

UNIVERSITÉ DU QUÉBEC À MONTRÉAL

**BLOCKCHAIN ET PROTECTION DES DROITS HUMAINS :
OPPORTUNITÉS ET DÉFIS JURIDIQUES D'UNE
RÉVOLUTION NUMÉRIQUE**

**TRAVAIL DE RECHERCHE DIRIGÉ BIDISCIPLINAIRE
PRÉSENTÉ
COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN DROIT**

**PAR
OUSSAMA KOUNNA**

JUILLET 2026

UNIVERSITÉ DU QUÉBEC À MONTRÉAL
Service des bibliothèques

Avertissement

La diffusion de ce document diplômant se fait dans le respect des droits de son auteur, qui a signé le formulaire *Autorisation de reproduire et de diffuser un travail de recherche de cycles supérieurs* (SDU-522 – Rév. 12-2023). Cette autorisation stipule que «conformément à l'article 11 du Règlement no 8 des études de cycles supérieurs, [l'auteur] concède à l'Université du Québec à Montréal une licence non exclusive d'utilisation et de publication de la totalité ou d'une partie importante de [son] travail de recherche pour des fins pédagogiques et non commerciales. Plus précisément, [l'auteur] autorise l'Université du Québec à Montréal à reproduire, diffuser, prêter, distribuer ou vendre des copies de [son] travail de recherche à des fins non commerciales sur quelque support que ce soit, y compris l'Internet. Cette licence et cette autorisation n'entraînent pas une renonciation de [la] part [de l'auteur] à [ses] droits moraux ni à [ses] droits de propriété intellectuelle. Sauf entente contraire, [l'auteur] conserve la liberté de diffuser et de commercialiser ou non ce travail dont [il] possède un exemplaire.»

REMERCIEMENTS

Je tiens tout d’abord à exprimer ma profonde gratitude à mon directeur de projet, Monsieur Bernard Duhaime. Ce fut un immense honneur de bénéficier de votre expertise et d’être guidé par un professionnel aussi éminent. Votre cours sur les droits humains et l’intelligence artificielle a constitué le point de départ intellectuel de ce travail, c’est cette rencontre académique qui a inspiré la genèse de ce mémoire.

J’adresse ensuite mes remerciements les plus sincères à mes parents. Vos sacrifices ont été le socle de toutes les opportunités qui m’ont été offertes. Chaque réussite que je rencontre est le reflet de votre dévouement et de votre amour inconditionnel. Je mesure pleinement la chance que j’ai de vous avoir, et je vous serai éternellement reconnaissant pour tout ce que vous avez fait pour moi.

Une pensée toute particulière est dédiée à ma grand-mère, MiMa. Tes prières m’accompagnent chaque jour, et je suis convaincu qu’elles ont été une source constante de force et de sérénité dans mon parcours.

À ma sœur Samia, affectueusement surnommée ma « petite Einstein » : malgré ton jeune âge, la justesse de tes conseils m’a été précieuse tout au long de ce cheminement. J’adresse également mes remerciements à Yousra, ma confidente et ma psychologue de cœur, pour ton écoute attentive et tes conseils avisés dans tous les aspects de ma vie. *Hamdoullah* pour mes sœurs extraordinaires qui m’entourent et me soutiennent.

Ce projet m’a permis de mûrir intellectuellement et d’approfondir ma compréhension des enjeux complexes à l’intersection du droit et de l’intelligence artificielle. Il marque le début d’une réflexion continue sur une technologie en constante évolution, qui nous invite à repenser sans cesse nos cadres juridiques.

Enfin, et avant tout, j’exprime ma gratitude la plus profonde envers Dieu pour m’avoir guidé et accordé la force, la sagesse et l’opportunité d’arriver à ce stade de mon parcours.

فَإِنَّ مَعَ الْعُسْرِ يُسْرًا ﴿١﴾ إِنَّ مَعَ الْعُسْرِ يُسْرًا

القرآن الكريم 94:5-6

RÉSUMÉ

Ce travail de recherche porte sur la manière dont la technologie blockchain pourrait contribuer à la protection des droits humains, tout en examinant les défis juridiques qu'elle pose. La blockchain est une technologie qui fonctionne sans autorité centrale et qui enregistre les informations de façon permanente et transparente. Ces caractéristiques offrent de nouvelles possibilités pour sécuriser des données sensibles, renforcer la confiance dans les échanges numériques et garantir le respect de certains droits fondamentaux.

Cependant, cette technologie entre en tension avec plusieurs principes du droit. Son fonctionnement repose sur l'immutabilité des données, ce qui complique l'application de règles juridiques actuelles, notamment en ce qui concerne la vie privée, la protection des données personnelles et la responsabilité en cas de litige. De plus, son caractère mondial rend difficile son encadrement par des lois nationales fondées sur des frontières territoriales.

L'objectif principal de cette recherche est de mieux comprendre dans quelle mesure la blockchain peut être intégrée dans les cadres juridiques existants, sans compromettre les principes fondamentaux de protection des droits humains. Le travail propose aussi des pistes pour adapter la régulation juridique à cette nouvelle réalité technologique, afin de trouver un équilibre entre innovation et respect des normes légales.

Mots-clés : Blockchain ; droits humains ; protection des données personnelles ; RGPD ; identité numérique ; décentralisation ; responsabilité juridique ; souveraineté numérique ; aide humanitaire ; régulation internationale.

ABSTRACT

This research examines how blockchain technology can contribute to the protection of human rights while identifying the legal challenges it raises. Blockchain is a decentralized, immutable, and transparent distributed ledger technology that has evolved far beyond its original application in cryptocurrency transactions. Today, it holds significant promise in areas such as digital identity management for displaced persons, humanitarian aid distribution, and the traceability of public funds.

However, this technology creates fundamental tensions with existing legal frameworks. Its immutability conflicts with the right to erasure enshrined in the General Data Protection Regulation (GDPR). Its decentralized nature complicates the attribution of legal responsibility in the absence of a central authority. Its transnational reach challenges the territorial foundations of national legal systems and raises critical questions of digital sovereignty.

This research draws on a doctrinal and critical methodology to analyze these tensions across four axes: the technical foundations and human rights applications of blockchain; the legal challenges it poses under current regulatory frameworks; the prospects for adapted international governance; and existing technical and humanitarian solutions. The study concludes that the successful integration of blockchain into human rights frameworks depends on the capacity of legal systems to evolve toward flexible, adaptive, and technologically informed regulation — one capable of balancing innovation with the effective protection of fundamental rights.

Keywords: Blockchain; human rights; personal data protection; GDPR; digital identity; decentralization; legal responsibility; digital sovereignty; humanitarian aid; international regulation.

TABLE DES MATIÈRES

REMERCIEMENTS	IV
RÉSUMÉ	VI
ABSTRACT	VII
TABLE DES MATIÈRES	VIII
TABLE DES SIGLES ET ACRONYMES	X
INTRODUCTION	1
CONTEXTE GÉNÉRAL	4
PROBLÉMATIQUE	6
PERTINENCE BIDISCIPLINAIRE DU SUJET	8
HYPOTHÈSE	9
MÉTHODOLOGIE ET CADRE THÉORIQUE.....	10
<i>Analyse doctrinale</i>	10
<i>Méthode critique</i>	12
REVUE DE LA LITTÉRATURE	15
BLOCKCHAIN ET PROTECTION DES DONNÉES PERSONNELLES	15
RESPONSABILITÉ JURIDIQUE DANS UN SYSTÈME DÉCENTRALISÉ	16
RÉGULATION INTERNATIONALE ET SOUVERAINETÉ NUMÉRIQUE	17
IMPACT SOCIO-ÉCONOMIQUE ET ÉGALITÉ D’ACCÈS	18
CHAPITRE 1 : LA BLOCKCHAIN, UN OUTIL POUR LA PROTECTION DES DROITS HUMAINS	19
1.1 FONCTIONNEMENT DE LA BLOCKCHAIN	19
1.1.1. <i>L’immuabilité et la transparence des données</i>	19
1.1.2. <i>La décentralisation du système blockchain</i>	20
1.1.3. <i>La cryptographie asymétrique</i>	20
1.1.4. <i>La double dépense</i>	21
1.1.5. <i>Le processus de minage</i>	21
1.2 PRINCIPES FONDAMENTAUX ET ENJEUX JURIDIQUES DE LA BLOCKCHAIN	23
1.3 APPORTS DE LA BLOCKCHAIN À LA PROTECTION DES DROITS FONDAMENTAUX	25
1.4 LES DROITS ÉCONOMIQUES, SOCIAUX ET CULTURELS : UN ANGLE SOUVENT NÉGLIGÉ	26
1.5 LA CRISE DES RÉFUGIÉS	26
1.6 APPORT DE LA BLOCKCHAIN DANS LA GESTION DE L’IDENTITÉ DES RÉFUGIÉS.....	29
1.7 L’EMPREINTE SOCIALE DE LA BLOCKCHAIN	31
CHAPITRE 2 : LES DÉFIS JURIDIQUES DE LA BLOCKCHAIN : ENTRE PROTECTION DES INNOVATIONS ET RESPECT DES CADRES NORMATIFS	32
2.1 LE CADRE JURIDIQUE DE LA BLOCKCHAIN : RÉGULATION ET ADAPTATION DES NORMES EXISTANTES	34

2.1.1.	<i>L'encadrement de la blockchain en France : une approche précurseur</i>	35
2.1.2.	<i>L'Union européenne et MiCA : vers une régulation harmonisée</i>	35
2.1.3.	<i>La régulation de la blockchain au Canada : un cadre en évolution</i>	37
2.1.4.	<i>La régulation de la blockchain aux États-Unis : un cadre fragmenté</i>	38
2.2	LA BREVETABILITÉ DE LA BLOCKCHAIN : UN CADRE JURIDIQUE ENCORE INCERTAIN	41
2.3	LA PROTECTION DES DONNÉES ET LE RGPD : UN CONFLIT AVEC L'IMMUTABILITÉ DE LA BLOCKCHAIN	43
2.4	RESPONSABILITÉ JURIDIQUE DANS LA BLOCKCHAIN DÉCENTRALISÉE	47
2.5	L'INSTRUMENTALISATION CRIMINELLE DE LA BLOCKCHAIN	51
CHAPITRE 3 : VERS UNE RÉGULATION JURIDIQUE ADAPTÉE DE LA BLOCKCHAIN POUR LA PROTECTION DES DROITS HUMAINS		52
3.1	LES LIMITES D'UNE APPROCHE PUREMENT NATIONALE.....	52
3.2	VERS UNE COORDINATION MULTILATÉRALE : L'INTÉRÊT DES ORGANISATIONS INTERNATIONALES.	54
3.3	RÉFORME DE LA RESPONSABILITÉ DANS LES SYSTÈMES DÉCENTRALISÉS	56
3.4	LA SOUVERAINETÉ NUMÉRIQUE ET LA NÉCESSITÉ D'UNE APPROCHE GLOBALE.....	58
CHAPITRE 4 : SOLUTIONS EXISTANTES POUR LA BLOCKCHAIN ET LA PROTECTION DES DROITS HUMAINS		60
4.1	INITIATIVES TECHNIQUES POUR MIEUX PROTÉGER LES DONNÉES	61
4.2	PROJETS HUMANITAIRES ET SOCIAUX S'APPUYANT SUR LA BLOCKCHAIN	63
4.3	PARTENARIATS PUBLIC-PRIVÉ UTILISANT LA BLOCKCHAIN DANS L'AIDE HUMANITAIRE	65
CONCLUSION		67
BIBLIOGRAPHIE		70

TABLE DES SIGLES ET ACRONYMES

Sigle	Définition complète
RGPD	Règlement général sur la protection des données
MiCA	Markets in Crypto-Assets (Règlement européen sur les marchés de crypto-actifs)
PSAN	Prestataire de Services sur Actifs Numériques
ICO	Initial Coin Offering
CNIL	Commission Nationale de l'Informatique et des Libertés (France)
EUDI	European Digital Identity Wallet (portefeuille d'identité numérique européen)
DSA	Digital Services Act (Règlement européen sur les services numériques)
DMA	Digital Markets Act (Règlement européen sur les marchés numériques)
DLT	Distributed Ledger Technology (technologie de registre distribué)
MNBC	Monnaie numérique de banque centrale
AMF	Autorité des marchés financiers (France)
SEC	Securities and Exchange Commission (États-Unis)
CFTC	Commodity Futures Trading Commission (États-Unis)
IRS	Internal Revenue Service (États-Unis)
FinCEN	Financial Crimes Enforcement Network (États-Unis)
DApps	Applications décentralisées
CANAFE	Centre d'analyse des opérations et déclarations financières du Canada
OEB	Office Européen des Brevets

INTRODUCTION

Les technologies numériques ont profondément redessiné les contours de nos systèmes économiques et juridiques. Cette transformation a favorisé l'émergence de nouveaux outils visant à repenser les mécanismes de confiance, de sécurité et de gouvernance des échanges.

Parmi ces innovations, la blockchain se démarque par ses caractéristiques singulières : elle est décentralisée, infalsifiable et offre une grande transparence. Il s'agit d'une technologie de stockage et de transmission de données reposant sur un registre distribué, sécurisé par des mécanismes cryptographiques et fonctionnant sans autorité centrale¹.

À l'origine, elle a été pensée pour sécuriser les transactions liées aux cryptomonnaies, mais ses usages ne se limitent plus à ce seul domaine. Aujourd'hui, elle suscite un vif intérêt dans des secteurs aussi variés que la protection des libertés fondamentales, la gestion de l'identité numérique ou encore la traçabilité des opérations, notamment dans une optique de transparence renforcée².

Cela dit, malgré ses promesses, la blockchain soulève également d'importants défis juridiques. Son immuabilité, qui fait sa force en matière de sécurité, entre parfois en contradiction avec certains droits fondamentaux, comme le droit à l'oubli, inscrit dans le Règlement général sur la protection des données (RGPD)³. De plus, l'absence d'une autorité centrale de contrôle complique la détermination des responsabilités juridiques en cas de litige. Cette décentralisation rend floue la question de la gouvernance et du recours en justice. Enfin, du fait de son fonctionnement transnational, la blockchain échappe souvent aux cadres juridiques traditionnels, fondés sur des

¹ CNIL, « Blockchain », consulté le 2 février 2025, <https://www.cnil.fr/fr/definition/blockchain>

² Boris Barraud, Les blockchains et le droit, Revue Lamy Droit de l'immatériel, n° 147, avril 2018, p. 1

³ Rahime Belen-Saglam et al., A Systematic Literature Review of the Tension between the GDPR and Public Blockchain Systems, arXiv preprint arXiv:2210.04541, 2022. P.2

principes de territorialité et de souveraineté numérique, ce qui constitue un véritable casse-tête pour les législateurs⁴.

Sur le plan doctrinal, ce travail s'appuie dans le prolongement des recherches de Primavera De Filippi, Aaron Wright et Michèle Finck sur les rapports entre blockchain et droit, ainsi que des réflexions de Kevin Werbach sur la gouvernance des technologies décentralisées. Ces auteurs et autrices ont posé les bases d'une réflexion juridique rigoureuse sur la blockchain, que cette recherche cherche à prolonger en l'ancrant dans le champ des droits humains et du droit international. Ces ancrages théoriques conduisent à une question qui traverse l'ensemble de cette recherche : Dans quelle mesure la blockchain peut-elle contribuer à la protection des droits humains sans entrer en contradiction avec les normes juridiques existantes, et comment le droit pourrait-il évoluer pour intégrer cette technologie décentralisée ?

Pour répondre à cette question, ce travail s'organise autour de quatre grands axes de réflexion, chacun apportant un éclairage complémentaire sur les liens entre blockchain et protection des droits humains.

Le premier axe vise à poser les bases techniques de la blockchain, en expliquant son fonctionnement et ses caractéristiques essentielles, telles que la décentralisation, l'immutabilité et la transparence. Il s'agira aussi d'en analyser les usages actuels dans des contextes sensibles, comme la distribution d'aide humanitaire ou la création d'identités numériques pour des populations marginalisées. Ce chapitre montrera en quoi la blockchain peut constituer un levier pour renforcer la traçabilité, lutter contre la fraude et garantir l'intégrité des données.

Le deuxième axe portera sur les limites juridiques que cette technologie peut rencontrer. Il examinera les tensions existantes entre les principes fondamentaux du droit, notamment ceux liés à la protection des données personnelles, et les propriétés techniques de la blockchain, comme l'impossibilité d'effacer ou de modifier une information une fois enregistrée. Seront également

⁴ La difficile appréhension des blockchains par le droit, *Revue internationale de droit économique*, 2018/4, p. 453

abordées les questions de responsabilité juridique dans un système sans autorité centrale, ainsi que les difficultés d'encadrement d'une technologie par nature transnationale.

Le troisième axe sera consacré aux perspectives d'adaptation des cadres juridiques actuels. Il examinera les pistes envisageables pour encadrer l'usage de la blockchain sans en freiner le potentiel. Parmi ces solutions, on s'intéressera notamment à la mise en place d'une gouvernance hybride mêlant régulation publique et autorégulation des acteurs, mais aussi à l'intégration de mécanismes de conformité ou de contrôle éthique. Des initiatives comme le règlement MiCA, porté au niveau européen, seront analysées pour mesurer les avancées et les limites d'une régulation sectorielle en construction.

Enfin, le quatrième et dernier axe s'appuiera sur des exemples concrets déjà mis en œuvre dans différents contextes, afin de montrer comment la blockchain est actuellement mobilisée pour répondre à des enjeux liés aux droits humains. Qu'il s'agisse d'initiatives portées par des institutions internationales, des ONG ou des partenariats public-privé, cette partie cherchera à mettre en lumière les usages réels de cette technologie sur le terrain. Elle permettra ainsi de mieux cerner les opportunités qu'offre la blockchain, les difficultés qu'elle soulève dans sa mise en œuvre, ainsi que les leçons que l'on peut en tirer en matière d'encadrement juridique. L'objectif est d'identifier, à partir de ces expériences, des pistes de réflexion pour une utilisation plus maîtrisée, conforme aux exigences de protection des droits fondamentaux.

Cette recherche vise ainsi à évaluer dans quelle mesure la blockchain peut être intégrée de manière cohérente dans les systèmes juridiques existants, sans compromettre les principes de transparence, de responsabilité et de protection des droits fondamentaux. Plus largement, il s'agit d'interroger la capacité du droit à s'adapter à une technologie en constante évolution, tout en garantissant les libertés individuelles dans un monde numérique.

