INTERNATIONAL JOURNAL OF **DIGITAL AND DATA LAW**

REVUE INTERNATIONALE DE DROIT **DES DONNÉES ET DU NUMÉRIQUE**

ISSN 2553-6893

IMODEV
LES ÉDITIONS

Vol. 8 - 2022

International Journal of Digital and Data Law
Revue internationale de droit des données et du numérique

Direction :
Irène Bouhadana & William Gilles

ISSN : 2553-6893

IMODEV
49 rue Brancion 75015 Paris – France
www.imodev.org
ojs.imodev.org

Les propos publiés dans cet article n'engagent que leur auteur.

The statements published in this article are the sole responsibility of the author.

Droits d'utilisation et de réutilisation

Licence Creative Commons – Creative Commons License -

CC-**BY-NC-ND**

Attribution
Pas d'utilisation commerciale – Non Commercial
Pas de modification – No Derivatives

À PROPOS DE NOUS

La **Revue Internationale de droit des données et du numérique (RIDDN)/ the International Journal of Digital and Data Law** est une revue universitaire créée et dirigée par Irène Bouhadana et William Gilles au sein de l'IMODEV, l'Institut du Monde et du Développement pour la Bonne Gouvernance publique.

Irène Bouhadana, docteur en droit, est maître de conférences en droit du numérique et droit des gouvernements ouverts à l'Université Paris 1 Panthéon-Sorbonne où elle dirige le master Droit des données, des administrations numériques et des gouvernements ouverts au sein de l'École de droit de la Sorbonne. Elle est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Elle est aussi fondatrice et Secrétaire générale de l'IMODEV. Enfin, associée de BeRecht Avocats, elle est avocate au barreau de Paris et médiateure professionnelle agréée par le CNMA.

William Gilles, docteur en droit, est maître de conférences (HDR) en droit du numérique et en droit des gouvernements ouverts, habilité à diriger les recherches, à l'Université Paris 1 Panthéon-Sorbonne où il dirige le master Droit des données, des administrations numériques et des gouvernements ouverts. Il est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Il est aussi fondateur et Président de l'IMODEV. Fondateur et associé de BeRecht Avocats, il est avocat au barreau de Paris et médiateur professionnel agréé par le CNMA.

IMODEV est une organisation scientifique internationale, indépendante et à but non lucratif créée en 2009 qui agit pour la promotion de la bonne gouvernance publique dans le cadre de la société de l'information et du numérique. Ce réseau rassemble des experts et des chercheurs du monde entier qui par leurs travaux et leurs actions contribuent à une meilleure connaissance et appréhension de la société numérique au niveau local, national ou international en en analysant d'une part, les actions des pouvoirs publics dans le cadre de la régulation de la société des données et de l'économie numérique et d'autre part, les modalités de mise en œuvre des politiques publiques numériques au sein des administrations publiques et des gouvernements ouverts.

IMODEV organise régulièrement des colloques sur ces thématiques, et notamment chaque année en novembre les *Journées universitaires sur les enjeux des gouvernements ouverts et du numérique / Academic days on open government and digital issues*, dont les sessions sont publiées en ligne [ISSN : 2553-6931].

IMODEV publie deux revues disponibles en open source (ojs.imodev.org) afin de promouvoir une science ouverte sous licence Creative commons_CC-**BY-NC-ND** :

1) la *Revue Internationale des Gouvernements ouverts (RIGO)/ International Journal of Open Governments* [ISSN 2553-6869] ;

2) la *Revue internationale de droit des données et du numérique (RIDDN)/International Journal of Digital and Data Law* [ISSN 2553-6893].

ABOUT US

The **International Journal of Digital and Data Law / Revue Internationale de droit des données et du numérique (RIDDN)** is an academic journal created and edited by Irène Bouhadana and William Gilles at IMODEV, the Institut du monde et du développement pour la bonne gouvernance publique.

Irène Bouhadana, PhD in Law, is an Associate professor in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where she is the director of the master's degree in data law, digital administrations, and open governments at the Sorbonne Law School. She is a member of the Institut de recherche juridique de la Sorbonne (IRJS). She is also the founder and Secretary General of IMODEV. Partner at BeRecht Avocats, she is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

William Gilles, PhD in Law, is an Associate professor (HDR) in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where he is the director of the master's degree in data law, digital administration and open government. He is a member of the Institut de recherche juridique de la Sorbonne (IRJS). He is also founder and President of IMODEV. Founder and partner at BeRecht Avocats, he is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

IMODEV is an international, independent, non-profit scientific organization created in 2009 that promotes good public governance in the context of the information and digital society. This network brings together experts and researchers from around the world who, through their work and actions, contribute to a better knowledge and understanding of the digital society at the local, national or international level by analyzing, on the one hand, the actions of public authorities in the context of the regulation of the data society and the digital economy and, on the other hand, the ways in which digital public policies are implemented within public administrations and open governments.

IMODEV regularly organizes conferences and symposiums on these topics, and in particular every year in November the Academic days on open government and digital issues, whose sessions are published online [ISSN: 2553-6931].

IMODEV publishes two academic journals available in open source at ojs.imodev.org to promote open science under the Creative commons license CC-**BY-NC-ND**:

1) the *International Journal of Open Governments*/ la *Revue Internationale des Gouvernements ouverts (RIGO)* [ISSN 2553-6869] ;

2) the *International Journal of Digital and Data Law* / la *Revue internationale de droit des données et du numérique* (RIDDN) [ISSN 2553-6893].

BITCOIN, SMART CONTRAT ET MÉTAVERS : RÉVOLUTION OU ARNAQUE

par **Jean HARIVEL**, Docteur en droit public, Chargé d'enseignement à l'Université Paris 1 Panthéon Sorbonne

---

Après le succès du WEB 2.0 qui a permis à l'Internet de toucher tous les individus au travers des messageries et des réseaux sociaux, la virtualisation de la vie réelle connaît une recrudescence avec les monnaies virtuelles, les smart contrats et maintenant les métavers. Ces notions nouvelles s'adossent aux technologies de la blockchain et de la réalité virtuelle développée initialement pour les jeux dits 3D. ces notions connaissent un engouement rapide et font l'objet de spéculations.

