *Dealroom* dans quatre pays européens recensant les startups actives dans le Web 3.0 ayant réalisé une levée de fonds[6]. La France, avec 80 startups, se situe à un niveau comparable à l'Allemagne (113), devant le Portugal (25) et les Pays-Bas (67) mais loin derrière le Royaume-Unis (337).

La comparaison des montants investis par des fonds de capital risque en 2022 vient conforter cette analyse des positions relatives des différents écosystèmes. En 2002, 1,6 Md$ ont été investis au Royaume-Uni, 1 Md$ en Suisse, 0,5 Md$ en Allemagne et 0,4 Md$ en France[7].

L'écosystème français peut compter sur plusieurs atouts :

- l'importance des entreprises françaises présentes dans les secteurs des jeux vidéo, du luxe et de l'art, qui constituent les principaux cas d'usage des jetons à vocation commerciale (*cf.* annexe III). Ces entreprises ont les moyens financiers et humains de lancer des projets Web 3.0 innovants, potentiellement coûteux, et offrent donc des débouchés aux startups du secteur ;
- sur le plan réglementaire, l'ensemble des acteurs s'accordent à reconnaitre les avantages présentés par la place de Paris. La France a ainsi été parmi les premiers pays à instaurer un cadre réglementaire clair et stable pour les cryptoactifs. Le fait que le règlement européen MiCA s'inspire du cadre réglementaire français renforce cet avantage comparatif : la faculté offerte par la loi PACTE d'obtenir dès aujourd'hui un enregistrement ou un agrément en tant que PSAN permet aux opérateurs d'anticiper l'entrée en application du règlement MiCA. Par ailleurs, la mise en place du cadre réglementaire a acculturé les pouvoirs publics (Autorité des marchés financiers, ministères financiers) aux enjeux du secteur et fait de ceux-ci des interlocuteurs fiables pour les acteurs économiques ;
- l'organisation à Paris de salons et d'événements professionnels d'envergure mondiale, notamment *NFT Paris* et *Paris Blockchain Week*, contribue à la promotion de l'écosystème français et à son développement par la rencontre d'acteurs mondiaux clefs. Ces événements rencontrent un grand succès, y compris auprès du grand public ;
- la compétence des chercheurs et des ingénieurs français en informatique et cryptographie est reconnue.

La mission a également pu constater la qualité et la densité des prestataires de services intervenant en soutien de cet écosystème, notamment les conseils juridiques et cabinets de conseil. Leur développement a été porté par la mise en œuvre de loi PACTE. Les acteurs du secteur se sont structurés autour de deux fédérations professionnelles : l'Association pour le développement des actifs numériques (ADAN) et la Fédération française des professionnels de la *blockchain* (FFPB).

Outre le développement de projets français, ces atouts permettent également d'attirer en France des acteurs étrangers majeurs, comme Binance, Crypto.com ou Circle. Lors de la Binance Blockchain Week 2022, à Paris, Changpeng Zhao, président-directeur général de Binance a ainsi qualifié la capitale française de « hub financier crypto en Europe ».

---

[6] Extraction *Dealroom* réalisée par la French Tech le 31 mars 2023. Deal Room est une base de données centralisant des données publiques telles que les communiqués de presse ou les déclarations de ses clients. Elle reprend essentiellement les investissements de fonds de capital risque. Le recensement Bpifrance est exhaustif et comprend des données qui ne sont pas publiques notamment les investissements de *business angels* ou d'industriels. Ceci explique l'écart en valeur absolue entre les deux séries de données. En revanche, les données *Dealroom* sont collectées de manière homogène au plan géographique et sont pertinentes à des fins de comparaison.

[7] State of European Crypto startups. Deal Room et RockawayX. Mars 2023

Le *European Blockchain Observatory and Forum* a publié en juin 2022 les résultats de son étude comparative de 31 pays européens menée selon deux axes : la maturité réglementaire et la dynamique de l'écosystème. Elle place la France dans le groupe de tête avec la Suisse et le Royaume Uni (*cf.* tableau 1).

**Tableau 1 : Comparaison des écosystèmes**

| | | Maturité réglementaire | | |
|---|---|---|---|---|
| | | Niveau 1 | Niveau 2 | Niveau 3 |
| **Maturité de l'écosystème** | Niveau 1 | Croatie, Grèce, Hongrie, Roumanie, Norvège, Tchéquie | Pologne, Bulgarie | |
| | Niveau 2 | Belgique, Slovaquie, Danemark, Suède, Irlande | Autriche, Finlande, Italie, Espagne, Portugal, Liechtenstein | Allemagne, Luxembourg |
| | Niveau 3 | | Lituanie, Slovénie, Pays-Bas | Chypre, Estonie, Malte, Suisse, France, Royaume-Uni |

*Source : European Blockchain Observatory and Forum, juin 2022.*

Les forces de l'écosystème français du Web 3.0 ne doivent néanmoins pas faire oublier qu'il reste embryonnaire à l'échelle de l'appareil productif français et même du secteur des startups innovantes.

La French Tech recense, à partir des données de *Dealroom*, 21 000 startups en France, à mettre en regard des 787 projets et startups Web 3.0 identifiés par Bpifrance.

Entre 2020 et 2022, les startups du Web 3.0 ont levé en moyenne 0,75 milliard d'euros par an[8], à rapporter aux 10 milliards levés par les startups françaises sur cette période[9] en moyenne par an, soit 7,5 % du total. Il convient de noter que Sorare et Ledger représentent respectivement 45 % et 29 % du montant total levé : une fois ces deux sociétés exclues du total, l'ensemble de l'écosystème Web 3.0 n'a représenté que 1,9 % des levées de fonds en France sur la période. Le succès de ces deux entreprises, qui figurent parmi les dix licornes françaises à la plus forte valorisation, contribue à l'image positive du Web 3.0 français mais masque en partie la faible densité du tissu de startups matures.

Outre Ledger et Sorare, onze startups ont levé plus de 10 millions d'euros, notamment dans le cadre d'une levée de fonds en série A[10]. Parmi celles-ci, Kaiko, Coinhouse, Morpho Labs, Arianee, Zama et Flowdesk sont citées parmi les plus prometteuses. Ceci signifie que très peu d'entreprises ont franchi l'étape de la « preuve de concept ».

Ce constat est cohérent avec les entretiens menés par la mission avec des fondateurs d'entreprises du secteur. À l'exception du domaine de la culture où plusieurs sociétés commercialisent des « œuvres », les projets dans le domaine du jeu, de la mode et du luxe ou de l'identité numérique sont encore en phase de développement.

[8] Extraction *Dealroom* par la French Tech

[9] Ernst and Young : Baromètre EY du capital risque en France – Bilan annuel 2022

[10] Une série A est le premier tour de financement institutionnel qui suit la phase d'amorçage. Il implique de valoriser la société et requiert, en général, un produit mur avec un début de commercialisation.

## 2. Le développement de l'écosystème français pâtit de deux difficultés

### 2.1. Les startups françaises du Web 3.0 ont un accès difficile au compte bancaire

La difficulté à ouvrir un compte bancaire constitue le principal obstacle cité par les acteurs de l'écosystème dans leur développement. Elle tient, d'après eux, au refus d'ouverture de compte par les banques compte tenu de leur lien avec l'univers des cryptomonnaies qui conduit les établissements financiers à refuser l'ouverture de comptes en s'appuyant sur les exigences en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT).

Ces sociétés se tournent alors vers les quelques établissements de petite taille en France, qui, à l'instar de la banque Delubac (qui est enregistrée en tant que PSAN auprès de l'AMF), ont une attitude ouverte vis-à-vis des sociétés du Web 3.0, ou des banques suisses, notamment Sygnum et SEBA, spécialisées dans l'économie du Web 3.0. Cette situation est peu satisfaisante dans la mesure où elle conduit à concentrer les risques de l'écosystème sur un petit nombre d'établissements spécialisés. Le risque de voir les difficultés d'un acteur contaminer l'ensemble de l'écosystème est élevé[11].

Cette question avait été identifiée lors de la préparation de la loi PACTE. L'article L. 312-23 du code monétaire et financier, dans sa rédaction issue du 13° de l'article 85 de la loi PACTE, dispose : « *Les établissements de crédit mettent en place des règles objectives, non discriminatoires et proportionnées pour régir l'accès des émetteurs de jetons ayant obtenu le visa mentionné à l'article L. 552-4, des prestataires enregistrés conformément à l'article L. 54-10-3 et des prestataires ayant obtenu l'agrément mentionné à l'article L. 54-10-5 aux services de comptes de dépôt et de paiement qu'ils tiennent. Cet accès est suffisamment étendu pour permettre à ces personnes de recourir à ces services de manière efficace et sans entraves. Les conditions d'application du présent article sont précisées par décret. Celui-ci précise notamment les voies et délais de recours en cas de refus des établissements de crédit.* ». Ces dispositions ne s'appliquent néanmoins qu'aux PSAN, donc à une fraction limitée de l'univers Web 3.0, qui exclut les startups.

Un groupe de travail du Forum Fintech ACPR-AMF a été constitué mi-2020 sur cette question afin d'établir un état des lieux des problématiques rencontrées et, sur cette base, identifier les pistes possibles d'amélioration. Il a permis le dialogue entre autorités publiques, représentants du secteur des cryptoactifs, du secteur bancaire et des consommateurs. Il a identifié des pistes de réflexions inspirées notamment du dispositif mis en place en Suisse où l'Association suisse des banquiers (ASB) a publié à l'attention de ses membres un guide « *d'ouverture de comptes d'entreprises pour des sociétés blockchain* ».

[11] *Cf.* les faillites de Signature Bank et Silvergate Bank aux États-Unis.

La Fédération bancaire française (FBF) et les banques participantes ont refusé de s'associer aux conclusions du groupe de travail par une note annexée au compte-rendu du groupe de travail : « *les pistes de solutions proposées ne répondent pas aux interrogations du secteur bancaire en termes d'évaluation des risques de LCB-FT présentés par chaque service en actifs numériques ni en termes de surveillance des opérations réalisées par les différents PSAN. Il est rappelé, à cet égard, la nécessité que des lignes directrices soient adoptées par l'ACPR comme le suggère, d'ailleurs, le GAFI*[12] ». Lors de son entretien avec la mission, la FBF a confirmé cette position et mis en avant les appels à la vigilance récurent des régulateurs s'agissant des sociétés réalisant des opérations sur cryptoactifs pour justifier la prudence de ses adhérents en matière d'entrée en relations d'affaires avec les clients Web 3.0. Elle attend une position claire des autorités de régulation.

Les enjeux en matière de LCB-FT concernant les cryptoactifs sont en voie de clarification, avec l'assujettissement des prestataires de services sur cryptoactifs (en anglais, CASP) agréés en vertu du règlement européen MiCA et avec l'extension aux échanges de cryptoactifs du règlement sur les informations accompagnant les transferts de fonds (« *travel rule* », *cf.* section 3 de l'annexe V). La mise en place de cet édifice réglementaire doit constituer une occasion de réunir à nouveau les régulateurs français et le secteur bancaire afin de remédier aux difficultés d'accès au compte bancaire du secteur.

**<u>Proposition n° 10</u> : Renouveler le dialogue entre régulateurs et secteur bancaire afin de garantir l'accès des entreprises du Web 3.0 à un compte bancaire.**

## 2.2. L'absence de fonds d'investissement français ayant la capacité d'investir en jetons freine le développement du secteur et pose un problème de souveraineté

Dans leur phase d'amorçage, le financement des startups de l'écosystème français est suffisamment fourni. En revanche, les fonds français sont absents des levées de fonds institutionnelles à partir de la série A pour des raisons essentiellement réglementaires.

### 2.2.1. Le financement des sociétés Web 3.0 au-delà de la phase d'amorçage repose sur les fonds étrangers

Les startups françaises peuvent s'appuyer sur une communauté dynamique de personnes physiques intervenant en soutien des projets innovants qui sont issues pour la plupart de la communauté des « *early adopters crypto* ». Ces entrepreneurs réinvestissent les plus-values réalisées dans des tours d'amorçage et deviennent *business angels*. Les règles fiscales relatives aux plus-values sur cryptoactifs (pas d'imposition des plus-values tant que les actifs numériques sont échangés contre d'autres actifs numériques, *cf.* annexe VI) peuvent faciliter le réinvestissement par les entrepreneurs dans des émissions de jetons par les startups.