CONTEXTE GÉNÉRAL

Dans un monde de plus en plus numérisé, la blockchain s'impose comme une technologie émergente susceptible de répondre à des enjeux structurels majeurs en matière de transparence, de traçabilité et de confiance. Fondée sur une architecture distribuée, elle repose sur la validation autonome des transactions par un réseau d'ordinateurs à l'aide de protocoles de consensus. Ce fonctionnement garantit trois principes fondamentaux qui la distinguent des systèmes traditionnels : la décentralisation, l'immuabilité et le pseudonymat⁵.

L'absence d'autorité centrale limite les risques de contrôle unilatéral⁶, tandis que l'immuabilité des données assure que les informations enregistrées ne peuvent être modifiées sans l'accord de la majorité du réseau⁷. Le pseudonymat, quant à lui, permet aux utilisateurs d'interagir sans divulguer directement leur identité, soulevant toutefois des enjeux importants en matière de protection des données personnelles⁸.

Ces caractéristiques ont conduit à des applications concrètes, notamment dans le domaine humanitaire. En 2017, les Nations Unies ont mené une expérimentation innovante en recourant à la blockchain pour la distribution de l'aide humanitaire aux réfugiés syriens et rohingyas en Jordanie et au Bangladesh. Cette initiative visait à assurer une traçabilité complète des fonds, tout en réduisant les risques de détournement et de corruption, illustrant ainsi le potentiel de la blockchain pour renforcer la protection des droits humains⁹.

⁵ CNIL, Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles, 2018.

⁶ La difficile appréhension des blockchains par le droit, *Revue internationale de droit économique*, 2018/4, p. 453.

⁷ Thibaut Labbé, *Le droit face aux technologies disruptives : le cas de la blockchain*, Thèse de doctorat, Université de Paris, 2021.

⁸ *Idem*.

⁹ Organisation des Nations Unies, "Blockchain Technology and Humanitarian Aid", disponible sur https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2020_7_french.pdf p.9 (consulté le 3 février 2025.)

Dans cette perspective, la blockchain permet de suivre la distribution des fonds humanitaires de manière efficace et sans risque de détournement ¹⁰. De plus, elle est vue comme un outil révolutionnaire pour garantir une identité numérique sécurisée, permettant à des millions de réfugiés et de personnes apatrides d'accéder à des services essentiels tels que l'éducation et la santé¹¹. Cela présente des opportunités uniques pour les populations vulnérables, souvent exclues des systèmes traditionnels de reconnaissance juridique et d'accès aux services publics.

Cette évolution technologique s'inscrit dans une dynamique plus large de transformation des modes de régulation. Historiquement, l'essor d'Internet dans les années 1990 avait déjà mis en évidence la capacité des technologies numériques à produire leurs propres formes de gouvernance. Le concept de Lex Informatica, introduit par Joel Reidenberg en 1998, souligne ainsi le rôle régulateur du code informatique, capable d'imposer des normes indépendamment des cadres juridiques étatiques¹². La blockchain prolonge cette logique en instaurant un système où la confiance repose principalement sur des protocoles algorithmiques plutôt que sur des institutions centralisées¹³.

La blockchain pousse encore plus loin cette logique d'auto-régulation par le code, en instaurant un système où la confiance repose exclusivement sur un protocole algorithmique, et non sur des institutions centralisées. Cette évolution rappelle les débats des débuts d'Internet, où certains théoriciens, tels que Timothy May et John Perry Barlow, considéraient le cyberspace comme un territoire affranchi de toute régulation étatique¹⁴. Internet a introduit une nouvelle ère de connectivité, mais il reste dépendant d'infrastructures centralisées (serveurs, fournisseurs d'accès). À l'inverse, la blockchain élimine ces points de contrôle en s'appuyant sur un registre totalement

¹⁰ Zwitter, A., & Boisse-Despiaux, M. (2018). *Blockchain for Humanitarian Action and Development*. *Journal of International Humanitarian Action*,

¹¹ *Idem*.

¹² Reidenberg, J. R., Lex Informatica: The Formulation of Information Policy Rules through Technology, *Texas Law Review*, 1998

¹³ Bruno Deffains, "Blockchain et justice décentralisée : un nouveau défi (Partie 2)", LexTech Institute, <https://www.lextechinstitute.ch/blockchain-et-justice-decentralisee-un-nouveau-defi-partie-2/>

¹⁴ Primavera de Filippi, Morshed Mannan, Wessel Reijers. Blockchain Technology and the Rule of Code: Regulation via Governance.p. Disponible sur : <https://hal.science/hal-03883249/document>

décentralisé, où chaque nœud du réseau joue un rôle équivalent. Cette caractéristique rend la blockchain plus résistante à la censure étatique, mais complique également son intégration dans les cadres juridiques traditionnels¹⁵.

La technologie de la blockchain, à l'instar de l'Internet, est aujourd'hui considérée comme un nouveau moyen d'échapper aux régulations territoriales et gouvernementales. Les arguments avancés par les premiers défenseurs de la blockchain sont similaires à ceux des pionniers d'Internet¹⁶. La décentralisation inhérente aux systèmes basés sur la blockchain favorise une gouvernance plus distribuée, limitant les risques de surveillance ou de contrôle par des structures centralisées, qu'elles soient étatiques ou privées. En raison de leurs caractéristiques distinctives, les plateformes blockchain sont parfois décrites comme « a-légales », opérant au-delà des cadres juridiques traditionnels¹⁷.

Ce potentiel décentralisé suscite un intérêt croissant pour son application aux droits humains, notamment dans des contextes où la surveillance gouvernementale et la censure représentent des risques importants pour les individus.

PROBLÉMATIQUE

La technologie blockchain met à l'épreuve plusieurs principes fondamentaux du droit contemporain. Un premier point de tension concerne le conflit entre l'immutabilité de la blockchain et le droit à l'oubli, consacré par le Règlement général sur la protection des données (RGPD) au sein de l'Union européenne. Ce droit permet à tout individu de demander la suppression de ses données personnelles. Or, par nature, les informations inscrites dans une blockchain ne peuvent pas être modifiées ni supprimées¹⁸. Cela crée un paradoxe : comment garantir le respect d'un droit

¹⁵ *Idem*.

¹⁶ Primavera de Filippi, Morshed Mannan, Wessel Reijers. Blockchain Technology and the Rule of Code: Regulation via Governance . p. 2 disponible sur : <https://hal.science/hal-03883249/document>

¹⁷ *Idem*.

¹⁸ Finck, M. (2019). Blockchain and the General Data Protection Regulation: Can Distributed Ledgers be Squared with European Data Protection Law? Journal of Data Protection & Privacy, p.6

fondamental dans un système conçu précisément pour rendre les données permanentes ? Ce dilemme juridique est au cœur des débats sur l'articulation entre innovation technologique et protection de la vie privée.

Un second défi concerne la responsabilité juridique dans un système décentralisé. Dans les systèmes traditionnels, une autorité centrale est responsable de la collecte, du traitement et de la sécurisation des données. Cette centralisation facilite l'identification des responsabilités en cas de faute ou de violation des droits. Dans une blockchain, en revanche, les décisions sont prises collectivement, par un réseau d'acteurs indépendants appelés « nœuds », chacun validant les transactions¹⁹. Cette gouvernance partagée rend difficile la désignation d'un responsable en cas de préjudice. Qui peut être tenu pour responsable dans un système où personne ne détient un contrôle exclusif²⁰ ?

De plus, la dimension transnationale de la blockchain remet en cause la notion même de juridiction. Une blockchain publique fonctionne sur des serveurs répartis dans le monde entier. Cela complique l'application des lois nationales, qui reposent sur des principes de territorialité. Par exemple, si des données personnelles d'un citoyen européen sont enregistrées sur une blockchain dont les nœuds sont situés aux États-Unis, en Chine ou au Brésil, quel cadre juridique s'applique ? Et quel tribunal peut être saisi en cas de litige ? Cette réalité oblige à repenser la souveraineté numérique des États face à une technologie qui dépasse les frontières classiques²¹ ?

Enfin, un autre enjeu important est celui de la durabilité écologique. Certaines blockchains, notamment celles qui utilisent le mécanisme de validation par preuve de travail (« Proof of Work »), comme Bitcoin, consomment énormément d'énergie. Ce modèle est de plus en plus critiqué pour son empreinte carbone, qui va à l'encontre des engagements internationaux en matière de lutte contre le réchauffement climatique. Intégrer la blockchain dans des systèmes respectueux des droits

¹⁹ *Idem.p.6*

²⁰ *Idem.p 6*

²¹ *Idem.p.9*

humains nécessite donc de prendre en compte aussi la dimension environnementale, souvent oubliée mais cruciale pour une approche globale des droits fondamentaux²².

Ces différentes tensions entre innovation technologique et protection des droits humains conduisent à une question centrale : comment articuler l'utilisation de la blockchain avec les normes juridiques internationales visant à garantir les libertés fondamentales ? Cette question implique non seulement des réponses techniques, mais aussi une réflexion profonde sur les fondements du droit, de la responsabilité juridique et de la souveraineté à l'ère numérique.

Pertinence bidisciplinaire du sujet

Le sujet traité dans ce travail se situe résolument à la croisée de deux disciplines : le droit et la technologie. Cette approche bidisciplinaire est non seulement pertinente, mais indispensable pour comprendre l'ensemble des enjeux soulevés par l'intégration de la blockchain dans le champ des droits humains.

Droit : Du côté juridique, il s'agit de confronter une technologie émergente à un ensemble de normes bien établies, souvent élaborées dans un contexte où les bases de données centralisées étaient la norme. Le RGPD, la Déclaration universelle des droits de l'homme, ou encore les chartes nationales sur les libertés publiques n'avaient pas anticipé l'apparition de registres décentralisés, immuables, et transnationaux²³. Ce décalage crée des tensions qu'une analyse purement technique ne saurait résoudre.

Technologie : Du côté technologique, la blockchain représente une rupture dans la façon dont les données sont créées, stockées, sécurisées et partagées. Comprendre son fonctionnement (nœuds, consensus, smart contracts, chiffrement, etc.) est essentiel pour ne pas tomber dans des approximations ou des peurs infondées. L'approche technique permet également d'identifier des

²² Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The Energy Consumption of Blockchain Technology: Beyond Myth. *Business & Information Systems Engineering*,

²³ Finck, M. (2019). Blockchain and the General Data Protection Regulation: Can Distributed Ledgers be Squared with European Data Protection Law? *Journal of Data Protection & Privacy*, 2(1), p.9

leviers d'action concrets : par exemple, la mise en œuvre de solutions de confidentialité avancées (zero knowledge proofs, private chains), ou l'utilisation de protocoles éco-responsables²⁴.

Ce croisement entre droit et technologie permet d'aborder des questions nouvelles, comme la légitimité des processus de gouvernance décentralisée, ou la reconnaissance juridique des décisions prises collectivement sur une blockchain. En d'autres termes, l'étude ne se limite pas à opposer une technologie innovante à des normes anciennes, elle vise à imaginer une rencontre possible, à travers un dialogue entre deux univers disciplinaires complémentaires²⁵. En définitive, ce travail s'inscrit dans une démarche résolument interdisciplinaire, pour explorer de manière nuancée les conditions dans lesquelles la blockchain peut contribuer à renforcer les droits fondamentaux, sans mettre en péril les principes juridiques qui les protègent.

Hypothèse

L'hypothèse centrale de ce travail repose sur l'idée qu'un équilibre est possible entre les potentialités techniques offertes par la blockchain et les exigences normatives des cadres juridiques existants. Si elle est juridiquement encadrée de manière adéquate, la blockchain peut devenir un outil de renforcement des droits fondamentaux plutôt qu'un facteur de menace. En effet, grâce à ses propriétés intrinsèques telles que la sécurité cryptographique, la transparence des transactions, ou encore l'absence de contrôle unique, cette technologie peut renforcer l'accès aux droits dans des contextes où les institutions sont fragiles ou corrompues. Elle peut, par exemple, contribuer à l'inclusion sociale via la création d'identités numériques sécurisées pour les personnes sans papiers ou déplacées.

Cependant, ces promesses ne peuvent être réalisées sans une adaptation des cadres juridiques actuels. Il est impératif de repenser certains principes, comme le droit à l'effacement ou la responsabilité des acteurs techniques. Certaines solutions existent déjà par exemple : des blockchains dites « hybrides », autorisant la suppression conditionnelle de données ; des smart

²⁴ Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. Penguin, p. 67

²⁵ *Ib.* p.68

contracts intégrant des clauses automatisées conformes au RGPD ; ou encore des instances de régulation supranationales capables de superviser l'usage des technologies distribuées dans le respect des droits fondamentaux.

L'hypothèse défendue est donc que le succès de l'intégration de la blockchain dans le champ des droits humains dépendra de la capacité des systèmes juridiques à évoluer vers des régulations souples, adaptatives et technologiquement conscientes, capables de garantir à la fois l'innovation et le respect des libertés fondamentales. Cette hypothèse sera testée à travers une analyse comparative de cas d'usage concrets, notamment dans les domaines de l'identité numérique, de la protection des données personnelles et de la gouvernance décentralisée.

Méthodologie et cadre théorique

Pour mener à bien cette recherche, une approche méthodologique mixte sera employée, combinant une analyse doctrinale approfondie, une étude critique des cas pratiques, et une perspective comparative. Ces méthodes sont choisies pour leur pertinence dans l'étude des problématiques juridiques complexes que pose la blockchain, mais également pour leur capacité à offrir une analyse complète et nuancée du cadre législatif en vigueur, tout en identifiant les réformes nécessaires pour concilier cette technologie avec la protection des droits humains.

Analyse doctrinale

L'analyse doctrinale est une approche essentielle pour toute recherche en droit, en particulier lorsqu'il s'agit d'examiner l'encadrement juridique d'une technologie émergente comme la blockchain. Cette méthode permet d'étudier en profondeur les textes juridiques, la jurisprudence et les travaux doctrinaux afin d'identifier les principes fondamentaux du droit, leurs interprétations et leur adéquation aux nouvelles réalités technologiques.

Dans le cadre de ce travail de recherche, l'analyse doctrinale est particulièrement pertinente pour plusieurs raisons. Premièrement, la blockchain est une technologie qui remet en cause certains principes classiques du droit, notamment en matière de protection des données personnelles, de responsabilité juridique et de régulation transnationale. L'analyse des sources normatives existantes

permet donc de comprendre comment le droit tente d'encadrer cette innovation et quelles en sont les limites. Par exemple, le Règlement Général sur la Protection des Données (RGPD) pose un cadre strict pour la gestion des données personnelles en Europe, mais il entre en contradiction avec l'un des principes fondamentaux de la blockchain : l'immutabilité des informations inscrites dans le registre. Une étude détaillée de ce texte et de ses interprétations jurisprudentielles est nécessaire pour évaluer dans quelle mesure il est applicable à cette technologie²⁶.

Deuxièmement, le cadre juridique de la blockchain est encore en construction. Contrairement à d'autres domaines du droit bien établis, comme le droit des contrats ou le droit pénal, la réglementation des technologies blockchain varie considérablement d'un pays à l'autre et est en constante évolution. Par conséquent, l'analyse des doctrines juridiques permet d'identifier les divergences dans les approches réglementaires et d'évaluer les tendances émergentes en matière de régulation. Par exemple, en France, la Loi PACTE de 2019 a introduit un cadre pour les prestataires de services sur actifs numériques, tandis qu'aux États-Unis, la réglementation de la blockchain est plus fragmentée, relevant à la fois de la Securities and Exchange Commission (SEC) et d'autres agences fédérales²⁷. Une approche doctrinale comparative permettra ainsi de mettre en lumière les différences d'interprétation entre ces systèmes.

Troisièmement, l'analyse doctrinale est indispensable pour comprendre les débats théoriques qui sous-tendent la régulation de la blockchain. Différentes écoles de pensée juridique s'opposent quant à la manière dont cette technologie devrait être encadrée. Certains auteurs considèrent que la blockchain, en tant que technologie fondée sur des règles immuables et automatiques, pourrait remplacer en partie l'intervention des institutions juridiques traditionnelles, une idée souvent résumée par l'expression "Code is Law", popularisée par Lawrence Lessig²⁸. D'autres juristes, en revanche, insistent sur la nécessité de préserver un contrôle humain et judiciaire sur les transactions effectuées via la blockchain, notamment en raison des enjeux éthiques et sociétaux qu'elle soulève.

²⁶ Finck, Michèle. Blockchain and the General Data Protection Regulation: Can Distributed Ledgers be Squared with European Data Protection Law? *Journal of Data Protection & Privacy*, vol. 2, no. 1, 2019, pp. 1-18.

²⁷ European Parliament and the Council of the European Union, Directive (EU) 2018/843 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (5AMLD), 30 May 2018.

²⁸ Lessig, Lawrence. *Code and Other Laws of Cyberspace*. Basic Books, 1999.

L'analyse doctrinale permet d'examiner ces différentes perspectives et d'en dégager les implications pratiques.

Enfin, l'étude des textes de loi, de la doctrine et de la jurisprudence est une étape essentielle pour formuler des propositions d'adaptation du droit. L'objectif d'un mémoire de recherche en droit n'est pas seulement de décrire l'état actuel du droit, mais aussi d'identifier les lacunes du système juridique et de suggérer des solutions. Par exemple, si l'analyse doctrinale révèle que le droit à l'oubli tel que prévu par le RGPD est difficilement compatible avec la blockchain, elle peut aussi mettre en lumière des pistes pour une adaptation du cadre réglementaire, comme la mise en place de mécanismes de suppression sélective des données ou d'outils cryptographiques permettant une gestion plus souple des informations personnelles²⁹.

Bref, l'analyse doctrinale constitue donc une méthode centrale dans ce travail, car elle permet d'analyser les fondements juridiques qui s'appliquent à la blockchain, d'identifier les tensions entre droit et technologie, d'évaluer les différentes approches doctrinales et de proposer des pistes d'évolution du cadre réglementaire.