Ce n'est pas un hasard si Facebook après son réseau social et les « amis virtuels », lance sa propre monnaie virtuelle, Libra[1]. Mark Zuckerberg, PDG de Facebook, veut aller encore plus loin dans la virtualisation du monde en lançant un métavers, entre réel et science-fiction[2] et change la dénomination de la société mère de Facebook à Meta.

Le monde virtuel est l'objet de spéculations réelles. Dans le Métavers, il sera possible d'acheter des parcelles « constructibles », des immeubles, des usines, etc. Les droits de propriété sont dématérialisés par des titres virtuels de propriété ou NFT[3], gérés avec la technologie des blockchains. Ces NFT sont déjà utilisés pour la propriété d'œuvres virtuelles, photographies, événements, etc. Les monnaies utilisées pour les échanges dans ce monde virtuel sont exclusivement des cryptomonnaies.

Toutes ces notions utilisent la technologie des blockchains censée sécuriser les transactions. Mais en manipulant des entités virtuelles objet de mouvements spéculatifs[4] créons-nous réellement de la valeur ou sommes-nous face à l'arnaque du siècle ? Outre que les

---

[1] M. TUAL, « Libra : tout ce qu'il faut savoir sur la cryptomonnaie de Facebook », *Le Monde*, 18 juin 2019, disponible à : https://www.lemonde.fr/pixels/article/2019/06/18/ce-qu-il-faut-savoir-sur-le-libra-la-cryptomonnaie-de-facebook_5477887_4408996.html (consulté le 26 avril 2022).

[2] *« Le métavers désiré et décrit par Mark Zuckerberg, le patron de Facebook, relève autant de la science-fiction que d'une réalité qui prend corps, très lentement, en dépit des critiques et des inquiétudes. Mais le chemin technologique à parcourir est encore très long. »* extrait de « Le métavers de Facebook, une réalité virtuelle qui grignote de l'espace-temps », *AFP* pour France Info, 29 octobre 2021, disponible à : https://www.france24.com/fr/info-en-continu/20211029-le-m%C3%A9tavers-de-facebook-une-r%C3%A9alit%C3%A9-virtuelle-qui-grignote-de-l-espace-temps (consulté le 26 avril 2022).

[3] NFT : Non-Fungible Token, ou jeton non fongible.

[4] Devant les sommes mise en jeu et l'absence de définition juridique des NFT, une tentative infructueuse d'amendement de la loi de finance 2022 visait à leur définition juridique et fiscale (Amendement n°I-CF879 déposé le jeudi 30 septembre 2021 à l'Assemblée nationale).

avoirs manipulés sont exclusivement virtuels, donc créés par des programmes informatiques, la sécurité des transactions est-elle réelle ? Des cryptomonnaies ont subi des piratages entraînant la perte de millions de dollars. Des intermédieires apparaissent et disparaissent empochant au passage les économies de spéculateurs naïfs. Devant de tels risques, la législation française tente de fiabiliser ces intermédiaires.
Après une présentation des technologies des blockchains et des nouveaux concepts, l'article s'attachera à montrer comment ces etchnologies peuvent ouvrir la voie à des arnaques rémunératrices pour leurs auteurs.

§1 – UNE TECHNIQUE AU SERVICE DE NOUVEAUX CONCEPTS

A) L'apport de la blockchain : un registre sécurisé

1) Des technologies d'enregistrement multiples

La technologie blockchain repose sur un registre d'enregistrement de transactions décentralisé et crypté. Un rapport parlementaire de 2018[5] cite la définition proposée par l'OPECST[6] :

> « Les blockchains sont des "technologies de stockage et de transmission d'informations, permettant la constitution de registres répliqués et distribués, sans organe central de contrôle, sécurisées grâce à la cryptographie, et structurées par des blocs liés les uns aux autres, à intervalles de temps réguliers" ».

Dans cette définition, il est question de plusieurs technologies utilisées pour la constitution de ces registres. Cette multiplication de technologies est reprise par l'ISO, organisme de normalisation international, dans ses normes concernant les chaines de blocs[7].
Ces technologies décentralisées, sans organe central de contrôle sont présentées comme inviolables, thèse reprise sur le site du ministère de l'Économie et des Finances[8] :

---

[5] L. de la BAUDIÈRE, J.-M. MIS, *Rapport d'information déposé en application de l'article 145 du Règlement par la Mission d'information commune sur les chaînes de blocs (blockchains)*, Assemblée Nationale, 12 décembre 2018.
[6] Office parlementaire d'évaluation des choix scientifiques et technologiques.
[7] ISO 22739:2020 : Chaîne de blocs et technologies de registres distribués — Vocabulaire (Blockchain and distributed ledger technologies — Vocabulary)
ISO/TR 23244:2020 : Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations
ISO/TR 23455:2019 : Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems
ISO/TR 23576:2020 : Blockchain and distributed ledger technologies — Security management of digital asset custodians
[8] Bercy Infos, « Qu'est-ce que la blockchain ? », *Innovation et data*, 12 avril 2022, disponible à :
https://www.economie.gouv.fr/entreprises/blockchain-definition-avantage-utilisation-application?msclkid=d298e026cf6d11ec9a5714735c273dc8 (consulté le 9 mai 2022).

> « En pratique, une blockchain est une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. La Banque de France en explique les principales caractéristiques : l'identification de chaque partie s'effectue par un procédé cryptographique ; la transaction est envoyée à un réseau (ou "nœud" de stockage) d'ordinateurs situés dans le monde entier ; chaque "nœud" héberge une copie de la base de données dans lequel est inscrit l'historique des transactions effectuées. Toutes les parties prenantes peuvent y accéder simultanément. Le système de sécurisation repose sur un mécanisme de consensus de tous les "nœuds" à chaque ajout d'informations. Les données sont déchiffrées et authentifiées par des "centres de données" ou "mineurs". La transaction ainsi validée est ajoutée dans la base sous forme d'un bloc de données chiffrées (c'est le "block" dans blockchain). La décentralisation de la gestion de la sécurité empêche la falsification des transactions. Chaque nouveau bloc ajouté à la blockchain est lié au précédent et une copie est transmise à tous les "nœuds" du réseau. L'intégration est chronologique, indélébile et infalsifiable ».