Un tissu d'incubateurs ou de startup studios ayant placé le Web 3.0 au cœur de leur stratégie de sélection de startups s'est également développé et comprend *PyratzLabs*, *Ubisoft entrepreneurs Lab*, l'incubateur de Binance situé à la Station F, *Binance Labs*, ou encore *Moonshot Labs* à Grenoble et l'incubateur iExec-H7 à Lyon.

[12] Compte-rendu des travaux du groupe de travail sur l'accès des prestataires de services sur actifs numériques (PSAN) aux comptes bancaires et sur le fonctionnement des comptes de clients bancaires lors d'achat ou de vente d'actifs numériques. Forum Fintech ACPR-AMF, mars 2021.

## Annexe VII

Le tableau ci-dessous retrace les chefs de file des levées de fonds des startups françaises supérieures à 10 millions d'euros depuis 2021. À l'exception de Flowdesk, Cryptio et la seconde levée de fonds de Coinhouse, toutes ont été structurées par des fonds situés en dehors de l'Union européenne.

**Tableau 2 : Investisseurs des principales levées de fonds de l'écosystème français depuis 2021**

| Société | Montant levé en M€ | Tour | Date | Investisseur chef de file (nationalité) |
|---|---|---|---|---|
| Ledger | 380 | C | 06/2021 | 10T Holding (USA) |
| Sorare | 680 | B | 09/2021 | Softbank, Benchmark (Japon, USA) |
| Sheeldmarket | 10 | A | 10/2021 | Atomico (UK) |
| Coinhouse | 18 | A | 01/2022 | True global ventures (USA) |
| Zama | 43 | A | 02/2022 | Protocol Labs (USA) |
| Arianee | 21 | A | 05/2022 | Tiger Global (USA) |
| Flowdesk | 30 | A | 06/2022 | Eurazéo, Aglae, Isai (FR) |
| Coinhouse | 40 | B | 06/2022 | pool incluant Oddo BHF (FR) |
| Kaiko | 53 | B | 06/2022 | Eight Roads(UK) |
| Cryptio | 10 | A | 06/2022 | Point Nine (DE) |
| Morpho Labs | 18 | A | 07/2022 | A16Z, Variant (UK) |
| Immortal game | 12 | A | 09/2022 | Chernin (USA) |
| Kiln | 18 | A | 11/2022 | Consensys, GSR, Kraken (USA) |
| Ledger | 108 | C | 03/2023 | Extension de juin 2021 (USA) |

*Source : Mission, à partir de l'extraction Dealroom réalisée par la French Tech au 31 mars 2023.*

Les fonds étrangers spécialisés en Web 3.0 sont également très actifs dès la phase de « seed », qui précède la série A au côté des acteurs français :

- White Star Capital est une société de gestion dirigée par une équipe canadienne avec une forte présence en France, dont un bureau à Paris. Elle gère un fonds spécialisé dans l'investissement Web 3.0 ayant investi dans un portefeuille de 19 sociétés au 28 mars 2023 dont 5 en France, au stade de l'amorçage. La France est la première destination des investissements du fonds, soutenu par Bpifrance ;
- Cygni capital, fondé en 2022 par Thomas France, ancien fondateur de Ledger, est basé en Californie mais a réalisé cinq investissements en France, dont la série d'amorçage de *La Collection*. Bpifrance est également investisseur du fonds ;
- Andreessen Horowitz (a16z) et Variant ont investi dans Morpho Labs, startup présente dans le domaine de la finance décentralisée, jugée très prometteuse, lors de sa dernière levée de fonds, en juillet 2022 ;
- les fonds « *corporate* » de Drapper Labs, Consensys, Kraken et plus généralement des acteurs américains de la crypto sont également très actifs en France.

Les gérants français sont également davantage présents dans cette phase d'amorçage qu'en série A. Des fonds d'investissement généralistes investissent dans des sociétés Web 3.0, sans stratégie d'investissement dédiée, comme Alven (*La Collection*), Daphni (*Morpho Labs*), Iris (*Cohort*), Kima Ventures (*Sheelmarket*), Isai (*Arianee*) ou Newfund (*ShareId*), Par ailleurs, trois sociétés de gestion de portefeuille françaises (Aglae Ventures du groupe LVMH, Cathay-Ledger et X Ange) ont la volonté de gérer des fonds dédiés au Web 3.0 et ont ainsi déposé une demande de modification de leur programme d'activité auprès de l'AMF afin de pouvoir investir en jetons (*cf.* 2.2.2).

Bpifrance intervient en soutien de l'écosystème à travers une allocation spécifique (100 M€), engagée à hauteur de 35 M€ et destinée à investir dans les fonds spécialisés dans le Web 3.0 basés en France et à l'étranger[13]. Les fonds étrangers prennent à cette occasion l'engagement de déployer une partie de leurs capitaux en France. Celle-ci n'a pas encore pu se développer en soutien des acteurs français à l'exception des fonds gérés par Xange et Cathay Capital en partenariat avec Ledger.

En effet, les gérants actifs dans le domaine du Web 3.0 et agréés par l'AMF n'ont pas la capacité d'investir dans les jetons émis par les sociétés qu'ils soutiennent en complément d'un apport en numéraire. Cette faculté est essentielle, surtout à partir de la série A, afin de permettre aux fonds de maximiser la rentabilité de leurs investissements et de proposer aux fondateurs des offres de financement compétitives (*cf.* encadré 1). **La résorption de cette difficulté est essentielle pour permettre aux gérants français d'accompagner les startups ayant dépassé la phase d'amorçage avec succès.**

**Encadré 1 : Les spécificités du financement des startups Web 3.0 : les « tokenomics »**

Les startups Web 3.0 peuvent recourir à deux modes de financement : l'émission d'actions nouvelles (*equity*) contre du numéraire ou l'émission de jetons (*tokens*) contre du numéraire. À la différence des actions nouvelles, ces jetons sont liquides peu de temps après leur émission et peuvent comporter des droits de gouvernance sur le protocole développé par la société. À l'inverse, ils ne confèrent aucun droit de propriété sur l'entreprise ou d'accès à la création de valeur liée à la société.

Le financement par l'émission de jetons, appelé *initial coin offering* (ICO) en anglais, a fait l'objet d'un cadre réglementaire dans la loi PACTE (*cf.* section 1 de l'annexe V).

Une transaction comportant des jetons est en général structurée en deux temps. Le financement intervient en amont afin d'apporter la trésorerie nécessaire au développement des logiciels. Les investisseurs reçoivent à cette occasion un engagement (*side letter* ou *simple agreement for future tokens* - SAFT) de la société leur donnant l'option de recevoir, à une date ultérieure, des jetons une fois le logiciel opérationnel.

La valeur des fonds propres et celle des jetons est liée. La question de la répartition des jetons entre les fondateurs, les investisseurs et la communauté d'utilisateurs, ainsi que celle de l'équilibre entre jetons et actions lors d'une levée de fonds ont donné naissance à des techniques d'analyse financière dites « *tokenomics* » (contraction de *token* et *economics*). Les investisseurs visent notamment à travers ces analyses à (i) préserver l'alignement d'intérêt avec les fondateurs et (ii) à maximiser leur accès à la création de valeur dont il peut être difficile de déterminer, *ab initio*, si elle proviendra de l'appréciation de la valeur des fonds propres ou du succès du jeton sur le marché secondaire.

Par ailleurs, les investisseurs et les fondateurs doivent s'accorder, le cas échéant, sur les droits de gouvernance associés aux jetons. Un juste équilibre doit être trouvé entre la centralisation de la détention des jetons et des droits entre les mains des fondateurs, permettant des évolutions rapides du protocole et à l'inverse, un fonctionnement décentralisé plus protecteur des intérêts des parties prenantes, mais qui peut s'avérer difficile à gérer si la détention des jetons est dispersée.

L'investissement dans les startups Web 3.0 nécessite donc :

- un savoir-faire spécifique aujourd'hui peu répandu dans les fonds français ;
- la possibilité pour l'investisseur d'investir en jetons et actions afin d'aligner les intérêts avec les fondateurs et de maximiser la valeur de son investissement.

[13] Cygni, White Star, Blocktower , Sparkle Ventures

### 2.2.2. Les barrières à l'investissement en jetons doivent être surpassées

Les sociétés de gestion de portefeuille (SGP) sont agréées par l'Autorité des marchés financiers (AMF). En application du II de l'article L. 532-9 du code monétaire et financier (CMF), l'AMF vérifie, pour délivrer cet agrément, que la société de gestion « *dispose d'un programme d'activité pour chaque activité ou service qu'elle entend exercer ou fournir, qui précise les conditions dans lesquelles elle envisage d'exercer la gestion des placements collectifs mentionnés au I de l'article L. 532-9 du code monétaire et financier et de fournir les services d'investissement pour lesquels elle est agréée et indique le type d'opérations envisagées et la structure de son organisation* ». Le programme d'activité décrit les instruments financiers susceptibles de constituer le portefeuille des fonds gérés. Toute modification du programme d'activité d'une société de gestion doit être validée par l'AMF.

L'investissement en jetons constituant une nouvelle activité pour une SGP, il doit faire partie des activités mentionnées dans le programme d'activité et ainsi, être validé par l'AMF. Des demandes de modification de programme d'activité ont été déposées par des SGP souhaitant investir en jetons et sont en cours d'instruction par les services de l'AMF. Elles n'ont pas abouti à ce jour mais pourraient connaître une suite favorable prochainement, ce qui devrait permettre à l'écosystème français de bénéficier de davantage de financements.

Deux questions sont soulevées dans le cadre de cet examen :

- la validation du programme d'activité suppose **l'identification des jetons susceptibles de constituer des supports d'investissement éligibles**, lesquels doivent notamment pouvoir être valorisés. Sur ce point, la mission préconise de retenir les jetons assujettis au titre II du règlement MiCA, qui ont fait l'objet de la publication d'un livre blanc, et les jetons constituant des actifs financiers au sens du règlement MiCA. Les jetons non fongibles qui ne sont pas admis à la négociation sur une plateforme réglementée n'auraient pas vocation à être éligibles, de même que les jetons utilitaires ;
- **l'exercice de sa mission par le dépositaire du fonds pose des questions nouvelles**. Les dépositaires[14] d'organismes de placement collectif en valeurs mobilières (OPCVM) et de fonds d'investissement alternatifs (FIA) agréés par l'AMF ont deux missions principales : conserver les actifs détenus par les organismes de placement collectifs (OPC) et s'assurer de la régularité des décisions de l'OPCVM ou du FIA ou de sa société de gestion par rapport aux dispositions législatives et réglementaires applicables ainsi que celles figurant dans son prospectus. Le dépositaire peut choisir de déléguer l'activité de conservation à un tiers appelé le sous-conservateur, cependant, la responsabilité de l'activité de conservation reste de son ressort. Dans l'univers du Web 3.0, la conservation des clés privées du portefeuille de la société de gestion[15] repose sur des prestataires spécialisés implantés en dehors de l'Union européenne[16]. Dans le cadre de sa responsabilité de conservateur, le dépositaire doit, en concertation avec l'AMF, expertiser ces dispositifs de conservation de clés qui présentent des caractéristiques techniques inédites afin de s'assurer de leur sécurité et de leur conformité.

[14] Un dépositaire, selon le lexique de l'AMF, « *est l'intermédiaire à qui le fonds confie la garde des actifs en portefeuille et la supervision des opérations affectant ces actifs* ».

[15] Une société de gestion ne détient pas les « clefs » lui permettant de mouvementer les portefeuilles sous gestion. Ces mouvements, qu'il s'agisse de cryptoactifs ou non, sont effectués par le dépositaire sur instruction de la SGP.