Méthode critique

La méthode critique complète l'analyse doctrinale en apportant une perspective plus réflexive sur les limites des solutions juridiques actuelles. Alors que l'analyse doctrinale se concentre sur l'application et l'interprétation des normes existantes, la méthode critique vise à remettre en question les paradigmes juridiques traditionnels en examinant les tensions et contradictions générées par l'intégration de la blockchain dans les systèmes juridiques nationaux et internationaux. Contrairement à une approche purement descriptive qui se limite à exposer les textes en vigueur, la méthode critique permet d'interroger les fondements du droit, d'identifier ses limites et de mettre en évidence les incohérences des cadres normatifs actuels. Cette approche est particulièrement pertinente dans le contexte de la blockchain, une technologie qui bouleverse

²⁹ Zyskind, Guy, Nathan, Oz, & Pentland, Alex 'Sandy'. *Decentralizing Privacy: Using Blockchain to Protect Personal Data*. 2015 IEEE Security and Privacy Workshops.

plusieurs principes fondamentaux, notamment en matière de responsabilité juridique, de souveraineté numérique et de protection des données personnelles.

Un des principaux apports de la méthode critique est qu'elle permet de déconstruire les présupposés juridiques qui entourent la blockchain. Très souvent, cette technologie est perçue comme un instrument neutre et objectif qui favorise la transparence et la sécurité des transactions. Pourtant, une analyse plus poussée révèle qu'elle peut également générer de nouvelles formes de pouvoir et d'inégalités. Par exemple, le Conseil de l'Europe a mis en avant le paradoxe selon lequel, bien que la blockchain puisse renforcer la transparence et la traçabilité, elle peut aussi être utilisée à des fins de surveillance accrue et compromettre le droit à la vie privée des individus³⁰. De plus, l'absence d'une autorité centrale dans les systèmes blockchain soulève la question de la gouvernance et du contrôle: qui décide des règles encadrant ces réseaux ? Une approche critique permet d'examiner ces tensions et d'identifier les conséquences juridiques d'une régulation par le code plutôt que par la loi.

La méthode critique est également indispensable pour analyser les asymétries de pouvoir engendrées par la blockchain. Bien qu'elle soit souvent présentée comme une technologie décentralisée, la réalité montre que son contrôle reste concentré entre les mains d'une minorité d'acteurs, notamment les grandes plateformes d'échange de cryptomonnaies, les développeurs de protocoles et les acteurs institutionnels qui régulent son utilisation. Ainsi, alors que la blockchain était initialement conçue pour se libérer des intermédiaires traditionnels, son développement a paradoxalement conduit à la création de nouveaux monopoles et oligopoles technologiques. Cette concentration du pouvoir pose des questions fondamentales en matière de justice sociale et d'accès équitable aux technologies numériques³¹.

Un autre aspect important de la méthode critique est qu'elle permet de repenser les mécanismes de gouvernance et de régulation à l'ère des technologies décentralisées. En identifiant les défis pratiques et éthiques liés à l'utilisation de la blockchain, cette méthode permettra de proposer des

³⁰ Conseil de l'Europe, *L'impact des blockchains sur les droits de l'homme, la démocratie et l'État de droit*, 2022 p.30
Disponible sur : <https://rm.coe.int/report-on-blockchains-fr/1680a8ffe7>

³¹ *Idem.* p.23

pistes de réforme législative visant à assurer que cette technologie soit utilisée de manière éthique et en conformité avec les principes de protection des droits humains. Elle examinera également comment des solutions hybrides, telles que des régulations spécifiques à certains aspects de la blockchain (p.ex., la protection des identités numériques ou la traçabilité des transactions), pourraient être mises en place pour mieux répondre aux défis posés par cette technologie.

L'adoption d'une méthode critique dans cette recherche permet donc de dépasser une analyse purement descriptive et d'ouvrir une réflexion plus large sur les transformations qu'implique la blockchain pour le droit et la société. En mettant en lumière les tensions entre innovation technologique et régulation juridique, elle contribue à une meilleure compréhension des enjeux sous-jacents et permet d'orienter la réflexion vers des solutions équilibrées, conciliant progrès technologique et respect des droits humains.

La complémentarité de l'analyse doctrinale et de la méthode critique est essentielle pour une recherche juridique portant sur une technologie en constante évolution, telle que la blockchain. D'une part, l'analyse doctrinale fournit une base solide pour comprendre comment les cadres juridiques existants répondent aux défis posés par cette technologie, tout en garantissant une rigueur juridique dans l'interprétation des normes actuelles. D'autre part, la méthode critique permet une ouverture réflexive sur les nouvelles réalités créées par la blockchain, en identifiant les lacunes des systèmes juridiques traditionnels et en proposant des réformes pour intégrer cette technologie tout en respectant les droits fondamentaux.

Ces deux méthodes combinées permettent donc d'aboutir à une analyse complète et nuancée des opportunités et des défis liés à l'utilisation de la blockchain dans le cadre de la protection des droits humains. Cette approche permettra non seulement d'identifier les incompatibilités entre les régulations actuelles et les réalités techniques de la blockchain, mais également d'anticiper les réformes nécessaires pour encadrer l'adoption plus large de cette technologie.

REVUE DE LA LITTÉRATURE

La blockchain est l'une des technologies les plus prometteuses du XXI^e siècle, mais son intégration dans les cadres juridiques soulève des défis majeurs, notamment dans le domaine des droits humains. La littérature existante traite plusieurs aspects cruciaux : protection des données personnelles, responsabilité juridique dans les systèmes décentralisés, et compatibilité de cette technologie avec les réglementations internationales. Certains auteurs y voient un outil révolutionnaire pour renforcer la transparence, garantir la traçabilité et protéger les populations vulnérables, tandis que d'autres soulignent les risques juridiques, réglementaires et socio-économiques associés à son adoption.

L'objectif de cette revue de la littérature est d'examiner ces différentes perspectives en mettant en lumière les principales contributions académiques et en identifiant les lacunes qui doivent encore être comblées pour permettre une intégration harmonieuse de la blockchain dans les cadres légaux actuels.

Blockchain et protection des données personnelles

L'un des principaux défis soulevés par la blockchain dans le cadre juridique concerne la protection des données personnelles. Le Règlement général sur la protection des données (RGPD), adopté par l'Union européenne, établit des droits clairs pour les individus, tels que le droit à l'oubli, qui permet de demander l'effacement de données personnelles³². Toutefois, la nature immuable de la blockchain rend cette exigence juridique difficilement applicable.

Finck (2019) est l'un des principaux auteurs à avoir analysé cette incompatibilité entre la blockchain et le RGPD. Son travail démontre que l'immuabilité et la décentralisation des données dans la blockchain créent un conflit structurel avec les principes du RGPD, notamment en ce qui concerne le droit à la rectification et l'effacement des données³³. Elle propose que cette tension

³² Finck, Michèle. Blockchain and the General Data Protection Regulation: Can Distributed Ledgers be Squared with European Data Protection Law? *Journal of Data Protection & Privacy*, 2019.

³³ *Idem*.

juridique appelle à une refonte des cadres réglementaires pour qu'ils tiennent compte des caractéristiques techniques uniques de la blockchain.

D'autres chercheurs, tels que Zyskind et al. (2015), proposent une approche différente en envisageant des mécanismes décentralisés pour gérer les données personnelles tout en respectant la vie privée. Ces auteurs suggèrent d'utiliser la blockchain comme un outil de protection des données, à condition que les individus contrôlent eux-mêmes les clés d'accès à leurs informations³⁴. Cette approche permettrait de concilier les avantages de la blockchain avec les exigences juridiques actuelles en matière de protection des données personnelles.

Toutefois, bien que ces solutions techniques existent, elles ne garantissent pas toujours la conformité totale avec les réglementations actuelles. Des chercheurs comme Sedlmeir et al. (2020) mettent en avant les limites du chiffrement des données sur la blockchain, notamment en raison de l'irréversibilité des transactions et de la difficulté de mise en œuvre d'un véritable droit à l'oubli³⁵.

Responsabilité juridique dans un système décentralisé

Un autre défi majeur posé par la blockchain est la question de la responsabilité juridique. Contrairement aux systèmes traditionnels, où une autorité centrale est responsable de la gestion des données et des actions, la blockchain fonctionne sans entité centrale. Cela soulève des questions complexes sur la responsabilité légale en cas de violation des droits humains ou d'abus de données. Wright et De Filippi (2015) ont introduit le concept de "Lex Cryptographia", où les règles et les lois sont directement codées dans les systèmes blockchain. Dans ce cadre, la blockchain devient une forme de régulation autonome, où les systèmes de gouvernance et de régulation traditionnels deviennent obsolètes ³⁶. Cependant, cette approche crée une tension entre l'autonomie

³⁴ Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. 2015 IEEE Security and Privacy Workshops, 180-184. <https://homepage.cs.uiowa.edu/~ghosh/blockchain.pdf>

³⁵ Sedlmeir, J., Buhl, H.U., Fridgen, G. *et al.* The Energy Consumption of Blockchain Technology: Beyond Myth. *Bus Inf Syst Eng* **62**, 599–608 (2020). <https://doi.org/10.1007/s12599-020-00656-x>

³⁶ Wright, A., & De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *SSRN Electronic Journal*, 5, 3-12. <file:///Users/36c4a/Downloads/ssrn-2580664.pdf>

technologique et les principes juridiques existants, notamment en matière de protection des droits humains.

Les smart contracts, qui sont des contrats auto-exécutables sur la blockchain, posent également des problèmes de responsabilité juridique. Werbach (2018) souligne que, bien que ces contrats soient efficaces pour automatiser certaines transactions, l'absence de contrôle humain peut conduire à des litiges complexes, notamment lorsque les résultats ne correspondent pas aux attentes des parties³⁷. L'ouvrage de Werbach met en lumière la nécessité de réformes juridiques pour offrir une flexibilité dans l'application des smart contracts et garantir des recours juridiques appropriés en cas de conflits.

Régulation internationale et souveraineté numérique

La régulation internationale de la blockchain constitue un défi majeur. La nature transnationale de la blockchain complique l'application des lois nationales, notamment en matière de protection des données et de droits humains. Tapscott D. et Tapscott A. (2016) ont analysé comment la blockchain modifie les systèmes de gouvernance à l'échelle mondiale, affirmant que les gouvernements et les organisations internationales doivent revoir leurs approches pour gérer cette technologie disruptive³⁸. Ils mettent en avant la nécessité de créer une régulation internationale harmonisée, tout en respectant les juridictions locales. Cela soulève des questions sur la souveraineté numérique des États, car la blockchain opère indépendamment des frontières géographiques et des réglementations nationales.

De Filippi et Hassan (2018) explorent également la gouvernance de la blockchain, suggérant qu'elle pourrait être régulée par des standards internationaux, mais avec une flexibilité pour s'adapter aux juridictions locales³⁹. Leur travail met l'accent sur le besoin d'un cadre de

³⁷ Werbach, K. (2018). *The Blockchain and the New Architecture of Trust*. MIT Press, pp. 140-150.

³⁸ Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. Penguin, pp. 60-70.

³⁹ De Filippi, P., & Hassan, S. (2018). *Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code*. First Monday, 23(12). https://www.researchgate.net/publication/311447869_Blockchain_Technology_as_a_Regulatory_Technology_From_Code_is_Law_to_Law_is_Code

gouvernance capable de respecter les caractéristiques décentralisées de la blockchain tout en protégeant les droits des individus. Cette perspective se situe à mi-chemin entre l'autorégulation technologique et la régulation étatique.

Impact socio-économique et égalité d'accès

Les répercussions socio-économiques de la blockchain, en particulier sur les droits humains, méritent également d'être examinées. Zwitter et Boisse-Despiaux (2018) démontrent que la blockchain pourrait jouer un rôle crucial dans la réduction de la corruption et la gestion des ressources publiques, notamment dans les pays en développement⁴⁰. Cette perspective doit être mise en dialogue avec une lecture critique des rapports de pouvoir à l'ère algorithmique. Martineau et Durand Folco soulignent à cet égard que les technologies numériques s'inscrivent dans une logique d'accumulation du capital algorithmique qui peut reproduire, voire amplifier, les inégalités économiques plutôt que de les corriger⁴¹. Leur étude montre que la traçabilité assurée par la blockchain permettrait de mieux allouer l'aide humanitaire et de garantir qu'elle atteigne les bénéficiaires finaux, réduisant ainsi le risque de détournement de fonds.

Cependant, Sedlmeir et al. (2020) soulignent que l'adoption de la blockchain nécessite une infrastructure numérique avancée, ce qui pourrait exclure certaines populations vulnérables, notamment dans les régions les moins développées⁴². Cela soulève la question de la fracture numérique et de l'inégalité d'accès à cette technologie. Leur contribution est cruciale car elle met en lumière le risque que la blockchain accentue les inégalités mondiales, en limitant ses avantages aux régions économiquement et géographiquement favorisées.

⁴⁰ Zwitter, A., & Boisse-Despiaux, M. (2018). Blockchain for Humanitarian Action and Development. *Journal of International Humanitarian Action*, 3(16), 1-7. <https://jhumanitarianaction.springeropen.com/articles/10.1186/s41018-018-0044-5>

⁴¹ Jonathan Martineau et Jonathan Durand Folco, *Le capital algorithmique : accumulation, pouvoir et résistance à l'ère de l'intelligence artificielle* (Montréal : \u00c9cosoci\u00e9t\u00e9, 2023).

⁴² Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The Energy Consumption of Blockchain Technology: Beyond Myth. *Business & Information Systems Engineering*, 62(6), 599–608 <https://link.springer.com/article/10.1007/s12599-020-00656-x>

Ainsi, cette revue de la littérature met en évidence un paradoxe fondamental : la blockchain est une technologie prometteuse pour la protection des droits humains, mais elle est encore incompatible avec de nombreux cadres juridiques existants. La protection des données personnelles, la responsabilité dans un système décentralisé, la régulation internationale, et l'impact socio-économique sont des questions qui nécessitent une réflexion approfondie et une réforme des cadres juridiques existants. Il est donc essentiel que régulateurs, législateurs, et experts juridiques collaborent pour créer un environnement réglementaire flexible, capable de tirer parti des avantages de la blockchain tout en protégeant les droits fondamentaux des individus. Cette recherche s'attachera à proposer une approche réglementaire équilibrée, garantissant à la fois l'innovation technologique et la protection des droits fondamentaux.

CHAPITRE 1 : LA BLOCKCHAIN, UN OUTIL POUR LA PROTECTION DES DROITS HUMAINS

1.1 Fonctionnement de la blockchain

La blockchain est un registre distribué qui fonctionne sous la forme d'une chaîne de blocs interconnectés. Chaque bloc regroupe un ensemble de transactions qui sont validées au moyen d'un mécanisme de consensus décentralisé, tel que la preuve de travail (*Proof of Work – PoW*) ou la preuve d'enjeu (*Proof of Stake – PoS*). Avant d'être ajouté à la chaîne, chaque bloc doit être approuvé par l'ensemble du réseau, ce qui empêche toute falsification ou modification ultérieure des données enregistrées ⁴³.

1.1.1. L'immuabilité et la transparence des données

Ces caractéristiques structurelles attribuent à la blockchain une caractéristique essentielle l'immuabilité des informations. Combinée à la transparence propre aux registres publics, cette immuabilité donne à la blockchain une valeur particulière dans le contexte de la protection des droits humains. En effet, en garantissant l'intégrité et la traçabilité des données, la blockchain peut

⁴³ IBM, "Qu'est-ce que la blockchain ?", IBM, <https://www.ibm.com/fr-fr/topics/blockchain>

contribuer efficacement à la lutte contre la fraude et la corruption, notamment dans des environnements où les systèmes centralisés sont vulnérables aux manipulations et aux abus de pouvoir ⁴⁴ .

1.1.2. La décentralisation du système blockchain

Contrairement aux plateformes logicielles centralisées, telles que Facebook, Amazon, Uber ou encore les banques en ligne, qui reposent sur le contrôle d'un acteur unique, la blockchain s'appuie sur un modèle décentralisé dans lequel chaque participant détient une copie du registre. L'absence d'intermédiaire central permet ainsi de limiter les risques de monopole, de censure et de cyberattaques, tout en renforçant la résilience du système ⁴⁵.

Dans ce cadre, les transactions sont validées collectivement grâce à un protocole de consensus, puis enregistrées de manière infalsifiable dans le registre distribué. Ce mécanisme garantit à la fois la sécurité et la transparence des échanges, éléments essentiels à la confiance des utilisateurs dans le fonctionnement du réseau⁴⁶.

1.1.3. La cryptographie asymétrique

La cryptographie asymétrique constitue le fondement du système d'identification des utilisateurs au sein d'un réseau blockchain. Elle permet d'assurer à la fois la confidentialité et la sécurité des échanges.

Concrètement, chaque utilisateur dispose d'une adresse publique, qui peut être librement partagée afin de recevoir des fonds, ainsi que d'une clé privée, strictement personnelle, indispensable pour autoriser et valider les transactions⁴⁷. Contrairement aux systèmes traditionnels reposant sur des

⁴⁴ Wright, A., & De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. SSRN Electronic Journal p. 6

⁴⁵ Martial Tanguy Kadji Ngassam, Jean Babei, Serge Guy Biloa Handbook of Research on Blockchain Technology and the Digitalization of the Supply Chain, 2023.

⁴⁶ *Idem.*

⁴⁷ *Idem.*

mots de passe, la blockchain utilise une signature électronique unique, ce qui réduit considérablement les risques d'usurpation d'identité et de réutilisation frauduleuse des informations. Ce mécanisme renforce ainsi la fiabilité du réseau en garantissant l'intégrité des transactions déjà enregistrées⁴⁸.

1.1.4. La double dépense

L'un des défis majeurs des systèmes décentralisés est la double dépense, qui permettrait à un utilisateur malveillant de dépenser plusieurs fois le même actif numérique. La blockchain résout ce problème grâce à un protocole de consensus, où les participants doivent s'accorder sur l'état unique du registre avant d'autoriser une transaction⁴⁹. Lorsqu'une transaction est créée, elle est diffusée sur le réseau et soumise à des vérifications portant sur la validité de la signature cryptographique et la disponibilité des fonds. Tant qu'elle n'a pas été intégrée à un bloc validé, elle reste en attente, ce qui garantit l'intégrité du système⁵⁰.

1.1.5. Le processus de minage

L'ajout de nouvelles transactions repose sur un processus appelé minage, qui assure la validation et la sécurisation du réseau. Les mineurs, qui sont des nœuds spécialisés, collectent les transactions en attente et les regroupent dans un bloc avant de les ajouter à la blockchain. Le droit d'inscrire un nouveau bloc est déterminé par un mécanisme de preuve de travail (PoW), basé sur la résolution de problèmes cryptographiques complexes⁵¹. Ce système repose sur la résolution de problèmes cryptographiques complexes, nécessitant une puissance de calcul importante. Une fois le bloc validé, il est propagé à l'ensemble du réseau, garantissant une synchronisation des informations entre tous les participants. Ce fonctionnement permet de maintenir un registre distribué où chaque

⁴⁸ *Idem.*

⁴⁹ Werbach, K. (2018). *The Blockchain and the New Architecture of Trust*. MIT Press.