Le rapport d'avril 2021 sur les verrous technologiques des blockchains[9] part d'une lettre de mission portant sur les thèmes suivants : la souveraineté, la sécurité, l'interopérabilité et l'évolutivité, l'énergie, les modèles économiques. Le rapport publié est structuré autour de la sécurité, le passage à l'échelle, la consommation énergétique, les modèles et mécanismes économiques, l'interopérabilité, la souveraineté.

De nombreuses offres technologiques existent : Bitcoin, Ethereum, Tezos, Hyperledger, etc. Dans une analyse de Gartner[10], l'année 2023 est citée comme l'année où les technologies blockchain pourraient être interopérables et garantir la protection des données personnelles :

> « Ne vous y trompez pas : l'époque de l'interopérabilité transparente de la blockchain au niveau "atomique" n'est pas encore arrivée. Pas plus que l'époque de la fonctionnalité inter-chaînes où un seul contrat intelligent peut mettre à jour plusieurs plates-formes blockchain en utilisant un seul processus. Nous ne verrons pas ces

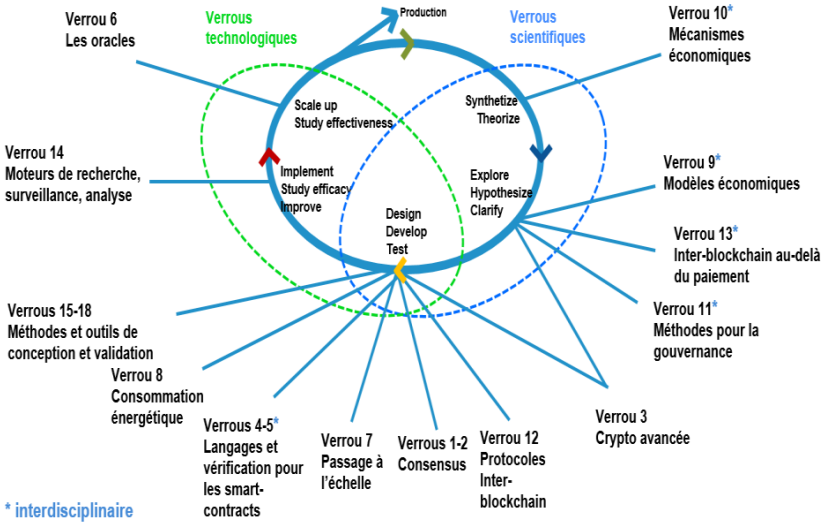
[9] Direction des entreprises, *Les verrous technologiques des blockchains*, BCom de la DGE, avril 2021, disponible à l'URL https://www.entreprises.gouv.fr/files/files/etudes-et-statistiques/rapport-final-blockchain.pdf?v=1649770476 (consulté le 9 mai 2022).

[10] Gartner, « Gartner 2019 Hype Cycle Shows Most Blockchain Technologies Are Still Five to 10 Years Away From Transformational Impact », *Newsroom Press Releases*, 8 octobre 2019, disponible à : https://www.gartner.com/en/newsroom/press-releases/2019-10-08-gartner-2019-hype-cycle-shows-most-blockchain-technologies-are-still-five-to-10-years-away-from-transformational-impact (consulté le 9 mai 2022).

fonctions nécessaires se généraliser avant au moins deux ans[11] ».

2) *Des techniques d'enregistrement non encore matures*

Afin que les techniques de blockchain deviennent matures, il est nécessaire que les utilisateurs n'aient pas à choisir la bonne plate-forme, le bon langage de contrat intelligent, les bonnes interfaces système et les bons algorithmes de consensus[12].
Ce sont ces mêmes verrous que formule le rapport de la direction des entreprises[13].



Extrait de Les verrous technologiques des blockchains, Direction Générales des Entreprises, avril 2021

Au niveau technique, les principaux besoins techniques listés dans le rapport sont l'interopérabilité ou les protocoles inter-blockchains qui permettraient d'échanger de la valeur entre actifs créés sur différentes plateformes, ou des données entre smart contrats, la sécurité liée aux moyens de preuve et et de confidentialité des données, la souveraineté, la vérification et la certification des chaînes et des applications distribuées.
De plus, les smart contrats correspondant à des programmes informatiques exécutés dans la blockchain ne doivent pas pouvoir

[11] « Make no mistake: The days of seamless blockchain interoperability at the 'atomic' level are not here yet. Nor are the days of cross chain functionality where a single smart contract can update multiple blockchain platforms using a single process. We won't see these needed functions go mainstream for at least two years ». traduit par l'auteur à partir de Avivah Litan, « Top Trends in Blockchain Technology; inching towards Web 3.0 », *Information Technology*, Gartner, 19 septembre 2019, disponible à : https://blogs.gartner.com/avivah-litan/2019/09/19/top-trends-blockchain-technology-inching-towards-web-3-0/?_ga=2.145901175.23291489.1652087368-1712553237.1652087368 (consulté le 9 mai 2022).
[12] Gartner, *ibid.*
[13] Direction des entreprises, *Les verrous technologiques des blockchains,* déjà cité.

être ni modifiés ni supprimés. Ils peuvent rester susceptibles de cyberattaques qui compromettent leur sécurité s'ils ne sont pas programmés correctement.

B) L'ouverture de nouveaux concepts utilisant la blockchain

Si les premières applications de la blockchain ont été liées aux cryptomonnaies, bitcoin ou autres, de nouveaux concepts ont bâtis sur ces technologies.