[16] Trois prestataires techniques dominent ce marché : *Fireblocks* en Israël, *Metaco* et *Taurus* en Suisse. Ledger est le seul prestataire européen à proposer une solution de conservation mais sa part de marché est encore marginale.

L'absence d'une solution de conservation de clés cryptographiques française ou européenne dépasse l'enjeu du financement de l'écosystème et doit être analysée au regard des objectifs de souveraineté numérique. **Le fait que la conservation des clés des portefeuilles d'actifs numériques des clients européens s'effectue hors de l'UE[17] constitue une faiblesse majeure de l'écosystème français dans la mesure où elle le rend dépendant d'acteurs extra-européens.**

**<u>Proposition n° 11</u> : Encourager l'émergence d'une solution de conservation française afin de faciliter l'investissement en jetons et de gagner en souveraineté. Une telle mission pourrait être confiée à la Caisse des dépôts et des consignations, qui a développé une expertise en la matière.**

[17] Ne s'applique pas aux clés conservées par leurs propriétaires (solution proposée par Ledger par exemple) mais à toutes les plates formes d'échange qui conservent les clefs de leurs clients (*hosted wallets*).

# Pièces jointes : fiches pays

La mission a interrogé les services économiques des ambassades aux États-Unis, en Israël, au Portugal et en Suisse. Des éléments d'analyse lui ont été fournis sur l'écosystème de chaque pays. Les éléments essentiels sont présentés ci-après.

## 1. États-Unis

**Le développement de l'écosystème des cryptoactifs aux États-Unis s'explique par plusieurs facteurs :**

- l'existence préalable d'un écosystème technologique et entrepreneurial dynamique : la présence, aux États-Unis, d'un écosystème *tech* déjà mature, avec ses filières de financement et des expériences réussies de création d'entreprises d'envergure internationale, a créé un environnement favorable à la création d'entreprises innovantes dans le secteur des *blockchains* et des cryptoactifs ;
- un marché de capitaux profond et sophistiqué : les États-Unis bénéficient des marchés de capitaux les plus développés au monde, avec une chaîne de l'investissement complète et éprouvée et des leaders mondiaux sur chaque étape du financement coté et non coté : *early stage*, accélération, introduction en bourse, marché secondaire ;
- la présence de pôles de recherche universitaire d'excellence, disposant de larges ressources et articulés avec le secteur privé. Le développement des technologies et des projets informatiques profite des importants moyens financiers des universités américaines. Nombre d'entre elles ont développé des incubateurs et accélérateurs d'entreprises technologiques, dont bénéficient certaines entreprises liées à la technologie *blockchain*. L'émergence de profils hybrides de chercheurs-entrepreneurs, souvent moteurs pour le développement des entreprises leaders du secteur, est favorisée par les écosystèmes universitaires américains et par une culture de la prise de risque.

**Au niveau fédéral, en l'absence de législation significative, la réglementation des cryptoactifs repose largement sur l'action des agences de régulation et de l'exécutif.**

Le Congrès tarde à faire émerger une législation sur les cryptoactifs, notamment en raison d'un clivage partisan : certains élus républicains insistent davantage sur les bénéfices économiques de ce développement, quand plusieurs élus démocrates soulignent régulièrement les risques pour la stabilité financière, pour les investisseurs ou les impacts environnementaux des cryptoactifs. Dans ce contexte, plusieurs autorités administratives ont contribué à définir le traitement des cryptoactifs dans leur champ de compétence.

Au niveau fiscal, l'*Internal Revenue Service* (IRS) a publié dès 2014 une série de directives visant à préciser les contours de l'imposition des cryptoactifs. Ce cadre fiscal a été complété par l'adoption, en 2021, de dispositions législatives portant sur la déclaration des transactions de cryptoactifs.

S'agissant des marchés de cryptoactifs, la *Securities and Exchange Commission* (SEC), autorité de régulation des marchés financiers, joue un rôle prépondérant sur le terrain des sanctions. Considérant qu'une majorité des cryptoactifs entrent dans la catégorie des *securities* (titres financiers), elle a engagé plusieurs procédures contre des acteurs liés aux cryptoactifs dont les pratiques contreviennent aux règles applicables aux titres financiers. En février 2023, la SEC a publié une proposition de règle visant à renforcer les exigences applicables aux sociétés de gestion en matière de conservation, visant explicitement à répondre aux défaillances des plateformes de cryptoactifs en matière de protection des encours de leurs clients. La règle étendrait les obligations applicables aujourd'hui aux fonds et titres des clients des sociétés de gestion à un plus grand périmètre d'actifs, incluant les actifs immobiliers, les produits dérivés, les titres de sociétés non cotées et les cryptoactifs. Elle prévoit notamment l'obligation de recourir aux services de conservateurs et de mettre en place une ségrégation des encours.

La *Commodity Futures Trade Commission* (CFTC), régulateur des marchés de dérivés, est également intervenue dans cet espace et revendique un rôle plus important en matière de cryptoactifs. Le bitcoin, principal cryptoactif en circulation, a été qualifié de *commodity* par la jurisprudence américaine, et relève donc de la supervision de la CFTC. Néanmoins, la législation fédérale confie uniquement à la CFTC une compétence de régulation des marchés de dérivés des *commodities*, et non des marchés au comptant (*spot markets*). L'absence de régulateur des marchés de *commodities* au comptant est considérée comme une carence du cadre de la régulation américain.

Au niveau bancaire, *l'Office of the Comptroller of the Currency* (OCC), régulateur des banques, a clarifié les conditions dans lesquelles les banques peuvent proposer des services liés aux cryptoactifs. La Réserve fédérale (Fed) et le département du Trésor se sont également impliqués dans les travaux du *Presidential Working Group* (qui intègre aussi la SEC et la CFTC) sur les *stablecoins*.

Enfin, *le Financial Crimes Enforcement Network* (FinCEN), organe du département du Trésor chargé de la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT), a précisé l'application des dispositions LCB-FT aux acteurs manipulant des cryptoactifs par une série de publications et par une directive consolidée publiée en mai 2019. L*'Anti-Money Laundering Act* de 2020 a par ailleurs confirmé l'intégration des cryptoactifs dans le champ de supervision du FinCEN.

De nombreux États fédérés ont développé ou étudient des législations spécifiques aux cryptoactifs, au premier rang desquels les États de New York et du Wyoming. L'État de New York a été le premier à développer une législation extensive, avec l'introduction en juin 2015 de l'agrément « BitLicense », nécessaire pour exercer des activités liées aux cryptoactifs dans l'État. Le dispositif est toutefois critiqué par des responsables du secteur ou des élus new-yorkais comme étant une procédure lourde et un frein au développement économique. L'État du Wyoming a adopté plusieurs lois visant à offrir un cadre attractif pour le secteur des cryptoactifs. Ce cadre prévoit notamment une licence bancaire spécifique pour les *crypto-banks* et l'enregistrement légal d'organisations autonomes décentralisées (DAO), acteurs importants de la finance décentralisée.

**Aux États-Unis, les NFT ne font pas l'objet d'un cadre réglementaire ou législatif fédéral spécifique, mais des affaires judiciaires en cours de jugement devraient permettre à la jurisprudence de dessiner les contours de leur réglementation**.

Compte tenu de leur nature protéiforme, la classification juridique des NFT comme instruments financiers est incertaine. À l'instar d'autres cryptoactifs, certains NFT font l'objet d'un débat juridique concernant un rattachement à la catégorie des titres financiers (*securities*), supervisés par la SEC, ou celle des commodités (*commodities*), supervisés par la CFTC. La Cour pour le district sud de l'État de New York a notamment déterminé dans un jugement préliminaire en février 2023 que des NFT vendus sur la place de marché *NBA Top Shot* constituent des *securities* et doivent à ce titre être enregistrés auprès de la SEC, mais il n'est pas certain que ce cas d'espèce puisse être étendu à l'ensemble des NFT[18].

En outre, le développement des NFT suscite des litiges concernant l'exercice et la cession des droits de propriété intellectuelle et de reproduction des actifs sous-jacents. En novembre 2022, à la demande de sénateurs du Congrès, *l'US Copyright Office* et *l'US Patent and Trademark Office* (USPTO) ont entrepris des travaux d'étude conjoints sur les questions de droit et de politique de la propriété intellectuelle découlant de l'utilisation des NFT. En effet, le développement des NFT suscite plusieurs difficultés juridiques, qui devront être tranchées et précisées par la jurisprudence, notamment s'agissant de l'usage artistique de marques enregistrées. Si les droits d'usage de marques enregistrées sont encadrés par le *Lanham Act* de 1946, la jurisprudence américaine a de longue date permis leur inclusion dans des œuvres artistiques au nom du premier amendement de la Constitution, garantissant la liberté d'expression. Le 8 février 2023, la société Hermès a obtenu gain de cause dans une affaire l'opposant à l'artiste Mason Rothschild. La société accusait l'artiste d'actes de contrefaçon, d'atteinte à son image de marque et de « cybersquatting » par l'émission et la commercialisation de créations sous forme de NFT reproduisant le célèbre sac « Birkin », arguant que la distribution de NFT est assimilable à un processus commercial classique[19].

[18] *Friel v. Dapper Labs, Inc*., United States District Court for the Southern District of New York, 22 février 2023.

[19] *Hermès Int. v. Rothschild*, United States District Court for the Southern District of New York, 2 février 2023.

## 2. Israël

**La cryptographie et plus généralement la cybersécurité sont des éléments centraux de l'expertise israélienne dans les technologies numériques.** L'expertise technique dérive souvent des formations militaires effectuées lors du service militaire obligatoire. L'innovation et la R&D sont une composante économique essentielle puisqu'environ 5 % du PIB y sont consacrés. Les équipes de développeurs israéliennes sont particulièrement compétentes dans les technologies du Web 3.0 et ont la capacité de mener à bien des projets complexes.

Avec l'Institut Weizmann, Israël possède aussi un vivier de chercheurs de premier plan qui sont à l'origine de nombreuses technologies ayant rendu possible le développement du secteur de la crypto (notamment les briques de base des *blockchains*). Cette institution continue d'irriguer le développement de ce secteur et permet à Israël de rester à la pointe des technologies.

Enfin, en matière d'infrastructures, le pays se dote d'importants centres de données dans lesquels investissent des fonds privés.

**Israël est le siège de plusieurs startups d'envergure mondiale, à la pointe des technologies et de l'infrastructure Web 3.0 :**

- **Fireblocks** est une plateforme de sécurité pour les actifs numériques qui permet aux institutions financières et aux entreprises de gérer en toute sécurité leurs transactions de cryptomonnaies. Elle offre des fonctionnalités telles que la gestion des clés privées, la protection contre les attaques et l'authentification pour garantir la sécurité des actifs numériques. Fireblocks est, avec les suisses Metaco et Taurus, l'un des trois acteurs mondiaux de la conservation d'actifs numériques ;
- **Starkware** est une entreprise spécialisée dans la conception de protocoles de passage à grande échelle de la *blockchain*. Elle offre des solutions de *layer 2* (*cf.* section 4 de l'annexe I) appelées *zero knowledge scalable transparent argument of knowledge* (zK-STARK). Celles-ci permettent d'accélérer les transactions et de réduire les coûts de traitement des données ;
- **eToro** est une plateforme de *trading* en ligne qui permet aux utilisateurs d'investir dans une variété d'actifs et de suivre les stratégies de *trading* d'autres utilisateurs (*social trading*).

Ces plateformes sont toujours en cours de développement et sont considérées comme des licornes.

## 3. Suisse

**D'après l'édition 2023 du rapport *CV VC Top 50*, l'écosystème suisse et liechtensteinois de la « Crypto Valley » regroupe un ensemble de 1 135 entreprises, principalement localisées dans les cantons de Zurich et de Zoug, et emploie près de 5 770 salariés**. Il abrite neuf licornes (valorisées à au moins 1 Md$), dont sept développent des *blockchains* : *Ethereum* (dont la cryptomonnaie éther est la deuxième la plus échangée dans le monde après le bitcoin), *Solana* (considérée comme la principale concurrente d'Ethereum et qui figure parmi les cryptomonnaies les plus valorisées au monde), *Cardano*, *Dfinity* (qui a implanté l'un de ses deux centres de R&D à Zurich), *Web3 Foundation* (qui héberge le protocole Polkadot), *Cosmos* et *Near*. Enfin, la plateforme blockchain Tezos (à laquelle est associée la cryptomonnaie Tez), si elle ne figure plus parmi les licornes suisses, reste une des principales entreprises crypto du pays (sa « fondation » étant domiciliée à Zoug).