⁵⁰ Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). *Research p.491 Perspectives and Challenges for Bitcoin and Cryptocurrencies*. P.107

⁵¹ Martial Tangui Kadji Ngassam, Jean Babei, Serge Guy Biloa Handbook of Research on Blockchain Technology and the Digitalization of the Supply Chain, 2023.

nœud détient une copie identique de la blockchain, assurant ainsi sa résilience et son infalsifiabilité⁵².

Ce mécanisme de minage soulève toutefois des préoccupations croissantes sur le plan environnemental et social, qui sont indissociables de toute réflexion sur la blockchain et les droits humains. Sur le plan énergétique, les blockchains reposant sur la preuve de travail exigent une puissance de calcul considérable. Le Cambridge Centre for Alternative Finance estimait en 2023 que la consommation annuelle du réseau Bitcoin dépassait celle de pays comme l'Argentine ou la Norvège, avec des émissions de CO₂ variables selon le mix énergétique utilisé⁵³. À l'inverse, les blockchains reposant sur la preuve d'enjeu, comme Ethereum depuis sa transition en septembre 2022, ont réduit leur consommation énergétique de plus de 99 %, ce qui démontre que toutes les blockchains ne se valent pas sur le plan écologique⁵⁴. Contrairement à l'intelligence artificielle, dont l'empreinte matérielle englobe également la consommation d'eau, les métaux rares et le refroidissement des centres de données, la blockchain pose avant tout une question de consommation de calcul, dont l'impact varie considérablement selon le protocole utilisé⁵⁵.

Ces enjeux environnementaux s'articulent par ailleurs à une réalité sociale tout aussi importante : la fracture numérique mondiale. Selon l'Union internationale des télécommunications, environ 2,6 milliards de personnes n'avaient toujours pas accès à Internet en 2023, soit près d'un tiers de la population mondiale⁵⁶. Cette exclusion structurelle soulève une question fondamentale : comment la blockchain peut-elle prétendre contribuer à la protection des droits humains si les populations les plus vulnérables n'ont pas accès aux infrastructures numériques nécessaires à son utilisation ? L'empreinte sociale de la technologie est donc indissociable de son empreinte

⁵² *Idem*.

⁵³ Cambridge Centre for Alternative Finance (CCAF), *Cambridge Bitcoin Electricity Consumption Index*, University of Cambridge, 2023, en ligne : <<https://ccaf.io/cbnsi/cbeci>> (consulté le 4 juin 2026).

⁵⁴ Ethereum Foundation, « The Merge », septembre 2022, en ligne : <<https://ethereum.org/en/upgrades/merge/>> (consulté le 4 juin 2026) ; Sedlmeir, J., Buhl, H.U., Fridgen, G. et Keller, R., « The Energy Consumption of Blockchain Technology: Beyond Myth », (2020) 62:6 *Business & Information Systems Engineering* 599.

⁵⁵ Marke, A., Mehling, M. et Corréa, F.d.A. (dir.), *Governing Carbon Markets with Distributed Ledger Technology* (Cambridge : Cambridge University Press, 2022).

⁵⁶ Union internationale des télécommunications (UIT), *Faits et chiffres TIC 2023* (Genève : UIT, 2023).

écologique, et ces deux dimensions doivent être prises en compte dans toute analyse sérieuse des rapports entre blockchain et droits humains.

1.2 Principes fondamentaux et enjeux juridiques de la blockchain

La blockchain repose sur trois principes essentiels qui garantissent son fonctionnement et sa fiabilité. D'abord, sa nature décentralisée élimine le besoin d'un intermédiaire de confiance, puisque la validation des transactions repose sur l'ensemble du réseau et non sur une entité unique. Cette caractéristique réduit les risques de manipulation, de censure ou d'abus de pouvoir, tout en assurant une résilience accrue du système face aux attaques informatiques. Ensuite, son immutabilité empêche toute modification rétroactive des données enregistrées dans la chaîne, puisque chaque bloc est lié aux précédents par un procédé cryptographique⁵⁷. Toute tentative d'altération nécessiterait de recalculer l'ensemble des blocs suivants, une opération pratiquement impossible en raison de la puissance de calcul requise. Ce mécanisme garantit l'intégrité et l'authenticité des transactions, un atout majeur dans des secteurs où la transparence et la traçabilité sont primordiales. Enfin, la transparence du registre permet à l'ensemble des participants d'accéder aux informations enregistrées, tout en préservant l'anonymat des utilisateurs grâce aux techniques de cryptographie avancées. Ce compromis entre accessibilité et confidentialité renforce la confiance dans le système, notamment dans des contextes où la protection des données personnelles est essentielle⁵⁸.

Bien que cette technologie puisse paraître complexe, elle peut être résumée ainsi : la blockchain est une base de données décentralisée, où chaque transaction est validée collectivement avant d'être définitivement enregistrée. Ce système élimine le besoin d'un tiers de confiance, réduit les risques de fraude et garantit une traçabilité parfaite des opérations. En assurant un registre partagé, sécurisé

⁵⁷ Martial Tangui Kadji Ngassam, Jean Babei, Serge Guy Biloa Handbook of Research on Blockchain Technology and the Digitalization of the Supply Chain, 2023.

⁵⁸ Idem.

et infalsifiable, elle ouvre de nouvelles perspectives dans des secteurs variés comme la finance, la logistique et la protection des droits fondamentaux⁵⁹.

Dans cette logique, les promoteurs de la blockchain mettent en avant plusieurs avantages par rapport aux systèmes centralisés. Elle garantit d'abord l'intégrité des données, car toute modification nécessiterait une réécriture complète de la chaîne, ce qui est pratiquement impossible. Ensuite, elle assure une décentralisation effective, limitant ainsi les risques de manipulation⁶⁰.

En outre, les transactions effectuées sur la blockchain sont rapides, sécurisées et peu coûteuses, notamment grâce à l'absence d'intermédiaires, contrairement aux transactions bancaires qui impliquent des délais et des frais supplémentaires. Enfin, la blockchain renforce la protection des données personnelles, en garantissant l'anonymat des utilisateurs tout en leur offrant un contrôle total sur leurs informations⁶¹.

Toutefois, ce système soulève également des défis juridiques majeurs. Son caractère décentralisé complique l'identification d'un acteur responsable en cas de litige, tandis que son immutabilité entre en conflit avec le droit à l'oubli, principe consacré par le RGPD (article 17)⁶². Ainsi, l'intégration de la blockchain dans les cadres juridiques existants nécessite une réflexion approfondie sur les adaptations législatives et techniques à mettre en place. Les régulateurs doivent trouver un équilibre entre innovation technologique et conformité réglementaire, en développant des solutions hybrides qui garantissent à la fois sécurité juridique et flexibilité technologique. À l'avenir, seule une coopération internationale efficace entre États, entreprises technologiques et

⁵⁹ Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique. "Blockchain : définition, avantages et applications." Économie.gouv.fr. Consulté le 5 février 2025. <https://www.economie.gouv.fr/entreprises/blockchain-definition-avantage-utilisation-application>.

⁶⁰ G'sell, Florence and Martin-Bariteau, Florian, L'impact des blockchains sur les droits de l'homme, la démocratie et l'État de droit (The Impact of Blockchains for Human Rights, Democracy and the Rule of Law) (March 15, 2022). Rapport, Conseil de l'Europe (2022), Available at SSRN: <https://ssrn.com/abstract=4170327> or <http://dx.doi.org/10.2139/ssrn.4170327> p.6

⁶¹ *Idem*.

⁶² Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Penguin, p. 67

institutions juridiques permettra d'encadrer cette révolution numérique tout en préservant les droits fondamentaux des individus.

1.3 Apports de la blockchain à la protection des droits fondamentaux

Au-delà de son fonctionnement technique et de ses principes fondamentaux, la blockchain peut également être envisagée comme un outil au service de la protection des droits fondamentaux. Dans un contexte marqué par la multiplication des crises humanitaires, des déplacements forcés et de l'exclusion administrative de millions de personnes à travers le monde, l'accès à une identité juridique constitue une condition essentielle à l'exercice effectif des droits humains, tel que le consacre l'article 6 de la Déclaration universelle des droits de l'homme⁶³ ainsi que l'article 16 du Pacte international relatif aux droits civils et politiques⁶⁴.

Dans de nombreux pays, des millions de personnes n'ont pas de documents d'identité officiels, ce qui limite leur accès aux services essentiels, tels que l'éducation, les soins de santé et l'emploi. Face à cette situation, la blockchain offre par l'une de ses applications les plus prometteuses une création d'identités numériques indépendantes de toute autorité centrale, mais sécurisées par des mécanismes de validation décentralisés⁶⁵. Ce type d'identité décentralisée permet à ces individus de prouver leur existence légale sans dépendre d'un gouvernement qui pourrait être défaillant ou corrompu.

Ces enjeux seront abordés, dans la section suivante, à travers l'analyse de la crise des réfugiés, qui illustre concrètement les difficultés rencontrées par les personnes privées de documents d'identité.

⁶³ *Déclaration universelle des droits de l'homme*, Rés AG 217 A (III), Doc off AG NU, 3^e sess, supp n° 13, Doc NU A/810 (1948), art 6.

⁶⁴ *Pacte international relatif aux droits civils et politiques*, 16 décembre 1966, 999 RTNU 171, art 16 (entré en vigueur le 23 mars 1976).

⁶⁵ Zwitter, A., & Boisse-Despiaux, M. (2018). Blockchain for Humanitarian Action and Development. *Journal of International Humanitarian Action*,

1.4 Les droits économiques, sociaux et culturels : un angle souvent négligé

L'analyse qui précède s'est largement concentrée sur l'apport de la blockchain à la protection des droits civils et politiques, notamment la liberté d'expression, le droit à la vie privée et la protection contre la censure. Or, les droits économiques, sociaux et culturels (DESC), bien que consacrés au même titre par le Pacte international relatif aux droits économiques, sociaux et culturels de 1966⁶⁶, occupent une place plus marginale dans la littérature sur la blockchain et les droits humains.

Le droit à l'éducation illustre bien ce potentiel encore peu exploité. Dans les contextes de crise humanitaire, la perte de documents scolaires empêche souvent les personnes déplacées de faire reconnaître leurs acquis éducatifs dans leur pays d'accueil. Des chercheurs ont proposé l'utilisation de registres distribués pour permettre aux personnes réfugiées de conserver une preuve infalsifiable de leur parcours scolaire, indépendamment des institutions d'origine, ce qui leur permettrait de poursuivre leurs études ou d'accéder au marché du travail malgré l'absence de documents physiques⁶⁷.

Cela dit, ces initiatives demeurent largement exploratoires et peu encadrées juridiquement. Une réflexion future sur la blockchain et les droits humains gagnerait à intégrer davantage cette dimension économique et sociale, qui touche directement les populations les plus vulnérables, plutôt que de se concentrer presque exclusivement sur les droits civils et politiques.

1.5 La crise des réfugiés

Dans le contexte social contemporain, la crise des réfugiés s'impose comme l'un des défis humanitaires les plus pressants. Elle met en lumière une problématique centrale, à savoir l'absence d'identité juridique pour des millions de personnes déplacées. La réponse apportée à cette crise demeure toutefois entravée par plusieurs obstacles majeurs, parmi lesquels figurent le manque

⁶⁶ Pacte international relatif aux droits économiques, sociaux et culturels, 16 décembre 1966, 993 R.T.N.U. 3 (entrée en vigueur le 3 janvier 1976).

⁶⁷ Voir l'étude systématique sur la reconnaissance des diplômes par blockchain dans des contextes de crise humanitaire (Jordanie, Rwanda) : « Blockchain and Higher Education Diplomas », en ligne : <<https://pmc.ncbi.nlm.nih.gov/articles/PMC8314335/>>.

d'identification officielle, l'insuffisance des financements alloués aux organisations humanitaires et des infrastructures dépassées qui tardent à intégrer les nouvelles technologies⁶⁸.

D'après la Banque mondiale, environ 850 millions de personnes dans le monde ne possèdent toujours pas d'identification officielle. Parmi elles, les réfugiés sont particulièrement touchés. Par exemple, près de 70 % des réfugiés syriens n'avaient pas leur carte d'identité nationale en arrivant dans leur pays d'accueil, 24 % des enfants de moins de cinq ans ne sont pas enregistrés officiellement, et 50 % mariés ne possèdent pas de certificats de mariage, ce qui complique considérablement leurs démarches administratives⁶⁹. Sans ces documents, ils se retrouvent exclus des services essentiels tels que l'accès aux soins, à l'éducation ou à l'emploi, et voient leur protection juridique fortement compromise⁷⁰.

En l'absence d'une identification officielle, ces populations deviennent invisibles et vulnérables. Elles ne peuvent ni prouver leur existence, ni faire valoir leurs droits fondamentaux. Dans certains cas, cette absence de papiers entraîne des conséquences dramatiques⁷¹.

Au Royaume-Uni, un récent rapport du Refugee Council révèle que des centaines de mineurs réfugiés sont placés dans des centres de détention pour adultes, faute de pouvoir prouver leur âge. Face à cette incertitude, les autorités recourent parfois à des méthodes controversées, comme l'analyse dentaire, pour estimer l'âge des demandeurs d'asile⁷².

En Suisse, le gouvernement a récemment consulté les parties prenantes afin de déterminer quelles données numériques pourraient être utilisées pour identifier les demandeurs d'asile, notamment à partir de leurs téléphones intelligents lorsque ces derniers ne possèdent pas de documents officiels.

⁶⁸ Cardano Foundation, How Blockchain Can Help in the Refugee Crisis, 2023. Disponible sur : <https://www.cardanofoundation.org/blog/how-blockchain-can-help-in-the-refugee-crisis> (consulté le 10 février 2025).

⁶⁹ *Idem*.

⁷⁰ The Blockchain Land, Identités numériques : La blockchain au secours des réfugiés, 7 décembre 2018. Disponible sur : <https://theblockchainland.com/fr/2018/12/07/identites-numeriques-blockchain-refugies> (consulté le 10 février 2025)

⁷¹ Cardano Foundation, How Blockchain Can Help in the Refugee Crisis, 2023. Disponible sur : <https://www.cardanofoundation.org/blog/how-blockchain-can-help-in-the-refugee-crisis> (consulté le 10 février 2025).

⁷² *Idem*.

En 2022, la Suisse a enregistré 24 511 demandes d’asile, soit une augmentation de plus de 64 % par rapport à 2021⁷³. Cette situation reflète une tendance plus large en Europe. La même année, les pays membres de l’UE ont observé une hausse d’environ 50 % des demandes d’asile. Face à cet afflux croissant de personnes déplacées, l’adoption de solutions numériques pour l’identification devient un enjeu crucial pour accélérer les procédures administratives et garantir un meilleur accès aux droits fondamentaux⁷⁴.

Une identité numérique basée sur la blockchain pourrait ainsi offrir une solution à ce problème en offrant un système d’identification accessible à l’échelle mondiale. Elle permettrait aux réfugiés de conserver leurs documents officiels tels que les papiers d’identité, les diplômes, les certificats de mariage et les titres de propriété, de manière sécurisée, immuable et accessible mondialement.

Cette technologie garantirait un accès continu à des informations essentielles, facilitant à la fois leur intégration dans les pays d’accueil et leur réinsertion future dans leur pays d’origine⁷⁵, tout en leur ouvrant l’accès aux services essentiels, tels que les soins médicaux, l’éducation ou encore les services bancaires, indépendamment des autorités nationales souvent défaillantes ou inaccessibles, même en situation d’exil⁷⁶.

Bien que cette approche puisse sembler difficile à mettre en œuvre dans les pays en développement, l’accès à la technologie numérique progresse rapidement. En 2018, par exemple, 30 % des Syriens disposaient déjà d’un accès à Internet, ce qui montre que l’adoption de solutions basées sur la blockchain reste envisageable, même dans des contextes fragiles. Toutefois, pour que ces identités

⁷³ Cardano Foundation, How Blockchain Can Help in the Refugee Crisis, 2023. Disponible sur : <https://www.cardanofoundation.org/blog/how-blockchain-can-help-in-the-refugee-crisis> (consulté le 10 février 2025).

⁷⁴ *Idem*.

⁷⁵ The Blockchain Land, Identités numériques : La blockchain au secours des réfugiés, 7 décembre 2018. Disponible sur : <https://theblockchainland.com/fr/2018/12/07/identites-numeriques-blockchain-refugies> (consulté le 10 février 2025)

⁷⁶ *Idem*.

numériques soient pleinement efficaces, une coopération internationale demeure indispensable afin d'assurer leur reconnaissance par les gouvernements et les institutions à travers le monde⁷⁷.

1.6 Apport de la blockchain dans la gestion de l'identité des réfugiés

La blockchain offre aux institutions gouvernementales et internationales un cadre sécurisé de gestion des identités. Grâce à des mécanismes décentralisés de stockage et de vérification des données, elle permet aux autorités de renforcer la fiabilité et l'efficacité des processus d'identification et de gestion administrative des populations déplacées.

Le Programme Alimentaire Mondial (PAM) a lancé en 2017 le projet "Building Blocks" en Jordanie, exploitant la blockchain pour assurer une distribution plus sécurisée et efficace de l'aide alimentaire aux réfugiés syriens. Ce système repose sur une blockchain privée où chaque transaction est enregistrée de manière immuable, permettant aux réfugiés d'acheter des denrées alimentaires dans les supermarchés des camps sans besoin de monnaie physique ni de cartes de rationnement. Grâce à un système de reconnaissance de l'iris, leur identité est vérifiée instantanément, et le montant correspondant est déduit de leur allocation humanitaire⁷⁸. Ce dispositif garantit plus de sécurité et de transparence, réduit les coûts liés aux transactions bancaires, et offre aux bénéficiaires plus d'autonomie et de dignité, en éliminant les risques de vol ou de perte de documents. Avec plus de 1,2 million de transactions enregistrées, ce projet démontre le potentiel de la blockchain dans le secteur humanitaire, en facilitant l'accès aux ressources vitales et en améliorant la gestion des aides internationales. Fort de ce succès, le PAM explore actuellement l'extension de cette technologie à d'autres formes d'aide, notamment pour l'éducation et la santé, afin de renforcer l'impact des missions humanitaires⁷⁹.