1) Les monnaies virtuelles

En 2009, la première cryptomonnaie est apparue : le bitcoin. L'intérêt de cette monnaie est de pouvoir effectuer des transactions anonymement et sans intermédiaires dans le but d'être indépendant du système bancaire et monétaire institutionnel. La cryptomonnaie est autonome et s'affranchit des organismes régulateurs.
Cette monnaie a connu un succès tel que de nombreuses autres monnaies sont apparues depuis, Ethereum, Monero, Ntx, Ripple, Litecoin, Solidcoin, ... et Libra[14].
Le principe de fonctionnement de ces monnaies numériques ou cryptomonnaies reste celui mis en œuvre pour le bitcoin par Satoshi Nakamato en 2009. Les protocoles mis en œuvre pour générer et gérer les bitcoins reposent sur les techniques de cryptographie asymétrique à deux clés, de hachage, d'arbre de Merkle, de base de données de type clé-valeur[15]. Seules des améliorations en termes de vitesse des transactions ou des mécanismes de validation diffèrent entre toutes ces monnaies électroniques.

2) Les smart contracts ou contrats intelligents

En 2015, un jeune canadien de 21 ans, Vitalik Buterin[16], constatant que la blockchain Bitcoin n'est pas adaptée à la gestion d'applications non financières, va développer Ethereum, une infrastructure blockchain étendant les possibilités de Bitcoin[17].
Comme précisé sur le site ethereum.org :

> « Ethereum s'appuie sur l'innovation du Bitcoin, avec quelques différences majeures.

[14] Selon les auteurs, le nombre de monnaies numériques en circulation va de 200 à plusieurs milliers.
[15] Pour une description plus complète des mécanismes mis en œuvre, consulter P. DE FILIPPI, *Blockchain et cryptomonnaies*, PUF, « Que sais-je ? », 2022, ISBN : 9782715409484 : https://www.cairn.info/blockchain-et-cryptomonnaies--9782715409484.htm
Il est également possible de se référer au livre blanc publié par Satoshi Nakamoto dans sa version du 24 mars 2009 et disponible à :
https://bitcoin.org/bitcoin.pdf.
[16] Vitaly Dmitriyevich plus connu sous le nom de "Vitalik" Buterin est né à Kolomna dans l'Oblast de Moscou. Il émigre au Canada avec ses parents à l'âge de six ans.
[17] Pour approfondir la connaissance d'Ethereum, lire le livre blanc Ethereum à : https://ethereum.org/fr/whitepaper/ (consulté le 27 juin 2022).

> Tous deux vous permettent d'utiliser de l'argent virtuel sans banque ni prestataire de paiement. En revanche, Ethereum est programmable, donc vous pouvez également l'utiliser pour de nombreux actifs numériques différents – même du Bitcoin !
> Cela signifie également qu'Ethereum permet plus que des paiements. Il s'agit d'un marché de services financiers, de jeux et d'applications qui ne peuvent pas vous pister ou vous censurer.[18]»

Ethereum se présente comme un ordinateur universel permettant l'exécution d'applications décentralisées permettant la création par les utilisateurs de contrats intelligents ou *smart contracts*. Il dispose d'un langage de programmation dont les instructions peuvent être interprétées par la machine virtuelle d'Ethereum.
Le site Ethereum donne cette définition pour un contrat intelligent ou *smart contract* :

> « Un "contrat intelligent" est simplement un programme exécuté sur la blockchain d'Ethereum. C'est un ensemble de code (ses fonctions) et de données (son état) qui réside à une adresse spécifique sur la blockchain Ethereum.
> Le contrat intelligent est un type de compte Ethereum. Cela signifie qu'il dispose d'un solde et peut envoyer des transactions sur le réseau. Cependant, il n'est pas contrôlé par un utilisateur, mais est plutôt déployé et exécuté comme un programme. Les comptes des utilisateurs peuvent ensuite interagir avec un contrat intelligent en soumettant des transactions qui exécutent une fonction définie sur le contrat intelligent. Un contrat intelligent peut définir des règles, comme un contrat normal, et les appliquer automatiquement via le code. Les contrats intelligents ne peuvent pas être supprimés par défaut et les interactions avec eux sont irréversibles. »

L'exécution des instructions incluses dans le contrat intelligent nécessite d'avoir une passerelle entre la blockchain et l'environnement réel afin de savoir si les conditions d'exécution du programme sont remplies. Les services capables d'inscrire dans la blockchain les données extérieures permettant le déclenchement des clauses contractuelles programmées sont appelés des « oracles », ce sont des sources d'informations certifiées provenant d'un ou plusieurs opérateurs spécialisés[19].
Après Ethereum qui fut la première plateforme capable de supporter des *smart contracts*, d'autres blockchains ont développé ce concept, soit en utilisant le langage Turing-complet de la machine virtuelle Ethereum, soit en développent d'autres langages, soit en s'appuyant sur des langages informatiques existants tels Javascript, C++, Python, etc.

[18] URL https://ethereum.org/fr/what-is-ethereum/ (consultée le 27 juin 2022).
[19] P. DE FILIPPI, *Blockchain et cryptomonnaies*, *op. cit.*, pp. 39-73.

3) Les droits de propriété virtuels ou NFT

Une blockchain permet l'enregistrement de transactions de manière sécurisée, elle peut être utilisée comme un registre de titres de propriété enregistrant les transactions sur un bien. C'est ainsi que sont nés les titres de propriété virtuels (jeton non fongible ou en anglais Non Fungible Token, abrégé en NFT). Non fongible signifie que chaque unité (jeton) est unique, et ne peut pas être reproduite ni échangée.
Créés sur une plateforme de contrats intelligents, majoritairement Ethereum, les NFT sont toutefois bien différents des autres crypto-monnaies. Ils correspondent à un titre de propriété puisque la personne qui détient un NFT détient la propriété de l'objet associé qu'il soit virtuel ou réel. Il existe des NFT d'œuvres d'art numériques non reproductibles ou des NFT d'événements sportifs. Pour acquérir ou vendre un NFT, il est nécessaire de pouvoir se connecter sur la plateforme idoine. Il existe plusieurs plateformes proposant la gestion de NFT : eToro, OpenSea, Cryto.com, Fundation, AtomicMarket, etc. Le choix de la plateforme ne suffit pas, il faut utiliser une extension capable de prendre en charge les applications associées aux NFT, par exemple *Metamask*. La plateforme propose les extensions supportées. Il faut ensuite paramétrer le portefeuille (*wallet* en anglais), puis connecter le portefeuille à une plateforme de trading[20].
Les NFTs s'annoncent aussi indispensables dans le futur métavers. Les tokens ou jetons non fongibles peuvent aussi permettre d'échanger de l'immobilier numérique dans des espaces virtuels.