**L'écosystème crypto suisse s'appuie également sur des prestataires de services financiers nombreux et puissants :**

- **21.co**, qui gère plus de 3 Md$ d'actifs, propose une palette de 48 produits financiers et emploie une centaine de salariés dans 7 pays ;
- la première banque dédiée aux actifs numérique agréée par la Finma (le régulateur suisse des marchés financiers), **Sygnum**, créée en 2017 et dont la gamme de services comprend, outre l'échange, la conservation et la gestion d'actifs numériques, des activités de prêt, de tokénisation d'actifs et de services bancaires (230 salariés) ;
- le pionnier crypto en Suisse, **Bitcoin Suisse**, créé en 2013, qui propose un ensemble de services dont les principaux sont l'échange et la conservation sécurisée de cryptoactifs ainsi que les prêts collatéralisés (enregistré comme intermédiaire financier auprès de la Finma ; plus de 200 salariés) ;
- le fournisseur de services financiers **Crypto Finance AG**, filiale de l'opérateur boursier allemand Deutsche Börse, dont les activités portent notamment sur les infrastructures de conservation des actifs crypto, le courtage de cryptoactifs et la gestion d'actifs crypto (titulaire d'une licence de gestionnaire d'actifs délivrée par la Finma ; 140 salariés) ;
- la deuxième banque suisse crypto agréée par le régulateur, **SEBA Bank**, fondée en 2018, spécialisée dans le trading, la conservation, les solutions d'investissement, la finance d'entreprise et les services bancaires liés aux cryptoactifs (environ 100 salariés) ;
- la plateforme d'échange d'actifs numériques **SDX** (SIX Digital Exchange), bourse numérique réglementée fonctionnant sur la *blockchain* gérée par l'opérateur de la bourse suisse SIX, qui a été mise en service en novembre 2021.

**Enfin, l'écosystème bénéficie d'un cadre réglementaire à la fois précoce et favorable.** La législation suisse est considérée comme étant l'une des plus avancées au monde en matière de cryptomonnaies, et est perçue comme un atout majeur pour la Crypto Valley. Au cœur de l'Europe, la Suisse présente ainsi une alternative au règlement MiCA de l'UE dont l'entrée en vigueur est attendue en 2024. Elle a été l'un des premiers pays au monde à instaurer des dispositions légales et réglementaires pour la technologie *blockchain* avec :

- la révision de l'ordonnance fédérale sur les banques, entrée en vigueur le 1er août 2017 et qui prévoit l'aménagement d'un « bac à sable réglementaire » (« *sandbox* »), dispositif dérogatoire permettant aux entreprises de tester leur modèle d'affaires en dehors des exigences habituelles de la réglementation bancaire dès lors que les dépôts de leurs clients se situent en dessous du seuil de 1 million de CHF ;
- la création d'une licence fintech (licence bancaire allégée) lors de la révision de la loi fédérale sur les banques, entrée en vigueur le 1er janvier 2019, agrément moins contraignant que la licence bancaire classique ;

- l'adoption de la loi fédérale sur l'adaptation du droit aux développements de la technologie des registres électroniques distribués (TRD) – « loi *blockchain* » – par le Parlement en septembre 2020 (à l'unanimité), pleinement entrée en vigueur le 1er août 2021, ainsi que l'ordonnance qui s'y rapporte. Plutôt que de créer une nouvelle législation *ad hoc*, les autorités suisses ont procédé à une modernisation des règles prévues par une dizaine de loi fédérales existantes, principalement en matière bancaire et financière (y compris en matière de blanchiment d'argent) ainsi qu'en droit des obligations. Ses principaux apports sont :
  - l'établissement d'une base légale au négoce de droits par l'intermédiaire d'une *blockchain* (la fonction des jetons d'investissement ayant la forme de droits-valeurs inscrits dans un registre est assimilée à celle des titres auxquels ils sont adossés et les titres et dérivés « tokénisés » sont traités comme des titres et dérivés classiques) consacrant la sécurité juridique des opérations de « tokénisation » ;
  - la reconnaissance d'un droit à la restitution des jetons aux investisseurs en cas d'insolvabilité ;
  - la création d'une nouvelle catégorie d'autorisation pour les systèmes de négociation fondés sur la *blockchain*, qui a permis la création de la plateforme d'échange d'actifs numériques SDX.

## 4. Portugal

Le Portugal a bâti son attractivité en matière d'écosystème crypto sur son cadre fiscal particulièrement avantageux. Avant le budget de l'État 2023, le Portugal était en effet considéré comme un paradis fiscal pour les utilisateurs de cryptoactifs dont les plus-values étaient exonérées d'imposition. Le caractère totalement dématérialisé de l'activité dans le secteur crypto a ainsi permis à des travailleurs nomades de s'implanter à Lisbonne pour développer leurs projets.

Les nouvelles législations fiscales, en vigueur depuis janvier 2023, prévoient l'imposition des plus-values réalisées sur les cessions de cryptoactifs par des particuliers à hauteur de 28 %. La plus-value est néanmoins exemptée d'imposition si le cryptoactif est détenu depuis plus d'un an. Ces nouvelles règles posent la question de la perte de compétitivité face aux autres pays européens.

Les NFT n'ont pour l'heure pas de cadre règlementaire spécifique.

# ANNEXE VIII

# Lettre de mission

GOUVERNEMENT

*Liberté*
*Égalité*
*Fraternité*

**Annexe VIII**

Paris, le 07 NOV. 2022

Nos références : MEFI-D22-04731

**Madame Catherine SUEUR**
Cheffe de l'Inspection générale des finances

**Objet : levier du développement des actifs numériques à des fins commerciales et dans le domaine des jeux d'argent.**

Le développement rapide des actifs numériques à partir de la technologie de registre distribuée (« *Blockchain* ») est une des principales innovations technologiques, commerciales et financières de la dernière décennie. La France, en précurseur, et bientôt l'Europe, se sont dotées d'un cadre réglementaire et de supervision afin de saisir les opportunités offertes pour notre économie, tout en maîtrisant les risques pouvant naître de ces développements.

Si le cadre réglementaire et de supervision encadrera notamment l'usage des « crypto-actifs » et des actifs numériques correspondant à des titres financiers, le développement rapide des jetons non-fongibles (NFT) et des jetons utilitaires ouvre la voie à de nouveaux usages, suscitant la mobilisation de nombreux acteurs du secteur privé notamment dans le cadre du développement de projets d'application décentralisée (Web3.0). C'est sur cette dernière dimension que nous avons décidé de vous confier la réalisation d'une analyse approfondie.

**Dans une première étape, vous aborderez la problématique spécifique des évolutions de la réglementation des jeux d'argent qui pourraient être requises afin d'accompagner, dans le respect des objectifs de cette réglementation, le développement des usages des actifs numériques et des biens immatériels numériques ou objets immatériels digitaux (NFT, avatars digitaux, metavers...) sous la forme de jeux en ligne.**

Vous tiendrez compte dans votre étude des perspectives de développement de ces usages dans l'activité des opérateurs de jeux d'argent et de hasard.



139 rue de Bercy
75572 Paris Cedex 12

Vous porterez une attention particulière à la pertinence du cadre réglementaire actuel pour permettre le développement de ces activités au regard des risques afférents à ces activités, notamment en termes de lutte contre les addictions, de lutte contre la fraude, et le blanchiment et le financement du terrorisme. Vous examinerez l'existence d'une concurrence avec l'activité d'opérateurs de jeux d'argent et de hasard et, le cas échéant, le respect d'une équité du traitement fiscal de ces activités. Vous vous prononcerez sur l'adéquation de la définition des jeux d'argent aux usages permis par les actifs numériques et autres biens immatériels et, plus généralement, aux évolutions des jeux en ligne.

Après avoir objectivé les difficultés à développer ces activités à cadre législatif et réglementaire inchangé, vous expertiserez l'opportunité et les modalités de mise en place d'un cadre dédié permettant à la France d'être attractive pour le développement des actifs numériques et des biens immatériels numériques ou objets immatériels digitaux (NFT, avatars digitaux, metavers...), tout en assurant l'atteinte des objectifs de la politique des jeux.

**Dans une deuxième étape, vous dresserez un panorama du développement des actifs numériques à vocation commerciale, autres que les « monnaies numériques » et titres financiers**. Vous identifierez à cet égard les usages actuels des jetons non-fongibles, des jetons utilitaires et des jetons de gouvernance et présenterez une cartographie des secteurs d'activité où ces usages sont les plus développés. La localisation respectivement de la production, de la commercialisation et de la base de consommateurs fera l'objet d'une attention particulière.

**Une troisième et dernière étape consistera à formuler des propositions pour soutenir le développement des actifs numériques en maximisant ses retombées pour l'économie nationale.**

Vous examinerez les opportunités de développement des usages de ces actifs numériques. Vous identifierez plus particulièrement les secteurs pour lesquels le développement de l'usage des actifs numériques pourrait représenter à l'avenir un gisement de croissance important pour l'économie française.

Enfin, vous identifierez les orientations de l'évolution souhaitable de la réglementation française et européenne relative aux actifs numériques à vocation commerciale, les obstacles au développement de leur usage et ce qui pourrait au contraire le favoriser (comme des efforts de standardisation). Votre analyse couvrira notamment le régime juridique et fiscal de ces actifs, le droit des données personnelles, la protection du consommateur et les questions d'impact environnemental et de concurrence.

Vous pourrez solliciter, pour l'ensemble de vos investigations, la direction générale du Trésor, y compris ses services économiques régionaux à l'étranger, la direction générale des Entreprises, la direction du Budget, la direction de la Législation fiscale, la direction générale de la Concurrence, de la Consommation et de la Répression des fraudes et les autres directions et services des ministères concernés ainsi que leurs établissements publics. Sur le premier volet de vos travaux, vous consulterez également l'Autorité nationale des jeux.

Vos conclusions sur la première étape nous seront remises à la fin du mois de décembre. Vos conclusions sur les deuxième et troisième étapes sont attendues pour la fin du mois d'avril.

**Bruno LE MAIRE**
Ministre de l'Économie,
des Finances et de la Souveraineté
industrielle et numérique

**Gabriel ATTAL**
Ministre délégué chargé des
Comptes publics

**Jean-Noël BARROT**
Ministre délégué chargé de la Transition
numérique et des Télécommunications

# ANNEXE IX

## Liste des personnes rencontrées

# SOMMAIRE

# 1. Cabinets ministériels

## 1.1. Première ministre

- M. Schwan Badirou-Gafari, conseiller chargé des services financiers ;
- M. Matthieu Landon, conseiller chargé de l'industrie, de la recherche et de l'innovation ;
- M. Antoine Mory, chef du pôle *culture* ;
- Mme Magali Valente, conseillère chargée de la culture.

## 1.2. Ministre de l'économie, des finances et de la souveraineté industrielle et numérique

- M. Antonin Dumont, conseiller chargé du financement de l'économie ;
- M. Étienne Floret, conseiller chargé de l'innovation, des PME, du numérique, du sport et de l'économie sociale et solidaire.

## 1.3. Ministre délégué chargé de la transition numérique et des télécommunications

- M. Renaud Vedel, directeur de cabinet ;
- M. Maxime Donadille, conseiller chargé des technologies d'avenir ;
- M. Hugo Lévy-Heidmann chargé de l'économie numérique et du financement de l'innovation.

## 1.4. Ministre délégué chargé des comptes publics

- M. Clément Larrauri, conseiller chargé de la fiscalité, de la douane et de la lutte contre la fraude.

## 1.5. Ministre de la culture

- M. Raphaël Coulhon, conseiller chargé de l'enseignement supérieur, de l'innovation, du numérique et du jeu vidéo.