En décembre 2022, le Haut-Commissariat des Nations unies pour les réfugiés (HCR) a lancé un projet pilote innovant en Ukraine, utilisant la technologie blockchain pour distribuer une aide

⁷⁷ *Idem.*

⁷⁸ Programme Alimentaire Mondial, Building Blocks: Blockchain for Humanitarian Assistance, 2023. Disponible sur : <https://featured.undp.org/beyond-bitcoin/fr/> (consulté le 12 février 2025)

⁷⁹ *Idem.*

financière aux personnes déplacées par le conflit. En collaboration avec le Centre international de calcul des Nations unies (UNICC) et la Stellar Development Foundation (SDF), le HCR a transféré des fonds directement aux bénéficiaires sous forme d'USD Coin (USDC), une cryptomonnaie stable indexée sur le dollar américain. Les bénéficiaires pouvaient accéder à ces fonds via une application mobile sécurisée, leur permettant de retirer de l'argent en dollars, euros ou monnaie locale dans n'importe quel point de retrait MoneyGram, y compris les 4 500 sites en Ukraine⁸⁰. Cette approche a permis une distribution rapide, sécurisée et transparente de l'aide, tout en renforçant l'autonomie financière des personnes déplacées. Ce projet pilote, une première mondiale, a valu au HCR le "Best Impact Project Award" lors de la Paris Blockchain Week 2023, reconnaissant l'impact significatif de cette initiative sur le terrain. Fort de ce succès, le HCR envisage d'étendre cette solution numérique à d'autres contextes humanitaires, démontrant ainsi le potentiel de la blockchain pour améliorer l'efficacité et la traçabilité de l'aide aux populations vulnérables⁸¹.

En novembre 2022, Switzerland for UNHCR, le partenaire national du Haut-Commissariat des Nations unies pour les réfugiés en Suisse, a annoncé une collaboration innovante avec la Fondation Cardano pour soutenir les personnes déplacées de force. Cette initiative consiste en la création d'un fonds de participation alimenté par une délégation de 3,5 millions d'ADA (la cryptomonnaie native de la blockchain Cardano) par la Fondation Cardano⁸². Le fonds est géré par Taurus, un fournisseur suisse d'infrastructures d'actifs numériques. Les récompenses générées par ce fonds sont entièrement reversées au HCR, dont 80 % sont destinés aux opérations sur le terrain et 20 % aux programmes d'innovation, promouvant ainsi l'utilisation de la blockchain comme solution aux défis auxquels sont confrontés les réfugiés. Cette collaboration illustre le potentiel de la technologie

⁸⁰ Haut-Commissariat des Nations unies pour les réfugiés (HCR), UNHCR wins award for innovative use of blockchain solutions to provide cash to forcibly displaced people, 2023. Disponible sur : <https://www.unhcr.org/us/news/press-releases/unhcr-wins-award-innovative-use-blockchain-solutions-provide-cash-forcibly> (consulté le 12 février 2025)

⁸¹ *Idem*.

⁸² Switzerland for UNHCR, Blockchain for Refugees, 2022. Disponible sur : <https://unrefugees.ch/fr/blockchain-refugees> (consulté le 12 février)

blockchain pour mobiliser des ressources de manière transparente et efficace au profit des populations vulnérables⁸³.

L'utilisation de la blockchain dans la gestion de l'identité et de l'aide humanitaire pour les réfugiés représente une avancée majeure en matière de sécurité, de transparence et d'autonomie pour les populations déplacées. Des initiatives menées par le HCR, le Programme Alimentaire Mondial et Switzerland for UNHCR démontrent que cette technologie peut répondre efficacement aux défis liés à l'absence de documents officiels, à l'accès aux ressources essentielles et à la distribution équitable de l'aide financière. En garantissant un stockage sécurisé et infalsifiable des données, la blockchain offre aux réfugiés un moyen de prouver leur identité, d'accéder aux services et de reconstruire leur vie avec dignité. Toutefois, son adoption à grande échelle nécessite une coopération internationale et une reconnaissance juridique afin d'intégrer ces identités numériques dans les cadres administratifs existants.

1.7 L'empreinte sociale de la blockchain

Au-delà des promesses technologiques, il convient de s'interroger sur ce que l'on pourrait appeler l'empreinte sociale de la blockchain. Le développement de ces infrastructures repose sur une chaîne de production mondiale qui n'est pas sans conséquences humaines directes. La fabrication du matériel informatique nécessaire au fonctionnement des réseaux blockchain, notamment les puces et les processeurs spécialisés, implique l'extraction de métaux rares dans des conditions souvent précaires, dans des régions où les droits des travailleurs sont peu ou mal protégés⁸⁴. Cette réalité est rarement évoquée dans les débats sur la blockchain et les droits humains, alors qu'elle en constitue pourtant un angle mort important.

Martineau et Durand Folco soulignent à cet égard que le développement des technologies numériques à grande échelle s'inscrit dans une logique d'accumulation capitaliste qui tend à

⁸³ *Idem.*

⁸⁴ Jonathan Martineau et Jonathan Durand Folco, *Le capital algorithmique : accumulation, pouvoir et résistance à l'ère de l'intelligence artificielle* (Montréal : Écosociété, 2023), p. 87–102.

reproduire, voire à amplifier, les inégalités existantes⁸⁵. Autrement dit, une technologie présentée comme émancipatrice peut simultanément perpétuer des formes d'exploitation dans les maillons invisibles de sa chaîne de valeur. Une réflexion honnête sur la blockchain et les droits humains ne peut donc pas faire l'économie de cette dimension, au risque de promouvoir une solution dont les bénéfices pour certains se construisent sur les préjudices subis par d'autres.

Ces constats n'invitent pas à rejeter la blockchain comme outil de protection des droits humains, mais à l'aborder avec une plus grande prudence. Une approche véritablement centrée sur les droits humains exige que le déploiement de ces technologies s'accompagne d'une attention soutenue aux conditions de production du matériel sous-jacent et à la protection des droits des travailleurs dans les chaînes d'approvisionnement technologiques mondiales⁸⁶.

CHAPITRE 2 : LES DÉFIS JURIDIQUES DE LA BLOCKCHAIN : ENTRE PROTECTION DES INNOVATIONS ET RESPECT DES CADRES NORMATIFS

L'utilisation de la blockchain dans le domaine des droits humains présente des défis juridiques significatifs. Si elle offre des opportunités significatives pour la protection des droits humains, comme démontré dans le chapitre 1, elle entre également en conflit avec des principes juridiques fondamentaux. La nature décentralisée et immuable de cette technologie complique la détermination de la loi applicable et de la juridiction compétente, étant donné que les données sont réparties mondialement sans autorité centrale⁸⁷. De plus, l'immutabilité des données sur la blockchain entre en conflit avec le droit à l'oubli consacré par le Règlement Général sur la Protection des Données (RGPD), rendant difficile la modification ou la suppression d'informations

⁸⁵ Idem, p. 45–60.

⁸⁶ Idem., p. 112–125.

⁸⁷ Conseil de l'Europe, Report on Blockchains and Fundamental Rights, 2020. Disponible sur : <https://rm.coe.int/report-on-blockchains-fr/1680a8ffe7 p.37>

personnelles⁸⁸. Les smart contracts, qui automatisent l'exécution des accords, posent des questions quant à leur reconnaissance légale et à la protection des parties impliquées⁸⁹. Enfin, l'absence d'une entité responsable clairement définie dans les systèmes blockchain complique l'attribution de la responsabilité en cas de violations des droits humains ou d'activités illicites⁹⁰. Cependant, l'adoption croissante de la blockchain soulève des défis juridiques complexes qui nécessitent une attention particulière.

Depuis sa première médiatisation dans *The Economist*, la blockchain a suscité un intérêt croissant dans le domaine juridique, au-delà de son adoption par les secteurs financiers et technologiques. Son caractère disruptif, c'est-à-dire sa capacité à bouleverser les cadres établis, a particulièrement interpellé les juristes, qui y voient à la fois une opportunité et un défi réglementaire⁹¹. Cette technologie, fondée sur un dispositif d'enregistrement partagé et immuable, remet en question des concepts fondamentaux du droit, notamment en matière de propriété numérique, de contrats intelligents et de protection des données personnelles. Bien que cette technologie puisse contribuer à moderniser les cadres normatifs existants, elle nécessite une redéfinition des règles juridiques pour garantir un équilibre entre innovation et régulation⁹². Ce chapitre analyse ces défis sous quatre angles principaux : la propriété intellectuelle, la protection des données personnelles, la responsabilité juridique dans les systèmes décentralisés, et les enjeux de souveraineté numérique.

⁸⁸ CNIL, Blockchain et RGPD : Quelles solutions pour un usage responsable en présence de données personnelles ?, 2018. Disponible sur : <https://www.cnil.fr/fr/blockchain-et-rgpd-queelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles> (consulté le 17 février 2025)

⁸⁹ Cairn.info, Réalités industrielles – La régulation des smart contracts, 2017. Disponible sur : <https://shs.cairn.info/revue-realites-industrielles-2017-3-page-20> (consulté le 17 février 2025)

⁹⁰ Village de la Justice, La blockchain face au droit : Quels défis juridiques? 2019. Disponible sur : <https://www.village-justice.com/articles/blockchain-face-droit,24049.html> (consulté le 17 février 2025)

⁹¹ Thibaut Labbé. Le droit face aux technologies disruptives : le cas de la blockchain. Droit. Université de Strasbourg, 2021. Français. P.9

⁹² Thibaut Labbé. Le droit face aux technologies disruptives : le cas de la blockchain. Droit. Université de Strasbourg, 2021. Français.

2.1 Le cadre juridique de la blockchain : régulation et adaptation des normes existantes

La blockchain, en tant que technologie émergente, fait l'objet de réglementations variées selon les pays, chaque juridiction cherchant à adapter son cadre légal face aux défis qu'elle soulève. Si certaines nations ont déjà mis en place des lois et des directives spécifiques, notamment dans les secteurs des crypto-actifs, de la finance et de la protection des données, d'autres peinent encore à structurer un cadre clair et adapté. Cette disparité des réglementations nationales, combinée à l'absence d'une approche uniforme, pose la question de l'harmonisation juridique à l'échelle internationale, essentielle pour assurer une application cohérente et efficace des normes.

Par ailleurs, la blockchain et les technologies de registres distribués (DLT) bouleversent profondément les mécanismes traditionnels des transactions commerciales, marquant une rupture conceptuelle dans le droit des affaires. Contrairement aux contrats papier classiques, les smart contracts introduisent des transactions automatisées et autonomes, redéfinissant ainsi les modalités de validité juridique et d'identification des parties⁹³. Cette évolution technologique impose aux législateurs d'adapter le cadre juridique aux nouveaux actifs numériques, identités décentralisées et espaces transactionnels virtuels. Dans un contexte où les grandes plateformes numériques exercent encore un contrôle dominant sur l'économie numérique, la blockchain représente une alternative décentralisée et plus résiliente face à la centralisation du web. De plus, l'essor du Web sémantique et de l'intelligence artificielle (IA) favorise l'interopérabilité des systèmes et l'automatisation du traitement des données, ce qui influence directement les réglementations sur la protection des actifs numériques et la sécurité des transactions. Ce constat souligne l'urgence d'un cadre juridique adapté, notamment en Europe, où les régulateurs tentent de suivre l'évolution rapide de ces technologies en ajustant progressivement leurs cadres législatifs⁹⁴.

⁹³ Pastor Sempere, C. (2025). The Legal Framework for New Digital Assets, Identities, and Data Spaces. Introduction. P. 4

⁹⁴ *Idem.* p.4-5

2.1.1. L'encadrement de la blockchain en France : une approche précurseur

La France s'est imposée comme l'un des premiers pays à établir un cadre juridique clair et structuré pour la blockchain et les crypto-actifs, dans un souci de protection des investisseurs et d'encadrement des entreprises du secteur. Face à la décentralisation et à l'évolution rapide de cette technologie, le gouvernement français a adopté la Loi PACTE (n° 2019-486) le 22 mai 2019, entrée en vigueur le 24 mai 2019⁹⁵. Cette loi marque une avancée majeure en matière de régulation des crypto-actifs, en instaurant un cadre légal pour les Initial Coin Offerings (ICO) et les prestataires de services sur actifs numériques (PSAN), incluant les plateformes d'échange et les services de conservation des cryptomonnaies. En garantissant plus de transparence et de sécurité aux investisseurs, cette régulation vise à renforcer la confiance dans l'écosystème des actifs numériques⁹⁶.

Dès 2017, la France avait déjà clarifié le régime fiscal et comptable des crypto-actifs, et en 2018, elle avait adopté une loi permettant l'enregistrement des titres financiers sur une blockchain. Ces initiatives s'inscrivent dans une volonté d'innovation et de compétitivité, visant à faire de la France un leader de l'industrie de la blockchain. Entre 2018 et 2019, plusieurs rapports officiels du gouvernement et du Parlement ont analysé les opportunités et les défis juridiques liés à cette technologie. L'approche française repose ainsi sur un équilibre entre innovation et réglementation, favorisant le développement des entreprises blockchain tout en assurant une protection efficace des utilisateurs et des investisseurs⁹⁷.

2.1.2. L'Union européenne et MiCA : vers une régulation harmonisée

L'Union européenne met en place un cadre réglementaire ambitieux pour encadrer la blockchain et les crypto-actifs, garantissant ainsi une intégration sécurisée de ces technologies dans l'économie

⁹⁵ Deloitte Avocats (2022). « Blockchain, crypto-actifs et régulation : le point sur la situation en France en 2022 », publié sur le blog Avocats Deloitte. Disponible à l'adresse : <https://blog.avocats.deloitte.fr/blockchain-crypto-actifs-et-regulation-le-point-sur-la-situation-en-france-en-2022/?amp=1>. (Consulté le 22 février 2025)

⁹⁶ *Idem*.

⁹⁷ Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique (France). « Régime fiscal des cryptomonnaies », disponible à l'adresse : <https://www.economie.gouv.fr/cedef/regime-fiscal-cryptomonnaies>. (Consulté le 22 février 2025)

numérique. Le règlement MiCA (Markets in Crypto-Assets), adopté en 2023, constitue la première tentative d'harmonisation des régulations sur les crypto-actifs au sein des États membres. Il impose des obligations de transparence, de protection des investisseurs et de surveillance des transactions, renforçant ainsi la stabilité et la fiabilité du marché des actifs numériques. Comme le souligne Finck dans son analyse de la gouvernance blockchain en Europe, cette approche reflète la volonté de l'Union européenne de concilier innovation technologique et protection juridique des utilisateurs⁹⁸. Ce règlement fonctionne en complément d'autres textes majeurs, tels que le Digital Services Act (DSA) et le Digital Markets Act (DMA), qui encadrent les plateformes numériques et leur utilisation des technologies blockchain afin d'assurer une concurrence loyale et une meilleure protection des utilisateurs⁹⁹.

L'Europe développe également des projets novateurs liés à la blockchain. Le portefeuille d'identité numérique européen (EUDI Wallet), introduit par le règlement eIDAS2, pourrait être utilisé sur des infrastructures blockchain pour sécuriser l'identité numérique des citoyens et des entreprises lors des transactions. En parallèle, l'euro numérique (CBDC), qui pourrait fonctionner sur une blockchain publique ou privée, suscite des débats quant à son intégration dans le système monétaire européen et aux moyens de lutte contre la fraude et le blanchiment d'argent¹⁰⁰.

Toutefois, malgré ces avancées, certains aspects restent incertains, notamment la distinction entre les crypto-actifs et les moyens de paiement traditionnels, ainsi que la fiscalité applicable aux transactions sur blockchain. L'évolution rapide de cette technologie, combinée à la montée en puissance de l'intelligence artificielle et des infrastructures de stockage décentralisées, exige une adaptation continue des régulations pour garantir un cadre juridique stable, sécurisé et en phase avec les nouvelles réalités du marché des actifs numériques¹⁰¹.

⁹⁸ Michèle Finck, *Blockchain Regulation and Governance in Europe* (Cambridge : Cambridge University Press, 2019).

⁹⁹ Pastor Sempere, C. (2025). The Legal Framework for New Digital Assets, Identities, and Data Spaces. Introduction. P. 7

¹⁰⁰ *Idem*.p.19

¹⁰¹ *Idem*.p.20

2.1.3. La régulation de la blockchain au Canada : un cadre en évolution

Le Canada adopte une approche progressive et pragmatique pour encadrer la blockchain et les actifs numériques, combinant régulations techniques et juridiques adaptées aux défis posés par ces technologies émergentes. Comme le montre Grinhaus dans son guide pratique du droit des contrats intelligents publié chez LexisNexis Canada, cette complexité réglementaire exige des praticiens une maîtrise à la fois des cadres provinciaux et fédéraux¹⁰². Contrairement à l'Union européenne, qui a instauré un cadre réglementaire harmonisé avec le règlement MiCA, le Canada applique des régulations distinctes selon les provinces, ce qui entraîne une certaine hétérogénéité législative. Au Québec, par exemple, les entreprises proposant des services liés aux crypto-actifs doivent s'enregistrer auprès de l'Autorité des marchés financiers (AMF) et se conformer à des exigences strictes en matière de protection des investisseurs et de lutte contre le blanchiment d'argent¹⁰³.

Sur le plan fédéral, la régulation des crypto-actifs et de la blockchain est encore en pleine évolution. Les Autorités canadiennes en valeurs mobilières (ACVM) travaillent actuellement à l'élaboration d'un cadre plus complet, visant notamment à réglementer l'émission et l'utilisation des jetons numériques¹⁰⁴. Actuellement, le Canada applique une approche d'assimilation aux catégories juridiques existantes, en tentant de rapprocher les crypto-actifs des modèles financiers traditionnels, bien que la nature hybride de ces actifs pose des défis juridiques. Pour favoriser l'innovation tout en limitant les risques, le pays a instauré un "bac à sable réglementaire", permettant aux entreprises blockchain d'expérimenter leurs modèles d'affaires sous la supervision des autorités¹⁰⁵. Cependant, l'absence d'un cadre juridique fédéral unifié et la disparité des réglementations provinciales freinent le développement du secteur et alimentent l'incertitude pour les acteurs du marché¹⁰⁶.

¹⁰² Aiden Grinhaus, *A Practical Guide to Smart Contracts and Blockchain Law*, 2^e éd. (Toronto : LexisNexis Canada, 2022).