4) Le métavers

En 2003, est sorti un jeu en 3D, Second Live. Les joueurs pouvaient y créer un avatar et y vivre des aventures dans un univers présenté en 3D. Ils pouvaient, dans le mode Premium[21], y acquérir des terrains et y construire des immeubles. Ce jeu est toujours actif[22].
Les métavers sont construits sur le même principe, et font appel aux techniques de réalité virtuelle et de réalité augmentée. Après le monde du jeu, le monde industriel et financier s'intéresse aux métavers. Les marques promeuvent leurs produits dans le métavers[23]. Le rapprochement entre le métavers et les NFT, qui permettent d'accéder à des titres de propriété numérique uniques,

[20] Annick, « NFT : Tout savoir sur la nouvelle forme de crypto-monnaie », 17 juin 2022, *Le Big Data,* disponible à https://www.lebigdata.fr/nft-tout-savoir (consulté le 29 juin 2022).
[21] Le mode Premium nécessite un abonnement. En échange, le joueur reçoit régulièrement une certaine somme en L$ qui lui permet de faire des achats.
[22] Pour y accéder, https://secondlife.com/?lang=fr
[23] Durant l'assemblée générale des actionnaires de L'Oréal, en juin 2022, le directeur général a dit s'intéresser aux métavers comme à une technologie nouvelle qu'il ne fallait pas ignorer.

est effectif. Il devient possible d'acheter des terrains[24], de construire des immeubles, des usines, etc. Le monde virtuel rejoint le monde réel. Cryptomonnaies, NFT et métavers sont les briques de base d'un monde virtuel merchandisé.
En 2014, Facebook devenu Meta a racheté l'entreprise spécialisée dans la réalité virtuelle Oculus VR pour 2 milliards de dollars. En 2020, Meta a lancé Horizon, un réseau social en réalité virtuelle et multijoueur fonctionnant avec le casque VR Oculus. L'objectif de Mark Zuckerberg serait de créer d'ici les 5 prochaines années, un métavers qui pourrait rassembler les différentes plateformes de l'entreprise en une seule. Il s'agit alors, en développant un ensemble d'expériences maximalistes et interconnectées aux confins du réel et du virtuel, de favoriser l'avènement de l'Internet incarné[25].

§ 2 – UNE TECHNOLOGIE PROPICE AUX ARNAQUES

Les cryptomonnaies comme les NFT ne sont pas régulés par un organisme modérateur centralisé. Ils font l'objet de mouvements spéculatifs pouvant entraîner aussi bien des gains importants que des pertes abyssales. Face à ces risques, la loi PACTE[26] renforce les pouvoirs de l'Autorité des marchés financiers (AMF) créée en août 2003. Cette institution dont la mission première est la protection de l'épargne investie en produits financiers, a désormais la possibilité de vérifier si l'offre proposée présente assez de garanties pour les traders et de délivrer un visa aux acteurs respectant un certain nombre de critères de protection des épargnants. Elle a ainsi mis en place et tient à jour une liste noire accessible en ligne[27] des sites et sociétés d'intermédiaires bannies du Forex.
L'AMF propose aussi des listes blanches de structures ayant sollicité et reçu un label pour leurs services[28].

---

[24] « *Considérant que l'avenir [des] mondes virtuels sera radieux, le fonds décentralisé dédié aux NFTs BlackPool vient d'acquérir toutes les parcelles liées à la tour Eiffel dans le métaverse d'OVR. Sous la forme d'un NFT rarissime comportant 60 OVRLands, celui-ci a trouvé son premier acquéreur le 30 avril [2021] pour la somme de 38,6159 ETH, soit l'équivalent de près de 105 000 dollars au moment de la vente* ». Extrait de « Le fonds décentralisé BlackPool acquiert la tour Eiffel dans le monde virtuel d'OVR », 3 août 2021, *Cryptoas,* à https://cryptoast.fr/fonds-decentralise-blackpool-tour-eiffel-monde-ovr/ (consulté le 29 juin 2022).
[25] Léa MENARD, « Le metaverse de Facebook, c'est quoi ? », *TBS Press*, 26 novembre 2021, disponible à :
https://rdvc.fr/2021/11/26/le-metaverse-de-facebook-cest-quoi/#:~:text=Le%20metaverse%20de%20Facebook%20est%20une%20nouvelle%20collection,d%E2%80%99univers%20conscient%20de%20lui-m%C3%AAme%20%C3%A0%20l%E2%80%99int%C3%A9rieur%20d%E2%80%99un%20autre (consulté le 29 juin 2022).
[26] Loi n° 2019-486 du 22 mai 2019 *relative à la croissance et la transformation des entreprises*.
[27] Les listes noires des sociétés et sites non autorisés sont disponibles à :
https://www.amf-france.org/fr/espace-epargnants/proteger-son-epargne/listes-noires-et-mises-en-garde#popin-download.
[28] La liste des prestataires de services en actifs numériques (PSAN) enregistrés auprès de l'AMF est disponible à :
https://www.amf-france.org/fr/espace-professionnels/fintech/mes-relations-avec-lamf/obtenir-un-enregistrement-un-agrement-psan#Liste_des_PSAN_enregistrs_auprs_de_lAMF, mars par contre au 30 juin 20122, aucun PSAN n'est agréé auprès de l'AMF.

A) Une technologie accessible au travers de plateformes spécialisées

L'accès aux cryptomonnaies ou aux NFT nécessite l'utilisation d'une plateforme d'accès proposant des services sur actifs numériques.