# 2. Administrations centrales

## 2.1. Ministères économiques et financiers

### 2.1.1. Direction générale du trésor

- M. Rodolphe Baroukh, adjoint au chef de bureau de l'épargne et des marchés financiers (FINENT1) ;

- M. Bastien Lafon, adjoint au chef de bureau des services bancaires et des moyens de paiement (BANCFIN4) ;
- M. David Sabban, adjoint au chef de bureau des services bancaires et des moyens de paiement (BANCFIN4) ;
- M. Arthur Frappereau, adjoint chargé des évolutions technologiques au pôle affaires internationales coordination européenne et enjeux technologiques du secteur financier (PAIET).

### 2.1.2. Direction du budget

- M. Alexandre Grosse, adjoint à la directrice, chef de service ;
- M. Jalal Froug, chef du bureau des recettes (1BR) ;
- Mme Caroline Baud, adjointe au chef de bureau des recettes, chargée de la régulation des jeux d'argent et de hasard.

### 2.1.3. Direction générale des entreprises

- M. Aurélien Palix, sous-directeur des réseaux et des usages numériques ;
- Mme Marie-Liane Lekpeli, directrice du projet *numérique responsable et sécurité* ;
- M. Nicolas Desruelles, chef du projet *Next40/FT120* à la mission *French Tech*.

### 2.1.4. Direction générale de la concurrence, de la consommation et de la répression des fraudes

- M. Pierre Chambu, chef du service de la protection des consommateurs et de la régulation des marchés ;
- M. Rémy Slove, directeur de cabinet du directeur général ;
- Mme Nadine Mouy, sous-directrice des services, des réseaux et du numérique (SD6) ;
- Mme Juliette Roth, adjointe au chef de bureau des services financiers et professions réglementées (6C) ;
- Mme Fatou Diallo, cheffe du service national des enquêtes ;
- M. Fabrice Berthier, chef de service au service national des enquêtes ;
- M. Guillaume-Arnaud Grasset, enquêteur.

### 2.1.5. Direction générale des finances publiques — direction de la législation fiscale

#### *2.1.5.1. Sous-direction de la fiscalité directe des entreprises (B)*

- M. Aulne Abeille, sous-directeur.

#### *2.1.5.2. Sous-direction de la fiscalité des personnes (C)*

- Mme Marie-Astrid de Barmon, sous-directrice ;
- M. Frédéric Parrenin, adjoint au chef du bureau de la fiscalité du patrimoine et de l'épargne (C2) ;
- M. Benoît Kointz, chef de section au bureau C2 ;

- M. Joachim Sessar, rédacteur au bureau C2.

#### *2.1.5.3. Sous-direction de la fiscalité des transactions, de la fiscalité énergétique et de la environnementale (D)*

- M. Matthieu Deconinck, sous-directeur ;
- M. Vincent Petit, chef du bureau de la taxe sur la valeur ajoutée ;
- M. Serge Korno, chef de section au bureau de la taxe sur la valeur ajoutée.

### 2.1.6. Service à compétence nationale TRACFIN

- M. Alban Genais, adjoint au directeur.

## 2.2. Ministère de la culture

### 2.2.1. Secrétariat général du ministère de la culture

- M. Romain Delassus, chef du service du numérique ;
- Mme Anne-Laure Janeczek, directrice de projet au service du numérique.

### 2.2.2. Direction générale des patrimoines et de l'architecture

- Mme Christèle Creff, adjointe au directeur général, cheffe du service des musées de France ;
- Mme Anne Dubile, adjointe au chef de bureau du pilotage des musées nationaux.

## 2.3. Ministère de la justice – direction des affaires civiles et du sceau

- Mme Catherine Raynouard, cheffe de service, adjointe au directeur.

## 2.4. Ministère de la santé – direction générale de la santé

- Mme Élise Riva, cheffe du bureau de la prévention des addictions (SP3) ;
- M. Sylvain Guého, adjoint au chef du bureau SP3 ;
- Mme Lorenza Luciano, bureau SP3.

## 2.5. Ministère de l'intérieur – direction générale de la police nationale

- M. Stéphane Piallat, chef du service central des courses et jeux (SCCJ) ;
- M. Nicolas Rocher, chef de la division de la surveillance générale des casinos et des cercles ;
- Mme Catherine Miossec, division des courses ;
- M. Nicolas Morin-Aristin, division des courses.

# 3. Autres autorités publiques

## 3.1. Commission européenne

- M. Rok Žvelc, conseiller juridique à la direction générale de la stabilité financière, des services financiers et des marchés de capitaux (DG FISMA);
- M. Peter Kesrtens, conseiller.

## 3.2. Autorités administratives indépendantes et autorités publiques indépendantes

### 3.2.1. Autorité des marchés financiers

#### *3.2.1.1. Direction de l'innovation et de la finance numérique*

- M. Charles Moussy, directeur de l'innovation et de la finance numérique ;
- Mme Juliette Le Drogou, *policy officer*.

#### *3.2.1.2. Direction de la gestion d'actifs*

- M. Alexis Charciarek, chargé senior.

#### *3.2.1.3. Direction des marchés*

- M. Pierre Subiger, expert juridique et international.

#### *3.2.1.4. Direction des affaires juridiques*

- Mme Laure Colli-Patel, adjointe au directeur des affaires juridiques, chargée de la gestion et des services d'investissement ;
- M. Clément Saudo, adjoint au directeur des affaires juridiques, chargé des marchés ;
- Mme Océane Margaron, juriste (pôle affaires) ;
- M. Benjamin Tubiana, juriste (pôle des opérations et de l'information financière) ;

### 3.2.2. Autorité de contrôle prudentiel et de résolution

- M. Olivier Fliche, directeur du pôle *fintech et innovation* ;
- M. Laurent Camus, expert au pôle *fintech et innovation*.

### 3.2.3. Commission nationale de l'informatique et des libertés

- M. Bertrand Pailhès, directeur des technologies et de l'innovation ;
- Mme Amandine Jambert, ingénieure experte en protection de la vie privée et sécurité des systèmes d'information.

#### 3.2.4. Autorité nationale des jeux (ANJ)

- Mme Isabelle Falque-Perrotin, présidente ;
- M. Rémi Lataste, directeur général ;
- M. Frédéric Guerchoun, directeur juridique ;
- M. Guillaume Labordière, analyste chargé des questions économiques ;
- Mme Florence Lascoux, chargée de mission.

## 4. Organisations professionnelles du secteur du Web 3.0

#### 4.1.1. Association pour le développement des actifs numériques (ADAN)

- Mme Faustine Fleuret, présidente ;
- Mme Mélanie Ambroise, directrice de la stratégie et des relations institutionnelles ;
- M. Frédéric Montagnon, président du comité « NFT » ;
- M. Cédric Pavao, rapporteur du groupe de travail sur la fiscalité des actifs numériques.

#### 4.1.2. Fédération française des professionnels de la *blockchain* (FFPB)

- M. Rémy André Ozcan, président ;
- Mme Gaëlle Marraud des Grottes, secrétaire générale.

## 5. Organismes financeurs et conseils en affaires

### 5.1. Fédération bancaire française

- Mme Solenne Lepage, directrice générale adjointe ;
- M. Dominique Rouquayrol de Boisse, directeur juridique et de la conformité.

### 5.2. Banque publique d'investissements (BPIFrance)

- Mme Adeline Lemaire, directrice exécutive des fonds de fonds ;
- M. Yoann Caujolle, directeur d'investissement et du pôle *Développement* ;
- Mme Véronique Jacq, directrice du pôle *Digital Venture* ;
- M. Ivan de Lastours, responsable *blockchain & crypptos*.

### 5.3. Caisse des dépôts et consignations (CDC)

- Mme Nadia Filali, directrice des programmes *blockchain* et pilote de LaBChain ;
- M. Grégory Chenue, adjoint à la directrice des programmes *blockchain* ;
- Mme Roxane Faure, cheffe de projets *blockchains & cryptoactifs* ;
- M. Bastien Voituriez, expert en *blockchains* et cryptoactifs.

## 5.4. Fonds d'investissement

### 5.4.1. Benchmark Capital

- M. Peter Fenton, *general partner*.

### 5.4.2. Daphni

- M. Charles-Henri Tranié, *managing partner* ;
- M. Stanislat Lot, *partner*.

### 5.4.3. New Fund

- M. François Véron, fondateur.

### 5.4.4. Avolta Partners

- M. Philippe Rodriguez, co-président, fondateur.

### 5.4.5. Aglaé Ventures

- M. Cyril Guenoun, directeur général ;
- M. Antoine Loison, *partner*.

### 5.4.6. Cygni Capital

- M. Thomas France, directeur général, fondateur.

### 5.4.7. Cathay Capital

- Mme Marguerite de Tavernost, vice-présidente de Cathay Innovation.

### 5.4.8. XAnge

- M. Luc Jodet, *partner* chargé du secteur du Web 3.0.

## 5.5. Incubateurs

### 5.5.1. PyraTzLabs

- M. Bilal El Alamy, co-fondateur, président ;
- Mme Houda Leroy, directrice des opérations.

#### 5.5.2. The Family

- M. Nicolas Colin, co-fondateur, directeur général.

### 5.6. Cabinets de conseil et agences

#### 5.6.1. Wagmi Studio

- M. Jean-Nicolas Hinard, co-fondateur ;
- M. Jérémie Barthés, co-fondateur.

#### 5.6.2. Bary

- M. Mathias Cohen Scali, co-fondateur.

#### 5.6.3. Indépendants

- Mme Claire Balva, conseillère indépendante, co-fondatrice de Blockchain Partner.

## 6. Juristes et professions juridiques

### 6.1. Universitaires

- M. Thibault Douville, professeur des universités à l'université de Caen-Normandie, co-directeur de l'institut caennais de recherche juridique ;
- Mme Amélie Favreau, maîtresse de conférences habilitée à diriger des recherches à l'université Grenoble-Alpes (UGA).

### 6.2. Cabinets d'avocats

#### 6.2.1. Cabinet Kramer Levin

- M. Hubert de Vauplane, avocat associé ;
- M. Victor Charpiat, avocat associé ;
- Mme Mathilde Carle, *counsel* ;
- Mme Morgane Fournel Reicher, juriste ;
- Mme Laëtitia Rebouh, juriste.

#### 6.2.2. Cabinet ORWL

- M. William O'Rorke, avocat associé ;
- M. Alexandre Lourimi, avocat associé.

#### 6.2.3. Skadden, Arps, Slate, Meagher & Flom LLP

- M. François Barrière, *French Counsel*, professeur des universités.

#### 6.2.4. Cabinet Osborne Clarke

- Mme Dorothée Chambon, associée.

#### 6.2.5. Cabinet Odoné

- Mme Joanna Masson, avocate indépendante.

#### 6.2.6. Cabinet Gide Loyrette Nouel

- M. Julien Guinot-Deléry, associé ;
- M. Franck Guiader, conseil scientifique, directeur de l'équipe Gide 255 ;
- M. Matthieu Lucchesi, *counsel* ;
- M. John Le Guen, consultant ;
- M. Luc Colin, collaborateur.

### 6.3. Officiers publics et ministériels et leurs représentants

#### 6.3.1. Conseil supérieur du notariat

- M. Stéphanie Jeanjean-Boudon, secrétaire du bureau du CSN ;
- M. Jérôme Fehrenbach, directeur général ;
- M. Christian Revelli, directeur des systèmes d'information.

#### 6.3.2. Conseil national des greffiers de tribunaux de commerce

- M. Thomas Denfer, président.

## 7. Aspects techniques transversaux relatifs aux *blockchains*

### 7.1. Universitaires

- M. Pablo Rauzy, maître de conférences en informatique à l'université Paris-VIII ;
- M. Georges Gonthier, chercheur *senior* à l'institut national de recherche en informatique et automatique (INRIA).