¹⁰³ Godbout, A-S. (2020). Le droit à l'ère numérique : entre la régulation technique et la régulation juridique des actifs numériques au Canada. P. 3

¹⁰⁴ *Idem.* p.58

¹⁰⁵ *Idem.* p.59

¹⁰⁶ *Idem.* p.61

Le Canada met également l'accent sur la lutte contre le blanchiment d'argent et la protection des investisseurs. Ainsi, la Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes (LRPCFAT) a été modifiée en 2019 afin d'inclure les plateformes de négociation de cryptomonnaies sous la supervision du Centre d'analyse des opérations et déclarations financières du Canada (CANAFE). Par ailleurs, les ACVM imposent aux plateformes d'échange de crypto-actifs des obligations similaires à celles des courtiers en valeurs mobilières, renforçant ainsi leur responsabilité réglementaire¹⁰⁷. Le Canada se distingue également par son approche exploratoire des innovations blockchain. Le projet Jasper, initié par la Banque du Canada, teste l'utilisation de la blockchain pour les paiements interbancaires et la mise en place d'une monnaie numérique de banque centrale (MNBC). Cette initiative reflète l'intérêt des institutions financières canadiennes pour les applications de la blockchain dans le secteur bancaire. Toutefois, malgré ces avancées, l'absence de législation fédérale harmonisée laisse place à des disparités réglementaires entre les provinces, notamment en ce qui concerne la reconnaissance juridique des crypto-actifs en tant que valeurs mobilières¹⁰⁸.

En définitive, bien que le Canada adopte une approche flexible et expérimentale, il demeure confronté aux défis de fragmentation réglementaire et d'incertitude juridique. Une harmonisation législative entre les provinces et une clarification du statut des crypto-actifs seraient des étapes cruciales pour assurer un cadre juridique stable et attractif pour les entreprises du secteur blockchain.

2.1.4. La régulation de la blockchain aux États-Unis : un cadre fragmenté

Les États-Unis adoptent une approche fragmentée et multipartite pour réguler la blockchain et les actifs numériques, ce qui contraste avec l'harmonisation réglementaire entreprise par l'Union européenne avec le règlement MiCA. En l'absence d'un cadre fédéral unique, la régulation repose

¹⁰⁷ Gouvernement du Canada, Gazette du Canada, Partie I, Volume 158, Numéro 27 – « Règlement sur les actifs numériques et la blockchain », publié le 6 juillet 2024. Disponible à l'adresse : <https://canadagazette.gc.ca/rp-pr/p1/2024/2024-07-06/html/reg3-fra.html>.

¹⁰⁸ Les implications des technologies de la blockchain pour le système financier canadien », Banque du Canada, Rapport sur la stabilité financière, juin 2017. Disponible à l'adresse : <https://www.banqueducanada.ca/wp-content/uploads/2017/05/rsf-juin-2017-chapman.pdf>.

sur plusieurs agences gouvernementales, chacune appliquant des règles spécifiques, et sur des réglementations distinctes au niveau des États, entraînant une incertitude juridique pour les acteurs du marché ¹⁰⁹.

Au niveau fédéral, la Securities and Exchange Commission (SEC) joue un rôle central dans la surveillance des offres et transactions de titres financiers. Elle considère que plusieurs cryptomonnaies relèvent de la définition de "securities" (valeurs mobilières), ce qui les soumet aux règles strictes du droit boursier américain. La SEC a intensifié ses actions en justice contre des plateformes crypto, affirmant que certaines d'entre elles facilitaient des transactions de titres non enregistrés, en violation du Securities Act of 1933¹¹⁰. En parallèle, la Commodity Futures Trading Commission (CFTC) revendique la compétence sur les dérivés liés aux crypto-monnaies, en considérant que certains actifs numériques, comme le Bitcoin et l'Ethereum, doivent être traités comme des commodités (marchandises), au même titre que l'or ou le pétrole ¹¹¹.

D'autres agences fédérales interviennent également dans la régulation du secteur. Le Financial Crimes Enforcement Network (FinCEN), rattaché au Département du Trésor, impose aux plateformes d'échange de cryptomonnaies de se conformer aux réglementations applicables aux services monétaires, notamment en matière de lutte contre le blanchiment d'argent (AML) et d'identification des clients (KYC)¹¹². De son côté, l'Internal Revenue Service (IRS) traite les cryptomonnaies comme des biens imposables, soumettant ainsi chaque transaction aux règles fiscales sur les gains en capital, ce qui complique leur adoption comme moyen de paiement ¹¹³.

En janvier 2025, l'administration Trump a signé deux décrets présidentiels visant à stimuler l'adoption des cryptomonnaies et de la blockchain. Ces nouvelles mesures prévoient un allègement de certaines contraintes réglementaires et cherchent à renforcer la compétitivité des États-Unis dans

¹⁰⁹ Forbes France, "Réglementation des crypto-actifs : L'Europe face aux États-Unis (consulté le 22 février 2025)

¹¹⁰ Reuters, "Crypto litigation brought against SEC: Implications for the new administration", 10 janvier 2025,

¹¹¹ Village de la Justice, "Politique juridique du département du Trésor américain sur les crypto-actifs

¹¹² Village de la Justice, "Politique juridique du département du Trésor américain sur les crypto-actifs (consulté le 22 février 2025)

¹¹³ *Idem*.

l'économie numérique. Toutefois, cette orientation suscite des débats quant aux risques liés à la protection des investisseurs et à la stabilité du marché financier¹¹⁴.

En parallèle, certains États américains ont développé leurs propres cadres réglementaires. L'État de New York, par exemple, a instauré le BitLicense, un système d'enregistrement obligatoire pour les entreprises opérant dans le secteur des cryptomonnaies. Cette licence impose des exigences strictes en matière de conformité, de sécurité et de transparence financière, ce qui dissuade certaines entreprises d'y opérer¹¹⁵. À l'opposé, le Wyoming a adopté une approche plus favorable aux cryptomonnaies, en les reconnaissant comme monnaie légale et en permettant aux banques d'offrir des services liés aux actifs numériques, ce qui en fait un État attractif pour les entreprises blockchain ¹¹⁶.

L'un des principaux défis de la régulation américaine réside dans l'absence d'un cadre juridique fédéral harmonisé, ce qui entraîne une insécurité pour les acteurs du marché. Les entreprises crypto doivent jongler entre des réglementations fédérales parfois contradictoires et des législations étatiques disparates, ce qui complique leur conformité et freine le développement du secteur ¹¹⁷. Pour garantir un développement stable et sécurisé de l'industrie blockchain, plusieurs solutions sont envisagées : harmoniser les réglementations à l'échelle nationale, clarifier le statut juridique des crypto-actifs pour éviter les conflits de compétence entre la SEC et la CFTC, et encourager les bacs à sable réglementaires permettant aux entreprises d'expérimenter sous supervision étatique ¹¹⁸.

En définitive, bien que les États-Unis occupent une place centrale dans l'écosystème blockchain mondial, leur cadre réglementaire demeure fragmenté et en évolution constante. L'absence d'une régulation fédérale unifiée complique la tâche des entreprises et investisseurs, ce qui souligne la

¹¹⁴ El País, "Trump approuve deux décrets pour impulser les cryptomonnaies et l'intelligence artificielle . (consulté le 22 février 2025)

¹¹⁵ Forbes France, "Réglementation des crypto-actifs : L'Europe face aux États-Unis (consulté le 22 février 2025)

¹¹⁶ *Idem*.

¹¹⁷ Village de la Justice, Droit et cryptomonnaies : Enjeux et perspectives site internet (consulté le 22 février 2025)

¹¹⁸ *Idem*.

nécessité d'une coordination plus efficace entre les autorités fédérales et étatiques afin d'établir une régulation plus claire et équilibrée.

La régulation de la blockchain et des crypto-actifs varie considérablement d'un pays à l'autre, oscillant entre des cadres législatifs stricts, comme en France et en Europe avec MiCA, et des approches plus fragmentées, comme aux États-Unis et au Canada. Si l'Union européenne cherche à harmoniser ses règles pour assurer transparence, protection des investisseurs et stabilité financière, les États-Unis et le Canada adoptent des régulations plus dispersées, rendant l'application du droit plus incertaine. Malgré ces efforts, plusieurs défis demeurent, notamment le manque d'harmonisation internationale, la distinction floue entre crypto-actifs et valeurs mobilières, ainsi que les problèmes fiscaux et de lutte contre le blanchiment d'argent. Pour garantir un développement sécurisé et équilibré de la blockchain, il est essentiel d'adopter des régulations flexibles et adaptées aux évolutions technologiques, tout en trouvant un équilibre entre innovation et sécurité juridique.

2.2 La brevetabilité de la blockchain : un cadre juridique encore incertain

La blockchain est une technologie qui repose sur un protocole informatique permettant d'enregistrer des transactions de manière sécurisée, décentralisée et immuable. Cependant, l'application du droit de la propriété intellectuelle à la blockchain soulève des défis spécifiques, notamment en matière de brevetabilités. En principe, les programmes informatiques ne sont pas brevetables en tant que tels, sauf s'ils font partie d'un procédé technique ayant un effet technique concret. Ainsi, bien qu'une blockchain seule ne puisse être brevetée, certaines de ses applications spécifiques peuvent l'être si elles impliquent des interactions techniques avancées (cryptographie, architecture matérielle spécifique) ¹¹⁹.

L'Office Européen des Brevets (OEB) et la jurisprudence française ont confirmé que le critère déterminant pour la brevetabilité est le caractère technique démontrable. Cependant, cette reconnaissance se heurte au principe de territorialité des brevets : un brevet délivré en France, par

¹¹⁹ Thibaut Labbé. Le droit face aux technologies disruptives : le cas de la blockchain. Droit. Université de Strasbourg, 2021. Français. P.53

exemple, n'a aucun effet en Chine ou aux États-Unis, ce qui complique la protection des inventions blockchain à l'échelle mondiale. Contrairement aux brevets classiques qui protègent des inventions dans un pays donné, la blockchain est un système global, rendant son contrôle juridique extrêmement complexe ¹²⁰.

Un exemple illustrant cette difficulté est la demande de brevet EP 3 200 167 déposée par Mastercard, qui vise à faciliter les remboursements via la blockchain. L'Office Européen des Brevets (OEB) a refusé sa délivrance, estimant que l'invention ne remplissait pas l'exigence d'activité inventive, car elle reposait simplement sur un échange de données entre utilisateurs et non sur un effet technique distinctif. Cette situation montre que les autorités européennes appliquent des critères plus rigoureux que les États-Unis, où la jurisprudence a également renforcé les exigences en matière de brevetabilité des logiciels¹²¹.

Un autre obstacle majeur réside dans le caractère mondial de la blockchain, qui entre en contradiction avec le système actuel des brevets, fondé sur des protections nationales. Chaque pays applique ses propres règles, ce qui signifie qu'une entreprise ne peut pas simplement déposer un brevet unique couvrant toute la blockchain. Pour renforcer la protection, les inventeurs doivent breveter des éléments techniques précis, comme les algorithmes de validation des transactions, afin de cibler des acteurs identifiables, tels que les fermes de minage ou les serveurs ¹²².

En revanche, certains brevets liés à la blockchain ont bien été délivrés, notamment pour des projets intégrant des innovations cryptographiques avancées ou des architectures techniques spécifiques. Ainsi, bien que la protection par brevet des technologies blockchain reste possible, elle demeure incertaine et soumise à une évaluation stricte des critères techniques. Cette situation pose un défi supplémentaire : une fois un brevet accordé, quelles seront les limites et les usages légaux possibles

¹²⁰ August Debouzy, Les "brevets blockchain" : état des lieux et perspectives, 2021. Disponible sur : <https://www.august-debouzy.com/fr/blog/1249-les-brevets-blockchain-etat-des-lieux-et-perspectives?utm>

¹²¹ *Idem*.

¹²² *Idem*.

? Cette question est d'autant plus pertinente que certaines entreprises pourraient utiliser ces brevets pour verrouiller l'innovation ou engager des contentieux stratégiques contre des concurrents ¹²³.

La protection juridique de la blockchain est un enjeu complexe, en raison de la décentralisation de cette technologie et des limites du droit des brevets. Alors que les innovations blockchain offrent des opportunités majeures, elles nécessitent un équilibre entre protection des inventeurs et maintien d'un accès ouvert à la technologie. La jurisprudence actuelle, notamment en Europe, montre une approche plus stricte sur la brevetabilité des logiciels blockchain, tandis que les brevets déjà accordés posent la question de leur usage et de leur impact sur l'innovation. Dans ce contexte, l'adoption de nouvelles stratégies de protection et une évolution des cadres normatifs seront essentielles pour garantir un développement équilibré et sécurisé de la blockchain.

2.3 La protection des données et le RGPD : un conflit avec l'immutabilité de la blockchain

L'un des principaux défis juridiques liés à la blockchain concerne sa compatibilité avec le Règlement général sur la protection des données (RGPD). Adopté par l'Union européenne en 2016 et appliqué depuis 2018, ce règlement vise à garantir aux citoyens des droits fondamentaux sur leurs données personnelles, notamment le droit à l'oubli, le droit de rectification et le droit à la portabilité des données ¹²⁴. Toutefois, ces principes entrent en contradiction avec les caractéristiques fondamentales de la blockchain, notamment son immuabilité et sa décentralisation, qui rendent impossible toute modification ou suppression des informations une fois enregistrées sur le registre distribué ¹²⁵.

Le RGPD impose également une exigence de responsabilité : chaque traitement de données personnelles doit être supervisé par un responsable du traitement identifié, chargé de garantir la conformité aux obligations légales. Or, dans une blockchain publique et décentralisée, où les données sont réparties sur un réseau de participants sans autorité centrale, il est extrêmement

¹²³ *Idem*.

¹²⁴ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, Journal officiel de l'Union européenne. Disponible sur : <https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=fr>

¹²⁵ Finck, M. (2018), "Blockchain Regulation and Governance in Europe", Cambridge University Press.P.6

difficile de désigner un responsable unique. Cette absence d'intermédiaire soulève un flou juridique sur l'application des obligations légales et sur la protection des utilisateurs ¹²⁶.

Un autre point de friction majeur concerne le droit à l'oubli, qui permet aux individus de demander l'effacement de leurs données lorsqu'elles ne sont plus nécessaires. Cependant, la blockchain repose sur un principe d'immutabilité, rendant techniquement impossible toute suppression de données sans altérer l'ensemble du registre. Modifier ou supprimer une seule information nécessiterait un consensus du réseau entier, ce qui est incompatible avec les règles actuelles du RGPD¹²⁷. Enfin, le droit à la portabilité des données, qui permet aux utilisateurs de récupérer et transférer leurs informations entre services, est difficile à mettre en œuvre dans un système blockchain. Contrairement aux bases de données traditionnelles, les blockchains ne sont pas nécessairement interopérables entre elles, ce qui limite la possibilité pour un utilisateur de transférer ses données vers une autre plateforme ¹²⁸.

Ces tensions entre les principes du RGPD et le fonctionnement technique de la blockchain illustrent la nécessité de trouver des solutions juridiques et technologiques adaptées. L'enjeu est de garantir la conformité réglementaire sans compromettre les avantages de la blockchain en matière de transparence, de sécurité et de résilience.

L'un des principaux défis juridiques liés à la blockchain concerne l'identification du responsable du traitement des données, une obligation centrale imposée par le Règlement général sur la protection des données (RGPD). Dans un système centralisé, une entreprise ou une institution est clairement responsable des données traitées. Or, la nature décentralisée de la blockchain complique cette identification, car aucune entité unique ne contrôle l'ensemble du registre. Plusieurs hypothèses ont été avancées pour désigner un responsable : certains considèrent que les plateformes d'échange de cryptomonnaies doivent assumer ce rôle, tandis que d'autres estiment que les

¹²⁶ Poullet, Y. & Jacquemin, H. (2018). Blockchain: une révolution pour le droit ? Disponible sur : <https://pure.unamur.be/ws/portalfiles/portal/54654924/8316.pdf>

¹²⁷ *Idem*.

¹²⁸ *Idem*.

développeurs des blockchains ou des applications décentralisées (DApps) devraient être tenus responsables, puisqu'ils conçoivent les protocoles permettant l'enregistrement des données ¹²⁹.

Toutefois, une fois une blockchain déployée, elle fonctionne de manière autonome, sans contrôle direct de ses créateurs, ce qui rend cette approche juridiquement discutable. Par ailleurs, les mineurs et les nœuds, qui valident les transactions sur la blockchain, jouent un rôle purement technique sans exercer d'influence sur le contenu des données traitées. Cela complique davantage l'attribution d'une responsabilité claire, rendant l'application du RGPD incertaine. Face à ce flou juridique, la Commission Nationale de l'Informatique et des Libertés (CNIL) a proposé que les utilisateurs eux-mêmes soient responsables des données qu'ils enregistrent sur la blockchain. Cependant, cette approche soulève des critiques, comment un utilisateur commun pourrait-il être responsable d'un processus qu'il ne maîtrise pas totalement ? Cette incertitude met en évidence la nécessité d'une adaptation du cadre réglementaire afin de garantir un équilibre entre innovation technologique et protection des données personnelles ¹³⁰.

Un autre défi majeur concerne la sécurité et la gestion des violations de données sur la blockchain. Dans un système traditionnel, en cas de fuite ou d'attaque informatique, les victimes peuvent demander réparation auprès du responsable du traitement. En revanche, dans la blockchain, l'absence d'autorité centrale pose un problème inédit : si des données personnelles sont compromises, aucun acteur identifié ne peut être tenu responsable¹³¹. De plus, même si un acteur de la blockchain était jugé responsable, il n'aurait pas forcément accès aux données en clair ni la capacité technique d'y remédier. En somme, l'absence de contrôle centralisé sur les données stockées sur la blockchain crée une incompatibilité majeure avec le RGPD, en empêchant non seulement l'exercice des droits fondamentaux (effacement, rectification, portabilité), mais aussi toute action en responsabilité en cas de violation des données. Ces défis soulignent l'urgence de trouver des solutions techniques et juridiques adaptées pour permettre une conformité de la

¹²⁹ Mornet, A. (2021). Y a-t-il un pilote dans la blockchain ? Réflexions sur l'identification d'un responsable de traitement dans le cadre de la blockchain.p.6

¹³⁰ *Idem*.p.7

¹³¹ *Idem*. p. 8

blockchain avec le RGPD, sans compromettre ses avantages en matière de transparence, de sécurité et d'intégrité des transactions¹³².