1) Les plateformes d'échange de crypto-valeurs

L'utilisation d'une plateforme de trading de cryptomonnaies permet à partir d'une seule plateforme ou prestataire de services sur actifs numériques d'avoir accès à plusieurs cryptomonnaies, c'est-à-dire à plusieurs blockchains. Les principales plateformes utilisent un accès internet pour leurs services mais aussi une application mobile pour smartphone.
La première opération nécessaire à l'achat d'actifs numériques est la création d'un compte sur une plateforme d'échange. Certaines plateformes, comme eToro, proposent des services de dépôts de fonds variés, carte bancaire, virement SEPA, services PayPal, etc.
Alors que l'achat et la vente de cryptomonnaie est anonyme, seule l'identification du portefeuille est nécessaire, les plateformes d'échange enregistrées auprès d'une autorité telle l'AMF, nécessitent une connaissance des utilisateurs afin de respecter les réglementations sur le blanchiment d'argent.
Une fois le compte créé et des fonds déposés, il devient possible d'acheter divers actifs numériques.
Les cryptoactifs peuvent être laissés sur le portefeuille ayant servi aux échanges ou être transférés dans un portefeuille logiciel connecté en ligne ou enregistré sur un support externe, clé USB ou disque. L'enregistrement externe peut sembler le plus sécurisé, mais tout dysfonctionnement du support fait perdre le portefeuille enregistré avec son contenu.
Il est également possible d'échanger des cryptomonnaies en peer-to-peer en se connectant sur des sites spécialisés par cryptomonnaie (LocalBitcoins pour le Bitcoin, LocalEtherum.com pour l'Ether, ou https://localcryptos.com/ pour le Bitcoin, l'Ether, le Litecoin, le Dash ou le Bitcoin Cash). Ces sites sont plus complexes à utiliser et comme ce sont des sites peer-to-peer, l'acheteur est face à son vendeur et doit lui faire confiance.
Il existe des places de marché (*marketplace* en anglais) pour les NFT qui fonctionnent selon le même principe après dépôt des NFT sur la place de marché et connexion d'un portefeuille de cryptomonnaie.

2) Les plateformes et la loi PACTE

La loi PACTE définit ce qu'est un actif numérique :

> « Pour l'application du présent chapitre, les actifs numériques comprennent : 1° Les jetons mentionnés à

> l'article L. 552-2[29], 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 »[30].

Cette définition inclut les cryptomonnaies et les jetons non fongibles ou NFT. Ces actifs numériques peuvent faire l'objet de services. Les services sur actifs numériques sont définis par le livre X du Code monétaire et financier. Ils concernent :

> « 1° Le service de conservation pour le compte de tiers d'actifs numériques ou d'accès à des actifs numériques, le cas échéant sous la forme de clés cryptographiques privées, en vue de détenir, stocker et transférer des actifs numériques ; 2° Le service d'achat ou de vente d'actifs numériques en monnaie ayant cours légal ; 3° Le service d'échange d'actifs numériques contre d'autres actifs numériques ; 4° L'exploitation d'une plateforme de négociation d'actifs numériques ; 5° Les services suivants : La réception et la transmission d'ordres sur 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 d'actifs numériques ; Le placement garanti d'actifs numériques ; Le placement non garanti d'actifs numériques.[31]»

Les prestaires de services en ligne non référencées par l'AMF ne peuvent pas proposer de services financiers sur le territoire français, mais internet permet d'accéder aux plateformes non référencées.

Chaque PSAN doit communiquer à ses clients des informations claires, exactes et non trompeuses, notamment les informations à caractère promotionnel, qui sont identifiées en tant que telles et avertir ses clients des risques associés aux actifs numériques.

De la qualité de ces plateformes dépend la sécurité des transactions.

---

[29] Code monétaire et financier, article L.552-2 : « *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* ».

[30] Code monétaire et financier, Chapitre X, Article L54-10-1, créé par l'article 86 de la loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises.

[31] Code monétaire et financier, Chapitre X, article L54-10-2.

B) Une sécurité des transactions non garantie

Les cryptomonnaies et les NFT sont des valeurs spéculatives dont la valeur ne dépend que de l'équilibre entre l'offre et la demande. Le nombre des bitcoins est limité par construction du système et la création de nouveaux bitcoins par minage devient de plus en plus couteux pour les sociétés de minage en relation avec le nombre de bitcoins déjà créés.
Ces mécanismes doivent protéger la valeur des cryptomonnaies, les sociétés de minage obtenant de nouvelles valeurs à coup élevé, n'ont aucun intérêt à brader ces nouvelles valeurs. Le marché étant inflationniste devrait voir la valeur des cryptomonnaies augmenter tant que la confiance perdure et que le marché est actif. Comme toute valeur spéculative non régulée, les cryptomonnaies connaissent de fortes variations de cours[32]. Les spéculateurs attirés par des gains faciles voient leur portefeuille fondre. Des États ayant opté pour le bitcoin comme monnaie légale voient leurs réserves disparaître[33]. Des sociétés de minage se retrouvent en situation de faillite.
Les NFT connaissent également un recul de leur valeur spéculative. Outre l'insécurité des valeurs spéculatives, la fiabilité des plateformes peut provoquer la perte des sommes investies. La loi PACTE tente de fiabiliser les plateformes opérant sur le territoire français[34], mais il faut noter que si plusieurs plateformes se sont fait référencer par l'AMF, aucune n'a reçu d'agrément.