## 7.2. Entreprises spécialisées dans les infrastructures techniques et financières du Web 3.0 et de la *blockchain*

### 7.2.1. Ledger

- M. Michael Louzado, vice-président chargé de la stratégie et des fusions-acquisitions ;
- M. Seth Hertlein, directeur international des affaires institutionnelles ;
- M. Julien Nivot, directeur des affaires réglementaires.

### 7.2.2. Aleph.im

- M. Jonathan Schemoul, président, fondateur.

### 7.2.3. Binance France

- Mme Stéphanie Cabossioras, directrice générale adjointe ;
- Mme Julia Fenart, responsable des relations institutionnelles.

### 7.2.4. BubbleMaps

- M. Nicolas Vaiman, cofondateur et directeur général.

# 8. Secteur des jeux

## 8.1. Entreprises du secteur des jeux à objets numériques échangeables

### 8.1.1. Sorare

- M. Nicolas Julia, co-fondateur et président-directeur général ;
- M. Thibaut Predhomme, chef du cabinet du président-directeur général ;
- Mme Gabrielle Dorais, directrice juridique ;
- Mme Sandy Arkwright, directrice juridique adjointe ;
- M. Jean-François Vilotte, associé chez De Gaulle Fleurance Associés, conseil juridique de Sorare.

### 8.1.2. Metafight

- Mme Julia Mahé, co-fondatrice ;
- M. Thomas Chauveau, co-fondateur.

### 8.1.3. Dogami

- M. Bilal El Alamy, co-fondateur ;
- M. Adrien Magdelaine, co-fondateur ;

- M. Paul Adler, directeur de cabinet des co-fondateurs.

#### 8.1.4. Sandbox

- M. Sébastien Borget, co-fondateur et *chief operation officier*, président de la *Blockchain Gaming Alliance*.

### 8.2. Entreprises du secteur des jeux d'argent et leurs représentants

#### 8.2.1. Association française des jeux en ligne (AFJEL)

- M. Emmanuel de Rohan Chabot, président ;
- Mme Juliette de la Noue, porte-parole.

#### 8.2.2. La Française des Jeux (FDJ)

- Mme Stéphane Pallez, présidente-directrice générale ;
- M. Charles Lantieri, directeur général délégué ;
- M. Jonathan Gindt, directeur de cabinet de la présidente-directrice générale ;
- M. Raphaël Botbol, directeur de la stratégie ;
- Mme Marion Hugé, directrice de la régulation et des affaires publiques.

#### 8.2.3. Pari mutuel urbain (PMU)

- M. Martial Houlle, secrétaire général ;
- M. Régis Bourgueil, directeur de cabinet de la directrice générale ;
- M. Constantin Garreau, directeur de l'innovation.

### 8.3. Entreprises du secteur des jeux vidéo et leurs représentants

#### 8.3.1. Syndicat national du jeu vidéo (SNJV)

- M. Lévan Sardjevéladzé, président ;
- M. Julien Villedieu, directeur général.

#### 8.3.2. Syndicat des éditeurs de logiciels de loisirs (SELL)

- M. Nicolas Vignolles, directeur général ;
- M. Julien Morel, consultant chez Lysios, conseil en affaires publiques du SELL.

#### 8.3.3. Ubisoft

- M. Emmanuel Martin, directeur des affaires institutionnelles ;
- Mme Virginie Gringarten, juriste ;

- M. Guillaume Tormo, juriste ;
- M. Nicolas Pouard, responsable des initiatives *blockchain innovation lab*.

### 8.4. Personnalités qualifiées

- M. Mario Blaise, psychiatre, addictologue, ancien membre du collège de l'ANJ ;
- M. Marc-Olivier Crisan, développeur de jeux vidéo.

## 9. Secteur de la culture et des arts

### 9.1. Entreprises Web 3.0 du secteur de la culture et des arts

#### 9.1.1. Pianity

- M. Kévin Primicerio, fondateur, directeur général ;
- M. Maxime Ubeda, directeur financier.

#### 9.1.2. EverRose

- Mme Lyne Stambouli, co-fondatrice, présidente ;
- M. Erwan Breuil, co-fondateur ;
- Mme Élizabeth Le Hot, diretrice des opérations.

#### 9.1.3. LaCollection

- M. Jean-Sébastien Beaucamps, co-fondateur ;
- M. Fabian Langlet, co-fondateur.

#### 9.1.4. Logical Pictures – Cascade8

- M. Frédéric Fiore, co-fondateur, président de LogicalPictures ;
- Mme Yannick Bossenmeyer, co-fondatrice, directrice générale de Cascade8.

#### 9.1.5. Exposure Arts – Rhapsody Curated

- M. Julien Zanet, président-directeur général ;
- M. Pierre Élie de Pibrac, directeur de la création ;
- M. Édouard Brossette, directeur technique.

#### 9.1.6. Billy

- M. Robin Champseix, cofondateur, directeur général.

## 9.2. Établissements publics du secteur de la culture et des arts

### 9.2.1. Centre des monuments nationaux

- Mme Valérie Senghor, directrice générale adjointe.

### 9.2.2. Centre national du cinéma et de l'image animée (CNC)

- Mme Pauline Augrain, directrice adjointe du numérique.

### 9.2.3. Établissement public du musée du Louvre

- M. Kim Pham, administrateur général ;
- Mme Aline François, directrice des expositions et des éditions ;
- M. Pierre-Emmanuel Fournier, sous-directeur du mécénat et de partenariats.

### 9.2.4. Centre national d'art et de culture Georges-Pompidou

- M. Xavier Rey, directeur du musée national d'art moderne – centre de création industrielle ;
- Mme Marcella Lista, cheffe du service des nouveaux médias ;
- M. Philippe Benaïche, directeur des systèmes d'information et de télécommunication.

### 9.2.5. Opéra national de Paris

- M. Martin Ajdari, directeur général adjoint ;
- M. Éric Grébille, adjoint au directeur du développement.

### 9.2.6. Musée Granet d'Aix-en-Provence

- Mme Paméla Grimaud, conservatrice du patrimoine, responsable du pôle *recherche et conservation* ;
- Mme Delphine Ract-Madoux, consultante en ingénierie culturelle.

## 9.3. Autres organisations rencontrées

### 9.3.1. Société des auteurs, compositeurs et éditeurs de musique (SACEM)

- Mme Cécile Rap-Veber, directrice générale ;
- M. Julien Dumon, directeur du développement, du phono et du numérique ;
- M. Julien Lefebvre, responsable de la stratégie digitale et de l'innovation.

### 9.3.2. Christie's

- M. Devang Thekkar, directeur de *Christie's Venture*.

### 9.4. Personnalités qualifiées

- Mme Pauline Hot, maîtresse des requêtes au Conseil d'État, rapporteresse de la mission du conseil supérieur de la propriété littéraire et artistique (CSPLA) sur les jetons non fongibles remis le 12 juillet 2022 ;
- M. Jean-Marc Pailhon, collectionneur de NFT.

## 10. Secteur de la consommation, du luxe et de la logistique

### 10.1. Entreprises spécialisées dans le Web 3.0

#### 10.1.1. Arianee

- M. Frédéric Montagnon, président, co-fondateur ;
- M. Pierre-Nicolas Hurstel, directeur général, co-fondateur ;
- Mme Juliane Dessard Jacques, directrice juridique.

#### 10.1.2. GoodsID

- M. Loÿs de la Soudière, président, cofondateur.

#### 10.1.3. *FanPrime*

- M. David Lozano, cofondateur, directeur general.

#### 10.1.4. Ownest

- M. Quentin de Beauchesne, cofondateur.

### 10.2. Autres entreprises

#### 10.2.1. Carrefour

- Mme Hélène Labaume, direction de l'innovation.

#### 10.2.2. Kering

- M. Grégory Boutté, directeur de la clientèle et du numérique.

#### 10.2.3. LVMH

- M. Pierre-Frédéric Rémi, directeur du financement et de la trésorerie du groupe ;
- Mme Nelly Mensah, vice-présidente chargée de l'innovation numérique, directrice des cryptoactifs et du métavers ;

- M. Pierre-Éric Coquard, responsable du département de la fiscalité ;
- Mme Margot Legent, département de la fiscalité.

#### 10.2.4. L'Oréal

- Mme Camille Kroely, *chief metaverse officer* ;
- Mme Hanissa Chouchou, directrice financière.

#### 10.2.5. Décathlon

- M. Valentin Auvinet, *chief metaverse officier* ;
- Mme Stéphanie Attias, responsable de la conformité réglementaire pour le numérique.

#### 10.2.6. Lacoste

- M. Benjamin Blamoutier, vice-président *global brand & customer experience*.

### 10.3. Personnalité qualifiée

- Mme Virginie Beaumeunier, inspectrice générale des finances, ancienne directrice générale de la concurrence, de la consommation et de la répression des fraudes.

## 11. Secteur de l'identité numérique

### 11.1. Archipels

- M. Hervé Bonazzi, fondateur, directeur général.

### 11.2. Synaps

- M. Florian Le Goff, président.

### 11.3. ShareID

- Mme Sara Sebti, cofondatrice, directrice générale.

## 12. Autres personnalités qualifiées

- M. Pierre Person, ancien député de la 6e circonscription de Paris ;
- M. Robert Ophèle, président de l'autorité des normes comptables, ancien président de l'autorité de contrôle prudentiel et de résolution (ACPR), ancien président de l'autorité des marchés financiers (AMF) ;
- M. François-René Burnod, auditeur au Conseil d'État, auteur du rapport particulier *le cadre juridique de la TVA* pour le conseil des prélèvements obligatoires (CPO) en 2023 ;
- M. Yorick de Mombynes, conseiller référendaire à la Cour des comptes.

# PIÈCE JOINTE

## Support de présentation de la mission

MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA SOUVERAINETÉ
INDUSTRIELLE ET NUMÉRIQUE

*Liberté*
*Égalité*
*Fraternité*

# Mission sur les jetons commerciaux

Mai 2023

Inspection générale des finances

Plan de la présentation

## 1. Les JVC : cas d'usage

## 2. Les problématiques juridiques liées au développement des JVC

## 3. L'écosystème français

1. Cas d’usage

# LES JETONS À VOCATION COMMERCIALE (JVC) : DÉFINITIONS, CARACTÉRISTIQUES, CAS D’USAGES

# Les jetons à vocation commerciale (JVC) : définition

**Les JVC se distinguent :**

- des jetons fongibles ayant vocation à servir de monnaie d'échange ou de réserve de valeurs : *crypto-monnaies, stable coins, jetons de monnaie électronique*
- des jetons équivalents au plan économique à des titres financiers : *security tokens*
- des jetons émis dans la perspective de donner accès à un service futur et dont le produit d'émission finance le développement : *jetons de levée de fonds ou ICO*