La pseudonymisation et l'anonymisation sont deux concepts essentiels du Règlement Général sur la Protection des Données (RGPD), visant à limiter l'exposition des données personnelles tout en garantissant leur sécurité. La pseudonymisation consiste à modifier les données de manière qu'elles ne puissent plus être directement attribuées à une personne sans utiliser des informations complémentaires sécurisées. Toutefois, ces données restent potentiellement identifiables si des moyens techniques suffisants permettent de les relier à un individu, ce qui les maintient sous le champ d'application du RGPD¹³³. L'anonymisation, en revanche, transforme les données de façon irréversible, rendant impossible toute identification, ce qui les exclut du cadre du RGPD. La difficulté réside dans la frontière entre ces deux procédés : certaines données pseudonymisées pourraient être requalifiées en données anonymes si les moyens nécessaires pour retrouver l'identité sont jugés "déraisonnables" en termes de complexité ou de coûts¹³⁴.

Dans le cadre de la blockchain, les transactions sont enregistrées sous forme de signatures électroniques cryptées, ce qui complique l'identification directe des utilisateurs. Cependant, ces données ne sont pas totalement anonymes, car les clés publiques utilisées pour signer les transactions peuvent permettre d'identifier une personne par l'analyse des interactions sur la blockchain¹³⁵. Cette particularité soulève un débat juridique fondamental : une blockchain peut-elle être considérée comme conforme au RGPD si elle utilise des données cryptées ou hashées. Si seules les parties autorisées (comme l'émetteur et le destinataire) peuvent décrypter les informations, alors les données conservent un caractère personnel, ce qui implique le respect des exigences du RGPD. En revanche, si le système utilise des techniques avancées de cryptographie, telles que des signatures renouvelées à chaque transaction ou des protocoles de confidentialité améliorés (comme les Zero-Knowledge Proofs), l'identification devient quasiment impossible pour

¹³² *Idem*.p.9

¹³³ Pouillet, Y. & Delforge, A. (2020). Les blockchains : un défi et/ou un outil pour le RGPD ? p. 102

¹³⁴ *Idem*.p.103

¹³⁵ *Idem*. p. 104

des tiers. Ce type d'approche rapprocherait la blockchain d'un modèle d'anonymisation, la soustrayant ainsi aux obligations du RGPD¹³⁶.

Ce débat est crucial, car il influence directement l'obligation ou non pour les blockchains de se conformer au RGPD. Il met en lumière la nécessité d'adapter les cadres réglementaires, soit en précisant les critères d'identification des données blockchain, soit en développant des solutions techniques permettant de concilier innovation et protection des données personnelles.

2.4 Responsabilité juridique dans la blockchain décentralisée

La responsabilité juridique dans une blockchain décentralisée est un enjeu complexe, car cette technologie repose sur l'absence d'une autorité centrale et sur un fonctionnement distribué impliquant plusieurs acteurs. Szostek, dans son étude comparative du droit de la blockchain, souligne que cette absence de responsable identifiable constitue l'un des défis les plus aigus posés par la technologie dans l'ensemble des systèmes juridiques contemporains¹³⁷. Contrairement aux systèmes traditionnels où une entité identifiable peut être tenue responsable, la blockchain répartit ses opérations entre développeurs, mineurs, nœuds validateurs, utilisateurs et plateformes d'échange. Cette décentralisation rend difficile l'application des règles de responsabilité civile et pénale et pose des défis aux régulateurs, notamment en matière de protection des consommateurs, de lutte contre la fraude et de respect des législations nationales et internationales. Il est donc nécessaire de clarifier les rôles et obligations de chaque acteur afin d'éviter des « zones grises » juridiques.¹³⁸

Dans un environnement fondé sur la technologie de la blockchain, la question de la responsabilité juridique se heurte à l'absence d'une autorité centrale capable d'exercer un contrôle direct sur les transactions et de faire respecter les obligations. Comme le souligne Savelyev, l'une des caractéristiques clés de la blockchain réside dans son « irréversibilité » et son « unicité » de l'information, ce qui signifie qu'il est pratiquement impossible de modifier ou d'annuler une

¹³⁶ *Idem*.p.105

¹³⁷ Dariusz Szostek, *Blockchain and the Law*, 1^e éd. (Baden-Baden : Nomos, 2019).

¹³⁸ Webinaire Blockchain & Risques : « Responsabilité et Gouvernance », p.3, p.4, Banque de France, 12 janvier 2021

transaction une fois qu'elle est inscrite dans la chaîne¹³⁹. Autrement dit, le système exécute automatiquement le contrat, sans tenir compte, par exemple, d'erreurs ou de fraudes. Les règles habituelles du droit (comme la possibilité de rompre un contrat pour vice de consentement)¹⁴⁰ s'appliquent mal à cette technologie, puisque personne ne peut « forcer » la blockchain à se corriger¹⁴¹. Cela pose un gros problème de responsabilité : si un juge estime qu'une transaction est illégale, il est quasiment impossible de faire refléter cette décision dans la blockchain elle-même. Ainsi, comme le souligne l'auteur, l'État doit donc choisir entre disposer d'un statut spécial lui permettant d'agir directement sur la chaîne (au risque d'en affaiblir la sécurité) ou poursuivre les responsables dans le monde « réel » d'où une vraie difficulté à faire coexister un système décentralisé et la protection légale traditionnelle¹⁴². Pour l'instant, la responsabilité juridique dans une blockchain décentralisée reste un grand défi, car elle doit concilier la nature immuable de la technologie avec la nécessité d'un contrôle légal efficace.

Un autre point de tension majeur concerne la responsabilité des mineurs et des nœuds validateurs, qui assurent la validation et l'enregistrement des transactions sur la blockchain. Leur rôle technique est essentiel, mais leur implication juridique est incertaine, car ils exécutent des tâches automatisées sans analyser le contenu des transactions validées¹⁴³. Cette absence de contrôle soulève des inquiétudes, notamment en matière de blanchiment d'argent et de financement du terrorisme, car certaines transactions illicites peuvent être validées sans que les mineurs n'en aient conscience. La Commission Nationale de l'Informatique et des Libertés (CNIL) a avancé l'hypothèse que les mineurs et nœuds pourraient être considérés comme co-responsables du traitement des données

¹³⁹ Savelyev, Alexander, Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law (December 14, 2016). Higher School of Economics Research Paper No. WP BRP 71/LAW/2016, Available at SSRN: <https://ssrn.com/abstract=2885241> p.6

¹⁴⁰ Bernier Fournier Avocats, «Le pouvoir de révision d'une clause du contrat en cas de dol», Publications, 2 mars 2020, <https://www.bernierfournieravocats.com/publications/2020/03/02/le-pouvoir-de-revision-dune-clause-du-contrat-en-cas-de-dol/> (consulté le 3 mars 2025)

¹⁴¹ *Idem.* p.16

¹⁴² *Idem.* p. 21

¹⁴³ Commission Nationale de l'Informatique et des Libertés (CNIL), La Blockchain face au RGPD : quelles solutions pour un usage responsable en présence de données personnelles? 24 septembre 2018, p. 6–7.

dans certaines circonstances, notamment dans les blockchains où la gouvernance est assurée par un nombre restreint d'acteurs¹⁴⁴.

Ces risques d'instrumentalisation criminelle sont loin d'être anecdotiques et méritent d'être pris au sérieux dans toute réflexion sur la blockchain et les droits humains. L'Office des Nations Unies contre la drogue et le crime rappelle que les cryptomonnaies sont devenues un vecteur de choix pour le blanchiment d'argent à l'échelle internationale, en raison notamment du pseudonymat des transactions et de la difficulté à retracer les parties impliquées¹⁴⁵. Les estimations de l'ONUDC font état de dizaines de milliards de dollars blanchis annuellement via les cryptomonnaies, une réalité qui fragilise les efforts des États en matière de lutte contre la criminalité organisée et qui soulève des questions directes en matière de droits humains, notamment pour les populations victimes de ces flux financiers illicites.

Dans le même ordre d'idées, l'OCDE relève que le crime organisé exploite de manière croissante les failles réglementaires entre les juridictions pour recourir à la blockchain à des fins illicites, tirant parti précisément de l'absence d'un cadre international harmonisé¹⁴⁶. Ce constat rappelle que la technologie, aussi prometteuse soit-elle, n'est pas neutre : sans mécanismes robustes de lutte contre le blanchiment d'argent et d'identification des parties, ses atouts peuvent être retournés contre les valeurs mêmes qu'elle prétend défendre.

Enfin, la question de la gouvernance et de la régulation globale reste un défi majeur. La blockchain fonctionne sur un réseau transnational, où les acteurs se trouvent dans plusieurs juridictions, ce qui rend difficile l'application d'une législation unique. La nature transnationale des réseaux blockchain, avec des acteurs répartis dans diverses juridictions, complique l'application d'une législation unique. Par exemple, une transaction initiée par un utilisateur en Europe, validée par des mineurs en Asie et enregistrée sur une blockchain hébergée aux États-Unis pose des défis

¹⁴⁴ *Idem.* p.12-13

¹⁴⁵ Office des Nations Unies contre la drogue et le crime (ONUDC), *Le crime international organisé et les cryptomonnaies* (Vienne : ONUDC). Voir aussi : ONUDC, *Organized Crime Strategy Toolkit for Developing High-impact Strategies* (Vienne : ONUDC).

¹⁴⁶ Organisation de coopération et de développement économiques (OCDE), *Crime organisé et corruption : Perspectives de l'OCDE sur l'intégrité et la lutte contre la corruption 2026* (Paris : OCDE, 2026).

juridiques complexes. L'affaire Tezos illustre ces enjeux : malgré les tentatives des défendeurs de situer l'entité vendeuse en Europe et les ventes en dehors des États-Unis, le tribunal a estimé que le fait qu'un plaignant américain ait effectué des achats via des sites web basés aux États-Unis, résultant d'un marketing ciblant les États-Unis, justifiait l'application des lois américaines sur les valeurs mobilières. Cette affaire souligne les défis liés à la détermination de la juridiction appropriée dans les transactions blockchain transnationales, en raison de la dispersion géographique des parties impliquées et de l'absence d'une autorité centrale régulatrice¹⁴⁷.

Ainsi, la responsabilité juridique dans la blockchain décentralisée est un enjeu crucial nécessitant des ajustements législatifs pour s'adapter aux spécificités de cette technologie. Si certaines réglementations comme MiCA en Europe¹⁴⁸ et l'action de la SEC aux États-Unis cherchent à structurer l'écosystème blockchain, plusieurs questions restent en suspens. Comment concilier décentralisation et régulation ? Qui doit être tenu responsable en cas de fraude ou de perte de fonds ? Comment assurer une protection efficace des utilisateurs tout en laissant place à l'innovation¹⁴⁹ ? L'avenir du droit appliqué à la blockchain repose probablement sur des solutions hybrides, combinant régulation intelligente, certification des smart contracts, mise en place d'autorités de supervision spécialisées et développement de blockchains conformes aux exigences légales. Un équilibre devra être trouvé entre progrès technologique, sécurité juridique et protection des droits fondamentaux, afin de garantir une adoption responsable et durable de la blockchain dans les systèmes économiques et sociaux¹⁵⁰.

¹⁴⁷ What's Extraterritorial on the Blockchain? In re Tezos Securities Litigation and the Application of U.S. Securities Law to Foreign ICOs," Washington Legal Foundation (WLF Legal Pulse), 10 septembre 2018. Disponible sur <https://www.kramerlevin.com/a/web/2335/160328-Blockchain-Note-de-position-Kramer-Levin-Croissance-Plus-PME-Finance.pdf>

¹⁴⁸ Autorité des marchés financiers (AMF), Le règlement européen Markets in Crypto-Assets (MiCA), disponible sur : amf-france.org.

¹⁴⁹ Skadden, Crypto Regulation: Who Will Protect Consumers Against Fraud : disponible sur <https://www.skadden.com/insights/publications/2025/02/crypto-regulation-who-will-protect-consumers?>

¹⁵⁰ Coin Center, Principles for Crypto Legislation, disponible sur: <https://www.coincenter.org/principles-legislation/>

2.5 L'instrumentalisation criminelle de la blockchain

La blockchain est souvent célébrée pour sa transparence et son potentiel en matière de protection des droits humains. Pourtant, cette même technologie peut être détournée à des fins bien moins nobles. Son architecture décentralisée et l'anonymat relatif qu'elle offre en font également un outil prisé par les réseaux criminels organisés, notamment pour le blanchiment de capitaux et le financement d'activités illicites à l'échelle transnationale¹⁵¹.

L'Office des Nations Unies contre la drogue et le crime (ONUDC) a documenté de manière approfondie comment les cryptomonnaies, dont la grande majorité reposent sur des infrastructures blockchain, sont utilisées pour déplacer des sommes considérables à travers les frontières en contournant les mécanismes de surveillance financière traditionnels¹⁵². Ce phénomène n'est pas marginal : il représente un défi structurel pour les États et les organisations internationales qui tentent de réguler ces flux. L'OCDE, dans ses perspectives sur l'intégrité et la lutte contre la corruption publiée en 2026, va plus loin en soulignant que les fonds ainsi détournés auraient pu, dans d'autres circonstances, alimenter des programmes humanitaires ou renforcer des institutions judiciaires fragilisées¹⁵³.

C'est là que réside le paradoxe le plus inconfortable de cette technologie : les propriétés techniques qui permettent à un militant des droits humains de communiquer à l'abri de la censure étatique sont précisément celles qui permettent à un réseau criminel d'échapper à toute surveillance judiciaire. Il ne s'agit pas d'un simple détail technique, mais bien d'une tension profonde qui devrait traverser toute réflexion sérieuse sur la régulation de la blockchain. Trouver le bon équilibre s'avère délicat : un encadrement trop strict risque d'étouffer les usages légitimes et protecteurs, tandis qu'une

¹⁵¹ Office des Nations Unies contre la drogue et le crime (ONUDC), Le crime international organisé et les cryptomonnaies (Vienne : ONUDC) ; ONUDC, Organized Crime Strategy Toolkit for Developing High-impact Strategies (Vienne : ONUDC), en ligne : <<https://www.unodc.org>>.

¹⁵² Idem. Voir également : Cryptomonnaies : un boulevard pour le blanchiment d'argent, rapport ONUDC, en ligne : <<https://www.unodc.org>>.

¹⁵³ Organisation de coopération et de développement économiques (OCDE), Crime organisé et corruption : Perspectives de l'OCDE sur l'intégrité et la lutte contre la corruption 2026 (Paris : OCDE, 2026), en ligne : <<https://www.oecd.org>>.

approche trop permissive expose les systèmes financiers et humanitaires à des risques systémiques réels¹⁵⁴.

CHAPITRE 3 : VERS UNE RÉGULATION JURIDIQUE ADAPTÉE DE LA BLOCKCHAIN POUR LA PROTECTION DES DROITS HUMAINS

Les chapitres précédents ont mis en évidence les opportunités et les défis qu'offre la blockchain dans le domaine des droits humains. D'une part, cette technologie ouvre la voie à une meilleure traçabilité et à la distribution plus équitable de l'aide humanitaire, en facilitant notamment la gestion d'identités numériques pour les populations les plus vulnérables. D'autre part, son caractère immuable et décentralisé entre souvent en tension avec des principes juridiques fondamentaux, tels que le droit à l'oubli et la responsabilité juridique. Dès lors, il paraît indispensable de s'interroger sur la manière dont les régulations nationales et internationales peuvent évoluer pour intégrer ces nouvelles réalités technologiques. Ce troisième chapitre propose d'analyser, dans un premier temps, la nécessité d'un cadre international harmonisé, avant d'examiner les perspectives d'évolution juridique pouvant concilier innovation et respect effectif des droits humains.

3.1 Les limites d'une approche purement nationale

La blockchain, en tant que technologie décentralisée et distribuée, dépasse par essence les frontières géographiques et juridiques des États, rendant ainsi inopérante une régulation cantonnée à un seul territoire.¹⁵⁵ Le fait que les nœuds du réseau puissent être localisés dans différentes juridictions accroît la complexité de la mise en conformité, surtout lorsqu'il s'agit de protéger efficacement les droits humains, tels que le droit à la vie privée ou le droit à l'identité. Les législations nationales actuelles, qu'elles soient issues de pays pionniers comme la France avec la Loi PACTE ou de grands ensembles régionaux comme l'Union européenne via le règlement MiCA,

¹⁵⁴ Michèle Finck, *Blockchain Regulation and Governance in Europe* (Cambridge : Cambridge University Press, 2019), p. 78–80 ; Kevin Werbach, *The Blockchain and the New Architecture of Trust* (Cambridge : MIT Press, 2018), p. 89–90.

¹⁵⁵ Finck, M., *Blockchain Regulation and Governance in Europe*, Cambridge University Press, 2019, p. 12

peinent à couvrir tous les enjeux transfrontaliers de la blockchain¹⁵⁶. D'une part, cette hétérogénéité réglementaire provoque un phénomène de "*forum shopping*", où les acteurs économiques choisissent délibérément la juridiction la plus favorable ou la moins contraignante, sans nécessairement se soucier de l'impact sur la protection des droits fondamentaux. Cette problématique est au cœur des travaux de Bonomi, Lehmann et Lalani sur la blockchain et le droit international privé, qui démontrent que la détermination de la loi applicable aux transactions blockchain demeure l'une des questions les plus ouvertes du droit transnational contemporain¹⁵⁷.

D'autre part, le manque de coordination entre États crée un vide juridique pour les usagers dont les données personnelles ou financières circulent dans un espace numérique mondial, échappant souvent à la compétence d'un juge national¹⁵⁸. En matière de droits humains, cette carence de cadre harmonisé se révèle particulièrement problématique : les victimes de violations constatent que les responsabilités sont diluées entre multiples intervenants, et que les voies de recours sont entravées par les divergences des lois nationales¹⁵⁹.

En outre, les évolutions rapides de la blockchain, combinées à l'émergence de nouvelles applications comme les identités numériques décentralisées ou les smart contracts humanitaires, soulignent la nécessité d'une coopération internationale réelle¹⁶⁰. Si certains pays ont tenté d'encadrer les crypto-actifs ou la gestion des données sur une blockchain, ces réformes demeurent souvent partielles et ne répondent pas pleinement aux défis majeurs liés à la protection des individus. Dès lors, il devient indispensable de dépasser l'approche purement nationale au profit

¹⁵⁶ Règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés de crypto-actifs (MiCA) ; Loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises (Loi PACTE).