1) Les cyberattaques contre les cryptomonnaies

Les algorithmes utilisés par les blockchains et par les plateformes d'accès sont programmés dans des langages informatiques et fonctionnent sur des ordinateurs en réseau. À ce titre, ils peuvent être l'objet de cyberattaques.
En juillet 2016, l'équipe de développement d'Ethereum a dû procéder à un *hard fork* après une attaque réussie par un groupe de pirates sur un fonds d'investissement en Ether appelé The DAO (*Decentralized Autonomous Organization*) dans laquelle près de 3 641 694 ETH (soit plus de 5 % du montant total de la crypto-monnaie en circulation, équivalant à 55 millions de USD) ont été détournés. Ce *hard fork* a permis d'annuler le détournement et de restituer ses fonds à l'organisation autonome décentralisée[35]. Ce changement

[32] Fin juin 2022, toutes les cryptomonnaies connaissent une baisse importante de cours : le bitcoin a chuté de 69 000 $ à environ 20 000 $, l'ether de 4 500 $ à 1 000 $.
[33] C'est le cas du Salvador pour échapper à la pression du dollar ou de la République centrafricaine pour payer le groupe de mercenaires russes Wagner [B. MANENTI, « Les fauchés des cryptomonnaies : "Je m'en veux d'avoir cru ceux qui disaient que c'était facile de devenir millionnaire" », *L'OBS*, 30 juin 2022, consulté le 30 juin 2022].
[34] Loi n° 2019-486 du 22 mai 2019, *op.cit.*
[35] K. DOTSON, « Ethereum DAO attacked, over $55 million of Ether cryptocurrency stolen », *siliconANGLE,* 17 juin 2016, consulté à : https://siliconangle.com/2016/06/17/ethereum-dao-attacked-over-55-million-of-ether-cryptocurrency-stolen/ (consulté le 4 juillet 2022).

n'a pas recueilli un consensus absolu de la communauté et une faible partie de la communauté n'a pas implémenté ce changement sur les plateformes, divergence qui a conduit à la formation de deux chaînes de blocs séparées : l'une officielle avec pour unité monétaire l'Ether (ETH) et son spin-off avec pour unité monétaire l'Ether classique (ETC)[36].

Ethereum a connu une cyberattaque le 14 septembre 2021[37]. Les assaillants ont pu émettre une chaîne d'environ 550 blocs, contenant de fausses informations, destinées à tromper la vigilance du réseau de cette monnaie virtuelle. La quasi-totalité des nœuds d'Ethereum ont automatiquement rejeté ces blocs de données factices, puisque leurs preuves de travail n'ont pas été validées. Seuls les nœuds exécutés par le client Nethermind sont tombés dans le piège en adoptant la fausse version de la blockchain, diffusée par les attaquants du réseau. Cette attaque, bien que non aboutie, doit alerter les gestionnaires des différentes cryptomonnaies. Malgré le niveau avancé de sécurité informatique de ces monnaies virtuelles, il est nécessaire pour eux de maintenir à jour et de moderniser leurs systèmes de cybersécurité et ne pas se satisfaire du niveau actuel qui facilite l'intrusion des hackers toujours plus inventifs.

Fin mars 2022, des pirates ont mené une cyberattaque sophistiquée contre la blockchain Ronin. D'après le FBI, le groupe de hackers Lazarus pourrait être derrière cette opération, désormais renommée « Ronin Validator Security Breach ». La société Ronin Network, à l'origine de la blockchain Ronin et du jeu Axie Infinity, a déclaré être « toujours en train d'ajouter des mesures de sécurité supplémentaires avant de remettre en ligne le jeu, pour atténuer les risques futurs. Il faudra attendre fin avril pour pouvoir de nouveau profiter du jeu ». Après cette attaque, les ponts permettant de transférer des fonds entre d'autres blockchains et Axie Infinity a été temporairement bloqué[38].

Mais l'insécurité peut aussi venir des plateformes ou de leurs gestionnaires.

2) L'insécurité liée aux gestionnaires de plateformes

Les cryptomonnaies, les NFT et les métavers sont l'objet de mouvements spéculatifs et à ce titre attirent des investisseurs attirés

[36] P. RIZZO, « Ethereum Hard Fork Creates Competing Currencies », *CoinDesk,* 24 juillet 2016, disponible à https://www.coindesk.com/markets/2016/07/24/ethereum-hard-fork-creates-competing-currencies/ (consulté le 4 juillet 2022).

[37] Yoann, « Le monde de la crypto en panique : une attaque sur le réseau ethereum », *L'univers Cyber*, 26 octobre 2021, disponible à https://www.cybersecurity-guide.com/le-monde-de-la-crypto-en-panique-une-attaque-sur-le-reseau-ethereum/ (consulté le 4 juillet 2022).

[38] V. CIMINO, « Les hackers nord-coréens de Lazarus ont volé 500 millions d'euros en Ethereum », *SiecleDigital,* 18 avril 2022, disponible à : https://siecledigital.fr/2022/04/18/les-hackers-nord-coreens-de-lazarus-ont-vole-500-millions-deuros-en-ethereum/ (consulté le 4 juillet 2022).

par un gain rapide et facile. De plus, les intervenants sont anonymes, reconnus seulement par l'identification de leur portefeuille ou *wallet*, anonymat utilisé pour l'achat de biens illicites ou pour le blanchiment d'argent.
Dans ce monde parallèle, certains intermédiaires n'agissent que pour capter l'argent réel de spéculateurs cupides.
Sur les marchés financiers traditionnels, les intervenants sont parfois obligés d'utiliser les services d'intermédiaires agréés, en anglais *brokers,* qui seuls peuvent agir sur les marchés. Les manipulations de ces marchés restent possibles. En effet, il est possible de lancer un ordre de vente massif de valeur pour en faire baisser le cours, d'annuler cet ordre avant son exécution, mais dans le laps de temps court où la valeur a baissé de passer un ordre d'achat réel pour une moindre quantité. Les organismes de gestion des marchés financiers en association avec les autorités de régulation traquent ces opérations frauduleuses. Cette régulation n'existe pas sur le marché des cryptomonnaies.
Des conseils de sécurité existent pour éviter les arnaques des intermédiaires véreux : investir directement sur des cryptomonnaies et non sur des produits dérivés ; éviter le démarchage indirect et sélectionner l'intermédiaire parmi les plateformes de service agréées auprès de l'AMF ou au moins référencées par l'AMF[39] qui sont seules habilitées à intervenir sur le territoire français ; ne pas croire que ces opérations à fort rendement sont sans risques ; ne pas réinvestir pour « sécuriser » les premiers versements avant d'avoir vérifié la réalité de l'investissement[40].
Parmi les principales arnaques, propres au monde des cryptomonnaies ou non, il est possible de citer : La disparition brutale du site d'accès à la plateforme d'échange qui provoque ainsi la disparition des cryptomonnaies gérées par le site (en février 2014, le mont Gox a suspendu toute possibilité d'échanges, faisant disparaître plus de 85 000 bitcoins[41]) ; La pyramide de Ponzi qui est un montage financier frauduleux qui consiste à rémunérer les investissements des clients essentiellement par les fonds procurés par les nouveaux entrants. Si l'escroquerie n'est pas découverte, elle apparaît au grand jour au moment où elle s'écroule, c'est-à-dire quand les sommes procurées par les nouveaux entrants ne suffisent plus à couvrir les rémunérations des premiers clients ; Les ICO