**Les JVC peuvent être identifiés par un faisceau d'indices :**

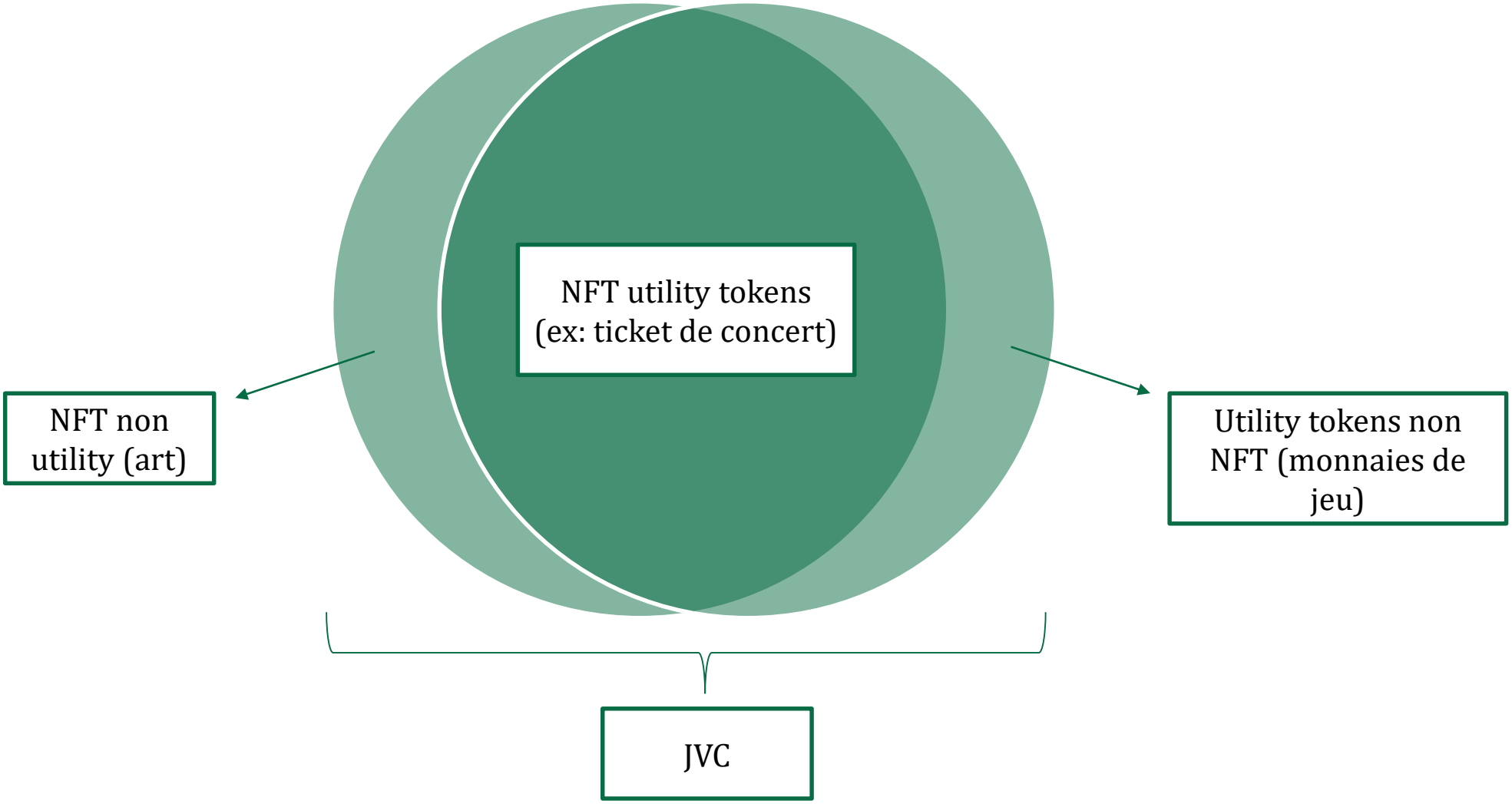
- proposés à des particuliers
- associés à des droits d'accès à des biens ou des services existants : *jetons utilitaires*
- ou bien « nus » c.à.d dépourvus de droits associés mais qui ont un valeur ostentatoire : *NFT artistiques ou de collection*
- généralement non fongibles d'un point de vue technique mais ils peuvent l'être (monnaie de jeu)
- ce sont donc, pour l'essentiel, les **NFT** et les **jetons utilitaires** au sens du règlement MiCA

**Les JVC ont une vocation commerciale et non financière.**

**Ils doivent être régulés comme les biens de consommation.**

# Les jetons à vocation commerciale (JVC) : définition





# Les caractéristiques des jetons à vocation commerciale

**Les JVC constituent des codes informatiques associés à un « portefeuille » sur une *blockchain* (*cf*. annexe) :**

- ces jetons peuvent permettre d'accéder à un service numérique (logiciel, jeu, réseau social…)
- ou contenir un lien vers des données stockés hors de la *blockchain* (image, documents…)

**Le jeton est souvent « l'accessoire » d'un « principal » (sous-jacent) :**

- sans association avec un service ou des données, le jeton n'est qu'un code informatique sans valeur
- le jeton n'apporte aucune garantie quant à la substance ou à la pérennité de son « principal »

**Les promesses de « rareté », « propriété » et « interopérabilité » sont ténues :**

- la *blockchain* retrace effectivement les détenteurs de jetons de manière infalsifiable créant une *« propriété »* et permettant les échanges entre portefeuilles, **mais la détention du jeton ne garantit pas la consistance du principal**
- la *« rareté »* apparaît **si et seulement si** l'accès au « principal » du jeton, définit hors *blockchain*, est associé de manière exclusive à la détention du jeton et non libre pour tous
- **l'interopérabilité** entre plateformes est, à ce jour, **inexistante**

**La seule détention d'un JVC ne confère aucun droit. L'écart entre le discours des promoteurs des JVC et la réalité technologique et juridique est significatif. Sa résorption est une des conditions de réussite de leur développement.**

# Trois cas d'usage principaux des JVC

**Les jeux vidéo :**

- « jeux Web 3.0 », ou jeux à objets numériques échangeables (JONUM)
- les joueurs « possèdent » leurs objets de jeux et les récompenses peuvent être cédées et monétisées
- problématique de la qualification de jeu d'argent (*cf.* phase 1 de la mission)

**Luxe et consommation :**

- biens de consommation dans les *métavers* (ex : objets de luxe)
- jetons pouvant suivre un bien et/ou créer une communauté d'utilisateurs
- opérations *marketing* pour s'adresser à de nouveaux publics

**Art et culture :**

- jeton lié à une à une œuvre digitale ou « tokénisée ». Le propriétaire du jeton est *assimilé à tort* au propriétaire de l'œuvre
- création de produits dérivés, financement d'actions de mécénat, *métavers*, animation de communautés

**Entreprises françaises**

*Sorare, Sandbox Dogami, Cross the Ages, Metafight, Immortal Games*

*Arianee, Sandbox, Kering, LVMH, Lacoste*

*LaCollection.io, Rhapsody Curated, Everrose, Centre Pompidou*

**Des cas d'usage pour l'instant limités à des « niches » et réservés à un public d'initiés**

2. Enjeux juridiques

# ACCOMPAGNER LE DÉVELOPPEMENT DES JVC REQUIERT UN CADRE JURIDIQUE CLAIR

# Associer au jeton sa documentation commerciale pour protéger le consommateur

**La documentation de vente du jeton et celle du service auquel il donne accès ne sont pas nécessairement associés :** les CGV d'un objet de jeu collectionnable peuvent ne pas faire référence à l'accès au jeu.

**Les droits associés au jeton peuvent être de nature très variable :**

- « consommables » de manière progressive ou limités dans le temps
- démembrables entre une prestation numérique et un bien physique
- ou non transférables en cas de revente du jeton

**Le sort de ces droits après une cession sur le marché secondaire est incertain :**

- le droit de la consommation ne s'applique pas aux transactions entre particuliers
- la chaîne de transaction rend difficile les recours contre l'émetteur

**Proposition n° 1**

À chaque JVC doivent être associés lors de l'émission des documents contractuels définissant les droits du porteur du jeton :

- droits à l'émission du jeton
- services associés au jeton
- conséquences d'une revente

Ces documents doivent être annexés au jeton de manière indissociable, pour le suivre lors des reventes.

Ils peuvent être inscrits directement sur la *blockchain* ou prendre la forme d'un lien sécurisé avec des informations stockées hors de la *blockchain*.

Cette obligation s'appliquerait aux jetons qui n'ont pas fait l'objet d'un livre blanc (*cf. infra*).

# Le cas spécifique des NFT « artistiques »

**Il est impossible de créer artificiellement de la rareté sur les œuvres numériques et de conférer une valeur juridique spécifique aux « NFT artistiques » :**

- l'œuvre associée au NFT est accessible à tous sur internet. Pas de possession « rivale » possible
- on ne peut détenir des droits patrimoniaux que sur l'œuvre associée au NFT qui, dans le cas d'une œuvre numérique librement accessible, sont difficiles à définir.

**Le NFT n'est donc jamais une œuvre d'art, un support d'œuvre d'art, un titre de propriété…**

- les organismes publics devraient éviter des formulations prêtant à confusion lorsqu'ils émettent des NFT
- ils ne devraient pas accréditer auprès du public l'idée selon laquelle acheter un NFT est équivalent à l'achat d'une œuvre d'art

**Proposition n° 2**

Une valeur juridique peut être donnée aux « NFT artistiques » *via* des contrats de licence :

- contrat entre l'artiste et le détenteur du jeton concédant un droit d'exploitation, ce droit pouvant lui-même être cédé
- conformité de cette solution à l'article L. 132-7 du CPI à confirmer (sous-cession de droits d'auteur en principe soumise au consentement de l'auteur)
- élaborer un modèle de contrat de licence public afin de sécuriser les « NFT artistiques »

Néanmoins, du fait du droit à la copie privée, la valeur intrinsèque des NFT restera principalement ostentatoire.

# La fiscalité des jetons en matière d'imposition des plus values des particuliers

## Le régime de la fiscalité des particuliers en matière de plus values lors des opérations sur actifs numériques

- article 150 VH bis du CGI
- les transactions entre **actifs numériques au sens de la « loi PACTE »** ne sont pas soumises à l'impôt sur les plus values
- cette définition d'actifs numériques est très large et englobe les JVC
- par exemple : pas d'imposition des plus values réalisées sur des éthers utilisés pour l'achat d'un JVC même si ces éthers sont en forte plus value
- pareillement, pas d'imposition des plus values en cas de cession d'un JVC contre éther
- pas de distinction entre l'accessoire (le jeton) et son principal

## Proposition n°3

- **Exclure les JVC des « actifs numériques » pour l'application du régime de l'article 150 VH bis du CGI** pour soumettre à l'impôt les plus values réalisées sur les actifs numériques utilisés pour l'acquisition du JVC.

- **Assujettir les plus values réalisées par les particuliers lors de la cession de JVC** sur le marché secondaire en fonction du sous-jacent du jeton. Application du régime des biens meubles incorporels.

Le régime proposé est cohérent avec les principes appliqués en matière de TVA notamment pour laquelle les droits sous-jacents priment sur le dimension numérique.

# Le règlement MiCA et son champ d'application

## Champ d'application du règlement

- **Ne s'applique pas aux NFT**
  - définition économique des NFT restrictive (petite série et collection)
  - exclusion par un considérant non repris dans les articles définition/champ du règlement => ambiguïté

- **S'applique partiellement aux jetons utilitaires**
  - pas d'assujettissement aux titres II et VI et partiellement au titre V
  - sauf si les jetons sont admis à la négociation sur une plateforme ou émis en vue d' un service en développement pour lever des fonds

- **Les plateformes de négociation pair à pair sont exclues** (*OpenSea*)

## Architecture générale

- **Titres II à IV** : obligations relatives aux émissions de crypto actifs
  - publication d'un livre blanc
  - par l'émetteur ou lors de l'admission à l'échange sur plateforme réglementée

- **Titre V** : obligations relatives aux prestataires de services (CASP) :
  - services de conservation, paiement et plateformes de négociation
  - LCB-FT et règles comparables à la finance traditionnelle

- **Titre VI** : lutte contre les abus de marché (opérations d'initié, manipulations de cours)

- **Règlements distincts en matière de LCB-FT** faisant référence à MiCA

# Le règlement MiCA et son champ d'application (synthèse)

| Type de JVC | Titre II applicable à l'émission de ces jetons (livre blanc) | Titre V applicable aux prestataires de services sur ces jetons (agrément CASP) | Titre VI applicable aux transactions sur ces jetons (abus de marché) |
|---|---|---|---|
| **JVC non fongibles (définis dans un sens économique)** | Non | Non. Les services impliquant à la fois des JVC non fongibles et des JVC fongibles sont cependant soumis au titre V | Non |
| **Autres JVC utilitaires donnant accès à un bien existant ou à un service opérationnel (*utility tokens*)** | Si et seulement s'ils sont admis à la négociation | Oui, exception faite de certains services (conservation, transfert) L'exception ne s'applique pas si les jetons sont admis à la négociation | Si et seulement s'ils sont admis à la négociation |
| **Autres JVC relevant des exceptions *de minimis*** | Si et seulement s'ils sont admis à la négociation | Oui | Si et seulement s'ils sont admis à la négociation |
| **Autres JVC** | Oui | Oui | Si et seulement s'ils sont admis à la négociation |

# Élargir le champ d'application du règlement MiCA en matière d'abus de marché

**La distinction entre jetons utilitaires (JU) et NFT par MiCA est peu pertinente :**

- les JU donnant accès à un service sont dans le champ du règlement mais assujettis à des obligations réduites
- alors que les NFT ne présentent pas de différences significatives en termes d'analyse des risques avec ces jetons, ils sont exclus du règlement

**Les JU et NFT présentent des risques comparables aux autres cryptoactifs :**

- la *blockchain* et les plateformes de pair à pair permettent des échanges électroniques
- elles publient des prix en continu, offrent une liquidité
- risque très élevé d'abus de marché et ce d'autant plus que certains marchés sont étroits

**Propositions pour « MiCA2 »**

- **n° 4 : assujettir les NFT au règlement** en les faisant entrer dans son champ et en les soumettant à des obligations comparables à celles des jetons utilitaires
- **n° 5 : application du titre VI sur les abus de marché** à tous les jetons, qu'ils soient négociés sur une plateforme centralisée ou non
- **n° 6 : créer un régime spécifique aux plateformes d'échange de pair à pair** de crypto actifs qui couvrira notamment les échanges de JVC (*cf*. LCB-FT)
- **n° 7 et 8 : interdiction aux émetteurs de JVC d'intervenir sur le marché secondaire** de leurs jetons et encadrer les transactions de leurs dirigeants

# Renforcer le dispositif de LCB-FT

**L'Union européenne vient d'étendre aux cryptoactifs les règles LCB-FT en :**

- assujettissant les CASP à ces règles
- instituant la vérification d'identité du client du CASP pour les transactions de plus de 1 000 € effectuées par des CASP ou des prestataires de service de paiement

**Les échanges de JU et de NFT échappent à ces obligations :**

- champ d'application calqué sur celui de MiCA
- aucune obligation pour les plateformes pair à pair

**Alors même que les risques en matière de LCB-FT sont comparables à ceux présentés par les autres cryptoactifs :**

- échanges électroniques
- anonymat
- conversion *in fine* en monnaie ayant cours légal

**Proposition n° 9**

**9.A :** Appliquer la *travel rule* aux NFT et au *Lightning Network*. Rendre obligatoire la vérification de l'identité des clients pour toute transaction en cryptoactifs :

- depuis ou vers un CASP
- ou à finalité professionnelle

Développer des services d'identité numérique pour fluidifier les contrôles.

**OU**

**9.B** : Interdire les transactions de plus de 1000 € entre portefeuilles hébergés et portefeuilles autohébergés.
Développer des services d'hébergement sans conservation alternatifs aux CASP.

# Les points de vigilance (1)

**Les *layers 2***

- « couches » de gestion des transactions dont un « résumé » est inscrit sur la chaine principale
- indispensables au passage à l'échelle et à la réduction des coûts de transaction pour permettre une plus large diffusion des JVC
- conséquences sur les opérateurs et les entreprises qui les utilisent en termes réglementaires (conservation d'actifs, gestion d'une plateforme, LCB-FT…) seront **à examiner en fonction de leurs modalités de mise en œuvre**

**La conformité au RGPD des solutions à base de blockchain**

- l'adresse de *wallet* et les transactions publiées sur la blockchain sont des données personnelles
- impossible d'appliquer, notamment, le droit à l'effacement et à la rectification des données prévus par le RGPD
- position pragmatique sur ces questions en 2018 de la CNIL qui accepte les technologies permettant d'approcher les objectifs du RGPD
- mais, sauf à accepter d'anonymiser totalement les transactions (pb de LCB-FT), **un noyau irréductible de données personnelles ne sera pas traité de manière conforme au RGPD**

# Les points de vigilance (2)

## La valeur probatoire des écritures sur la blockchain en droit civil

- le juge peut reconnaitre la valeur probatoire des écritures sur la blockchain à droit constant
- lorsque le code civil exige un écrit comme preuve, la simple écriture sur *blockchain* ne suffit pas à ce que la transaction soit valide : la signature par clé cryptographique couramment utilisée dans le Web 3.0 n'est pas une signature électronique valable en droit car l'association entre la signature et l'identité du signataire doit être validée par un tiers
- deux issues possibles : recours à des prestataires de confiance ou modification du droit de la signature électronique (non lié aux *blockchains,* dépasse le champ de la mission)

## L'évaluation des conséquences de ces technologies sur l'environnement

- la consommation des *blockchains* à preuve de travail (PoW) est considérable. 15 GW (10 EPR) pour 5 transactions par seconde et le bilan carbone d'une transaction est de 400 kg eq. $CO_2$ pour la chaine *Bitcoin*
- les *blockchains* à preuve d'enjeu (*Ethereum*) permettent des consommations moindres. Un rapport de 1 à 1 000 selon leurs promoteurs sans contre-expertise indépendante.
- **quelle que soit la solution technique, ces technologies ont une consommation d'énergie supérieure à des bases de données centralisées** sans que leurs fonctionnalités soient toujours nettement supérieures aux systèmes « classiques »

3. L’écosystème français du Web 3.0

# FORCES ET FAIBLESSES D’UN ÉCOSYSTÈME DYNAMIQUE

# Un écosystème prometteur

**Trois forces identifiées :**

- qualité des ingénieurs et de la recherche
- entreprises et institutions d'envergure mondiale dans le luxe, le jeu vidéo et sur le marché de l'art qui investissement dans ces technologies et dynamisme des opérateurs de salons et d'événements
- un cadre réglementaire précoce et innovant (PACTE) sur lesquels les acteurs peuvent appuyer leur développement et qui conduit des entreprises étrangères (Binance, Circle…) à s'implanter à Paris

**Un tissu de startups dynamique mais très jeune :**

- 800 projets et entreprises recensés par BPI France
- une centaine de levées de fonds auprès d'investisseurs pour environ 2 Md€ depuis 2018 soit moins de 8 % des fonds levés par des entreprises innovantes
- une quinzaine d'entreprises seulement ont dépassé le financement d'amorçage
- deux licornes (Sorare et Ledger)

**Une position de co-leader au sein de l'Union européenne :**

- un nombre d'entreprise et des montants levés comparables à ceux de l'Allemagne
- le Royaume-Uni et la Suisse ont des écosystèmes au moins 4 fois plus importants
- faible présence française dans les fondements « technologiques » du Web 3.0

# Dynamiser l' écosystème Web 3.0 français

## Deux obstacles identifiés :

**Difficulté pour les entreprises à ouvrir des comptes bancaires**

- banques prudentes face aux risques LCB-FT
- identifiée dans la loi PACTE pour les PSAN mais plus large

**L'investissement en jetons par les fonds de capital risque n'est pas encore autorisé par l'AMF**

- toutes les levées de fonds significatives de startups françaises sont pilotées par des fonds étrangers qui ont cette capacité
- difficulté principale liée à l'absence de dépositaire de ces actifs est en voie de résorption
- mais problème plus général de la conservation des actifs numériques effectuée par des sociétés étrangères

**Proposition n° 10**

Reprise sous l'égide de l'AMF et de l'ACPR des échanges avec les banques et les entreprises pour résorber cette difficulté.

**Proposition n° 11**

Encourager l'émergence de solutions souveraines de conservation aux côtés de celles proposées par Ledger. De tels services pourraient notamment être fournis par la CDC.

# ANNEXE TECHNIQUE

# *Blockchains* et jetons : quelques notions techniques

## Les *blockchains* sont des registres distribués

- registres de données : seulement des possibilités d'écritures nouvelles
- distribués : toute personne peut obtenir une copie
- *blockchain* publique : tout le monde peut proposer de nouvelles inscriptions
- des règles sur la façon dont des données peuvent être écrites

    exemple : disponibilité des fonds, signature électronique de l'ordre de transaction…

### Qui décide ce qui s'écrit sur le registre ?

- modèle centralisé (banque, État civil) : une autorité identifiée valide ou délègue
- *blockchains* publiques : protocoles cryptographiques (preuve de travail notamment) sans autorité de dernier ressort

## Les *smart contracts* permettent de créer des jetons

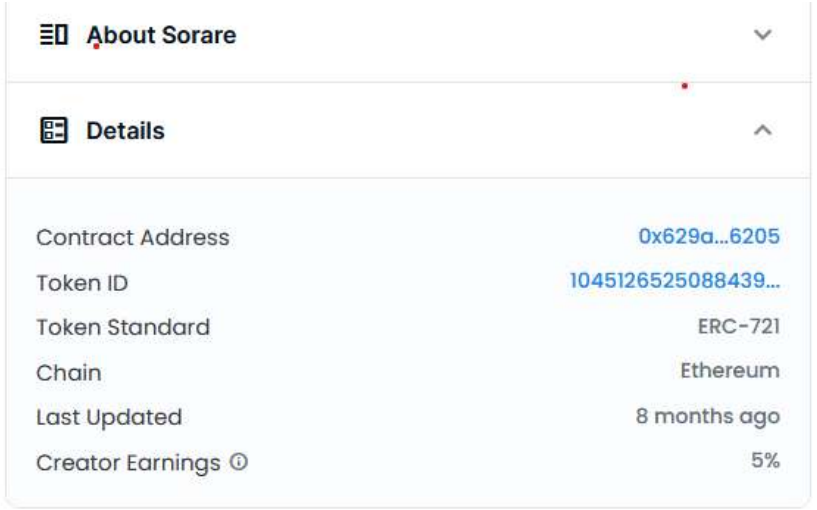
- certaines *blockchains* sont programmables : on peut y écrire des **programmes autonomes** (« *smart contracts* »)
- dans la mémoire de ces programmes, possibilité de tenir une liste de comptes dans une unité *ad hoc* : le jeton
- le jeton peut être non fongible (un unique exemplaire indivisible)

### Quelles conséquences à détenir un jeton ?

- « *on chain* » : se traduit par des conséquences sur la *blockchain* (ex. : flux financiers)
- « *off chain* » : à l'extérieur (ex. : droits de votes à une assemblée, livraison d'un service…)

# Un jeton à vocation commerciale sur OpenSea.io






éditeur du jeton

identifiant qui permet d'accéder aux données du jeton

Historique de transactions du jeton

Item Activity

Filter

| Event | Price | From | To | Date |
|---|---|---|---|---|
| List | 0,001 ETH | 1298EA | | 19d ago |
| List Expired | 0,0029 ETH | 1298EA | | 1mo ago |
| Transfer | | Sorare_StarkEx_escrow... | 1298EA | 8mo ago |
| Transfer | | Sorare_StarkEx_escrow... | 1298EA | 8mo ago |
| Airdrop | | NullAddress | Sorare_StarkEx_escrow... | 8mo ago |

mise en vente sur la chaine *Ethereum* par opensea.io

sortie du *layer 2* Sorare

création du jeton

# Le jeton renvoie vers une image et donne accès à un jeu



Métadonnées du jeton

{"name":"Kim Hyun-Tae 2022-23 • Limited 91/1000","description":"Limited Player Cards are only issued at 1000 editions per season.","background_color":"f3f2f3","external_url":"?referrer=opensea","image":"https://assets.sorare.com/carddata/f9022a44-7830-4b17-b70d-7430c6dd6464/picture/a02298fe5fb8c47027a5a116f35705a9.png","attributes":[{"trait_type":"scarcity","value":"Limited"},{"trait_type":"club","value":"Seongnam"},{"trait_type":"season","value":"2022-23"},{"trait_type":"position","value":"Midfielder"},{"trait_type":"serial_number","value":91,"max_value":1000,"display_type":"number"},{"trait_type":"edition","value":"classic"},{"trait_type":"jersey","value":"home"},{"trait_type":"language","value":"en"},{"trait_type":"print_date","value":1650652025,"display_type":"date"},{"trait_type":"level","value":3,"max_value":20,"display_type":"ranking"},{"trait_type":"XP","value":490,"max_value":21000,"display_type":"ranking"},{"trait_type":"power","value":"1.065","display_type":"number","max_value":0.5}]}

Clic sur le ce lien pour obtenir l'image


De plus, le logiciel de jeu Sorare reconnait ce jeton et donne accès au jeu