[39] Cf. note 28.
[40] Il existe des sites donnant des conseils pour investir en toute sécurité dans les cryptomonnaies, par exemple :
https://kingcoin.fr/comment-investir-dans-les-crypto-monnaies-en-toute-securite/
ou https://www.net-investissement.fr/placement/cryptomonnaies/comment-acheter-des-cryptomonnaies-en-toute-securite-3509.html (consultés le 4 juillet 2022).
[41] G. CUOFANO, « Qu'est-il arrivé au mont Gox ? », *FourWeekMBA*, 1 mai 2022, disponible à :
https://fourweekmba.com/fr/qu%27est-il-arriv%C3%A9-%C3%A0-mt-gox/
(consulté le 4 juillet 2022) ;
Cryptus, « Le hack de MT. Gox et Mark Karpelès : le dossier complet », *CryptoSous*, 12 août 2018, disponible à https://www.crypto-sous.fr/mt-gox/ (consulté le 4 juillet 2022).

(Initial Coin Offering) ou les introductions en bourse de nouvelles cryptomonnaies par des startups qui créent des offres initiales pour la vente de leurs cryptomonnaies dans l'objectif de lever des sommes substantielles d'argent. Cependant, beaucoup d'entre elles surestiment largement la valeur de leur démarrage, et ces introductions ne sont souvent que des méthodes d'aspiration ; Les groupes de Pump & Dump qui utilisent Telegram ou Facebook pour manipuler les marchés. Dans un premier temps, les initiateurs achètent un nombre significatif de valeurs pour faire monter les cours et inciter d'autres acheteurs à les suivre. Dès que le nombre d'acheteurs devient suffisant et important, ils revendent leurs valeurs en empochant une forte plus-value mais provoquent la chute des cours des valeurs détenues par les derniers acheteurs[42] ; L'hameçonnage, autre forme courante d'escroquerie dans le monde de la cryptomonnaie, qui consiste à tenter d'obtenir les informations de connexion aux plateformes d'exchange ou les clefs privés de portefeuille en trompant et en manipulant les propriétaires ; Les utilisateurs de réseaux sociaux qui se faisant passer pour des personnalités du monde des cryptomonnaies demandent un versement sur un compte donné en échange d'une plus-value importante qui ne viendra jamais ; Les fausses publicités qui envoient vers un site d'échange de cryptomonnaies contrefait pour réaliser une opération d'hameçonnage ou *phishing*.

D'autres arnaques peuvent apparaître selon l'imagination des arnaqueurs. En mars 2022, 20 minutes faisait état d'une nouvelle arnaque, baptisée *CryptoRom* et faisant l'objet d'une alerte de la société Sophos[43]. L'arnaque consiste à inciter un utilisateur Android ou I-Phone à installer une fausse application de transfert de cryptomonnaie.

CONCLUSION

Si les technologies blockchain sont réputées fiables, sécurisées, robustes, les plateformes nécessaires pour y accéder peuvent présenter des failles de sécurité exploitables par des hackers. De plus, l'appât d'un gain rapide et facile peut pousser à utiliser des plateformes non sûres, mises en place par des arnaqueurs qui feront main basse sur les sommes investies.

Des précautions doivent donc être prises lors de l'utilisation de ces plateformes. L'utilisation de portefeuilles d'actifs numériques sur support externe, type clé USB, doit être privilégiée tout en sachant que de tels supports peuvent se dégrader dans le temps et que comme un portefeuille réel ils peuvent être volés ou perdus.

[42] Y. ZOUHAIR, « Crypto : le pump-and-dump, manipulation à un milliard de dollars », *pressecitron,* 28 août 2018, disponible à https://www.presse-citron.net/crypto-pump-dump-manipulation-milliard-dollars/ (consulté le 4 juillet 2002).

[43] « Cryptomonnaie : Une nouvelle arnaque circule », *20 minutes,* 18 mars 2022, disponible à https://www.20minutes.fr/high-tech/3255407-20220318-cryptomonnaie-nouvelle-arnaque-circule (consultée le 4 juillet 2022).

BIBLIOGRAPHIE

BAUDIÈRE (de la) L. et MIS J-M., *Rapport d'information déposé en application de l'article 145 du Règlement par la Mission d'information commune sur les chaînes de blocs (blockchains)*, Assemblée Nationale, 12 décembre 2018

DE FILIPPI P., *Blockchain et cryptomonnaies*. Presses Universitaires de France, « Que sais-je ? », 2022, ISBN : 9782715409484

FAVIER J., LÉCRIVAIN J-S., TAKKAL-BATAILLE A., *Bitcoin et protocoles à blockchain. Comprendre l'avènement de la seconde ère numérique*, Mardaga, « Gestion, Entreprise, Finance », 2019, ISBN : 9782804707729

GAYARD L, *Comprendre les NFT et les metavers*, Slatkine et Cie, 20 janvier 2022, ISBN : 2889442047

RODRIGUEZ P., *La Révolution Blockchain. Algorithmes ou institutions, à qui donnerez-vous votre confiance?*, Dunod, « Hors collection », 2017, ISBN : 9782100763603