¹⁵⁷ Andrea Bonomi, Matthias Lehmann et Shazia Lalani (dir.), *Blockchain and Private International Law* (Leiden : Brill/Nijhoff, 2023).

¹⁵⁸ Werbach, K., *The Blockchain and the New Architecture of Trust*, MIT Press, 2018, p. 89-90 disponible sur : <https://direct.mit.edu/books/book/4168/The-Blockchain-and-the-New-Architecture-of-Trust>

¹⁵⁹ De Filippi, P. et Hassan, S., "Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code", *First Monday*, vol. 21, n°12, 2016, en ligne : disponible sur : https://www.researchgate.net/publication/311447869_Blockchain_Technology_as_a_Regulatory_Technology_From_Code_is_Law_to_Law_is_Code

¹⁶⁰ Lessig, L., *Code and Other Laws of Cyberspace*, Basic Books, 1999, chap. 7

d'un modèle fondé sur un dialogue multilatéral, afin de garantir que les principes fondamentaux (dignité, sécurité, vie privée) soient préservés au-delà des frontières¹⁶¹.

3.2 Vers une coordination multilatérale : l'intérêt des organisations internationales.

La complexité de la régulation de la blockchain, notamment lorsqu'elle concerne des enjeux de protection des droits humains, exige une approche concertée entre les États et les grandes organisations internationales¹⁶². En effet, si chaque pays s'efforce de légiférer sur l'utilisation de la blockchain dans sa propre sphère de compétence, l'absence d'un cadre commun risque de maintenir une fragmentation réglementaire peu propice à la protection effective des individus. Les Nations unies, via ses agences spécialisées comme le Haut-Commissariat pour les Réfugiés (HCR) ou le Programme Alimentaire Mondial (PAM), ont déjà démontré l'intérêt de la blockchain pour sécuriser et tracer l'aide humanitaire, tout en soulignant la nécessité de règles internationales claires pour encadrer ces pratiques¹⁶³.

Une coordination multilatérale présente l'avantage de pouvoir établir des standards minimaux, tant sur le plan de la gouvernance technique que sur celui de la protection juridique. Magnuson, dans son analyse de la blockchain comme phénomène démocratique, affirme que la gouvernance distribuée ne peut fonctionner sans un ancrage dans des institutions légitimes capables de protéger les droits des individus¹⁶⁴. Dans le même sens, Lehmann démontre que l'émergence d'une économie crypto à l'échelle mondiale rend inévitable l'élaboration de règles de droit international capables de s'appliquer aux transactions blockchain au-delà des frontières¹⁶⁵. À l'image des conventions internationales en matière de cybercriminalité ou de droits de l'enfant, un instrument

¹⁶¹ Wright, A. et De Filippi, P., "Decentralized Blockchain Technology and the Rise of Lex Cryptographia", SSRN, 2015

¹⁶² Finck, M., *Blockchain Regulation and Governance in Europe*, Cambridge University Press, 2019, p. 25

¹⁶³ Programme Alimentaire Mondial (PAM), "Building Blocks: Harnessing Blockchain to Improve Humanitarian Assistance", WFP Official Website, 2020 En ligne : (<https://innovation.wfp.org/project/building-blocks>) consulté le 8 mars 2025

¹⁶⁴ William J. Magnuson, *Blockchain Democracy: Technology, Law and the Rule of the Crowd* (Cambridge : Cambridge University Press, 2020).

¹⁶⁵ Matthias Lehmann, *Crypto Economy and International Law: Determining the Regulatory and Private Law Rules Governing the Blockchain* (Leiden : Brill/Nijhoff, 2025).

juridique spécifique pourrait fixer des lignes directrices applicables aux blockchains transnationales, définissant par exemple les mécanismes de contrôle ou de sanction à mettre en place en cas de violation des droits fondamentaux¹⁶⁶. Cette approche s'avèrerait particulièrement pertinente pour traiter des problématiques telles que l'immutabilité des données, la responsabilité des acteurs impliqués et la vision des identités numériques.

À cet égard, la Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit¹⁶⁷, adoptée en 2024 et signée par le Canada le 11 février 2025, constitue un précédent normatif important. Bien que ce traité porte spécifiquement sur l'intelligence artificielle, ses principes directeurs notamment l'exigence de transparence, de responsabilité, de non-discrimination et de respect des droits fondamentaux dans la conception et le déploiement des systèmes algorithmiques sont directement transposables, par analogie, aux technologies décentralisées comme la blockchain. Cette convention illustre la capacité du droit international à s'adapter aux défis posés par les technologies émergentes et pourrait servir de modèle pour l'élaboration d'un instrument similaire dédié à la blockchain¹⁶⁸.

Le Manuel de Tallinn 2.0 offre également un éclairage précieux sur ces questions. Rédigé par un groupe d'experts internationaux à l'invitation du Centre d'excellence en cybersécurité coopérative de l'OTAN, ce document analyse l'applicabilité du droit international au cyberspace. Ses règles 84 à 95, consacrées aux droits humains dans l'espace numérique, affirment clairement que les États restent tenus par leurs obligations internationales même dans le cyberspace, en ce qui concerne notamment le droit à la vie privée et la liberté d'expression¹⁶⁹. Bien que ce manuel ait été conçu principalement pour les situations de conflit armé dans le cyberspace, ses principes sur la souveraineté numérique (règle 35) et la responsabilité étatique (règle 6) restent pertinents pour

¹⁶⁶De Filippi, P., *Blockchain and the Law: The Rule of Code*, Harvard University Press, 2018, p. 36 En ligne : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5086109 consulté le 8 mars 2025

¹⁶⁷ *Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit*, STCE n° 225, ouverte à la signature le 5 septembre 2024, signée par le Canada le 11 février 2025.

¹⁶⁸ *Idem*.

¹⁶⁹ Michael N. Schmitt (dir.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2^e \u00e9d. (Cambridge : Cambridge University Press, 2017), règles 6, 35 et 84–95, pp. 168–170 et 180–196.

encadrer la blockchain, dont le déploiement transnational soulève des questions très similaires de gouvernance et de protection des individus à l'échelle internationale.

Par ailleurs, dans le domaine de la protection des droits humains, la coopération avec les ONG et la société civile revêt une importance cruciale. Ces dernières pourraient contribuer à la définition de bonnes pratiques en participant à des groupes de travail aux côtés d'institutions publiques et d'experts techniques¹⁷⁰. Enfin, cette logique de concertation internationale faciliterait également l'échange d'expériences et la mutualisation de solutions techniques pour respecter l'exigence de confidentialité des données et assurer un contrôle efficace en cas d'abus.

3.3 Réforme de la responsabilité dans les systèmes décentralisés

Dans un système de blockchain, la responsabilité juridique se trouve profondément remise en question par l'absence d'autorité centrale et par le fonctionnement collaboratif du réseau. Alors que, dans les architectures classiques, on identifie aisément un responsable du traitement ou un opérateur principal, la décentralisation induit une multiplicité d'acteurs comme les développeurs, mineurs, validateurs, utilisateurs etc. Dont aucun ne détient, à lui seul, la maîtrise complète du registre¹⁷¹. Cette division du pouvoir de décision soulève de manière inédite la question de la responsabilité en cas de litige, d'atteinte aux droits humains ou d'usage illicite de la blockchain.

D'abord, la notion même de « faute » est brouillée : un mineur qui valide un bloc, par exemple, n'a pas nécessairement connaissance de son contenu, pas plus qu'il ne peut exercer un contrôle effectif sur la nature légale ou illégale des transactions qu'il incorpore dans la chaîne¹⁷². De la même façon, un développeur de smart contract peut écrire le code, mais il ne gère pas toujours son exécution, car celle-ci est automatique et dépend de conditions prédéfinies. Les règles classiques de

¹⁷⁰ Programme Alimentaire Mondial (PAM), "Building Blocks: Harnessing Blockchain to Improve Humanitarian Assistance", *WFP Official Website*, 2020 En ligne : (<https://innovation.wfp.org/project/building-blocks>) consulté le 8 mars 2025

¹⁷¹ De Filippi, Primavera and Mannan, Morshed and Reijers, Wessel, Blockchain Technology and the Rule of Code: Regulation via Governance (December 22, 2024) p. 26. Available at SSRN: <https://ssrn.com/abstract=5086109> or <http://dx.doi.org/10.2139/ssrn.5086109>

¹⁷² Raskin, Max, The Law and Legality of Smart Contracts (September 22, 2016). 1 Georgetown Law Technology Review 304 (2017), p. 306 Available at SSRN: <https://ssrn.com/abstract=2959166>

responsabilité civile ou pénale, basées sur l'idée de lien de causalité et de faute personnelle, ont donc du mal à s'appliquer directement à un système décentralisé ¹⁷³.

Pour répondre à ce problème, certains spécialistes parlent de « responsabilité partagée » : tous les acteurs que ce soit mineurs, créateurs ou utilisateurs endosseraient collectivement les conséquences en cas de dysfonctionnement. Toutefois, c'est difficile à mettre en pratique : il serait injuste de tenir pour responsables tous les participants lorsque seuls quelques-uns ont participé à une fraude ou causé une violation d'un droit¹⁷⁴. À l'inverse, tout faire reposer sur la personne ou l'organisation qui lance la blockchain comme une entreprise ou une fondation irait à l'encontre du principe même de décentralisation, qui doit fonctionner de manière autonome¹⁷⁵.

D'autres proposent un modèle d'auto-régulation technique, en s'appuyant sur la « Lex Cryptographia » décrite par Wright et De Filippi. Selon cette approche, les règles légales seraient remplacées ou complétées par le code informatique lui-même¹⁷⁶. Les smart contracts, qui s'exécutent automatiquement, élimineraient en théorie une partie des incertitudes liées aux interventions humaines. Toutefois, cela ne règle pas la question de la justice : que faire lorsqu'un smart contract agit de façon abusive ou en violation des droits humains ? Qui peut le stopper, le modifier ou le rendre invalide si tout est supposé être immuable.

Une solution en développement consiste à mélanger droit étatique et régulation décentralisée en créant des « bacs à sable » réglementaires où les projets blockchain sont testés sous la surveillance des pouvoirs publics¹⁷⁷. Dans ce cadre, on peut exiger des règles de transparence pour les développeurs, ainsi que des mécanismes de gouvernance comme l'arbitrage ou les DAO disposant de procédures de règlement des litiges. Les gouvernements ou les organisations internationales pourraient aussi obliger à installer des « garde-fous » techniques par exemple la possibilité d'un «

¹⁷³ *Idem.* p. 306-307

¹⁷⁴ De Filippi, P. et Wright, A., *Blockchain and the Law: The Rule of Code*, Harvard University Press, 2018, p. 84-86

¹⁷⁵ *Idem.*

¹⁷⁶ Wright, Aaron and De Filippi, Primavera, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia* (March 10, 2015). P. 46 Available at SSRN: <https://ssrn.com/abstract=2580664>

¹⁷⁷ Commission européenne, "La Commission lance un bac à sable réglementaire européen pour la blockchain", 14 février 2023, disponible sur : digital-strategy.ec.europa.eu (consulté le 8 mars 2025)

hard fork » validé par une large majorité pour corriger la blockchain quand il y a une atteinte grave aux droits fondamentaux¹⁷⁸.

En fin de compte, réfléchir à la responsabilité dans la blockchain montre bien qu'il faut trouver un équilibre entre l'innovation et la protection des individus. Il ne s'agit pas de nier la décentralisation, mais plutôt de l'organiser légalement pour que les victimes de violations ne soient pas sans recours. Le recours à des instances spécialisées arbitrales ou judiciaires et la mise en place de cadres législatifs souples, tenant compte des spécificités techniques, ouvrent la voie à une meilleure cohérence entre l'autonomie de la blockchain et les principes de responsabilité essentiels dans toute société qui respecte les droits humains¹⁷⁹.

3.4 La souveraineté numérique et la nécessité d'une approche globale

La blockchain, par sa nature distribuée et transfrontalière, bouscule aussi les notions de souveraineté numérique, c'est-à-dire la capacité d'un État à exercer son autorité sur l'espace numérique présent sur son territoire. En effet, lorsqu'une blockchain s'étend sur plusieurs pays, aucune autorité nationale n'a véritablement le pouvoir d'imposer à l'ensemble du réseau un cadre légal unique¹⁸⁰. Cette situation complique la tâche des gouvernements qui souhaitent, par exemple, appliquer leurs lois sur la protection des données ou contrôler les flux financiers associés aux crypto-actifs.

D'un côté, certains États tentent de mettre en place des réglementations nationales strictes, afin d'imposer des obligations d'enregistrement aux entreprises et de mieux identifier les acteurs opérant sur leur territoire. C'est le cas, par exemple, de la BitLicense instaurée à New York, qui exige une autorisation préalable pour toute société souhaitant proposer des services liés à la

¹⁷⁸ Coindesk, "Understanding The DAO Attack", disponible sur <https://www.coindesk.com/learn/understanding-the-dao-attack> consulté le 8 mars 2025

¹⁷⁹ Village de la Justice, « Résolution décentralisée des litiges : arbitrage, blockchain et smart contracts », Village de la Justice, 1er octobre 2024. Disponible en ligne : <https://www.village-justice.com/articles/resolution-decentralisee-des-litiges-arbitrage-blockchain-smart-contracts,50983.html> (consulté le 8 mars 2025)

¹⁸⁰ Werbach, K., The Blockchain and the New Architecture of Trust, MIT Press, 2018, p. 521-522 En ligne : http://www.btlj.org/data/articles2018/vol33/33_2/Werbach_Web.pdf

blockchain et aux cryptomonnaies dans cet État¹⁸¹. De l'autre côté, des pays adoptent une approche plus flexible, voire incitative, en se positionnant comme des refuges réglementaires pour attirer les projets innovants. Cette diversité crée une mosaïque législative où chaque juridiction tente de protéger ses intérêts, sans toujours prendre en compte la dimension transnationale de la technologie¹⁸².

Pour garantir une meilleure protection des droits humains comme le droit à la vie privée ou le droit à l'identité, beaucoup d'experts recommandent de dépasser le cadre étroitement national au profit d'une approche internationale, voire d'un traité multilatéral spécifique à la blockchain¹⁸³. Un tel accord pourrait fixer des normes communes : respect minimum de la vie privée, responsabilités partagées entre acteurs du réseau, principes de coopération judiciaire en cas de cybercriminalité ou de fraude. En outre, des organismes comme l'ONU, par l'intermédiaire du Haut-Commissariat pour les Réfugiés (HCR) ou le Programme Alimentaire Mondial (PAM), pourraient jouer un rôle pivot pour promouvoir ces standards dans les contextes humanitaires, où la blockchain sert déjà à distribuer l'aide ou à gérer des identités numériques¹⁸⁴.

Cependant, l'idée d'un traité international soulève elle-même des questions politiques. Tous les États ne partagent pas la même vision de la souveraineté ni de la protection des droits fondamentaux, et certains craignent de perdre une partie de leur pouvoir de régulation. De plus, les géants du numérique, dont certains investissent massivement dans la blockchain, exercent aussi une influence considérable sur les décisions législatives et pourraient chercher à orienter la

¹⁸¹ Département des services financiers de l'État de New York (NYDFS), BitLicense Regulatory Framework, 2015, En ligne : https://www.dfs.ny.gov/virtual_currency_businesses consulté le 9 mars 2025

¹⁸² Tapscott, D. et Tapscott, A., Blockchain Revolution, Portfolio Penguin, 2016, p. 146

¹⁸³ Primavera De Filippi, Morshed Mannan & Wessel Reijers, « Blockchain Technology and the Rule of Code: Regulation via Governance », The George Washington Law Review, vol. 92, n° 6, décembre 2024, p. 1236-1237. Disponible en ligne : <https://www.gwlr.org/wp-content/uploads/2024/12/92-Geo.-Wash.-L.-Rev.-1229.pdf> (consulté le 9 mars 2025)

¹⁸⁴ Programme Alimentaire Mondial (PAM), "Building Blocks: Harnessing Blockchain to Improve Humanitarian Assistance", WFP Official Website, 2020 En ligne : (<https://innovation.wfp.org/project/building-blocks>) consulté le 9 mars 2025

réglementation en leur faveur¹⁸⁵. Pour surmonter ces obstacles, plusieurs auteurs suggèrent une gouvernance “multi-acteurs” : rassembler au sein d’un même forum des représentants des États, des organisations internationales, des entreprises technologiques et de la société civile, à l’image de ce qui a été mis en place pour la gouvernance de l’Internet¹⁸⁶.

Cette approche collaborative permettrait non seulement de définir des règles communes, mais aussi d’anticiper les évolutions technologiques, de gérer les situations d’urgence comme les atteintes massives à la vie privée ou les attaques informatiques et de favoriser l’échange de bonnes pratiques. En somme, face à la globalisation du numérique, la souveraineté nationale gagnerait à être repensée sous la forme d’une souveraineté partagée ou coordonnée, capable de s’adapter à l’échelle internationale¹⁸⁷. L’enjeu majeur est donc de concilier le respect des droits humains, la sécurité juridique et l’innovation technologique, en élaborant un cadre clair, stable et universellement reconnu.

CHAPITRE 4 : SOLUTIONS EXISTANTES POUR LA BLOCKCHAIN ET LA PROTECTION DES DROITS HUMAINS

La recherche sur les technologies décentralisées n’en est plus à ses commencements, et plusieurs solutions opérationnelles ont déjà vu le jour pour concilier la blockchain avec la protection des droits fondamentaux. Qu’il s’agisse de projets humanitaires concrets ou de cadres réglementaires nationaux et internationaux, ces initiatives fournissent des points de repère utiles pour envisager une intégration plus large de la blockchain dans le respect des droits humains.

¹⁸⁵ Conseil constitutionnel, « Les dimensions internationales de la souveraineté numérique », Nouveaux Cahiers du Conseil constitutionnel. Disponible en ligne : <https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/les-dimensions-internationales-de-la-souverainete-numerique> (consulté le 9 mars 2025)

¹⁸⁶ Les dimensions internationales de la souveraineté numérique », Nouveaux Cahiers du Conseil constitutionnel. Disponible en ligne : <https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/les-dimensions-internationales-de-la-souverainete-numerique> (consulté le 9 mars 2025)

¹⁸⁷ Internet Society, « Explorer la souveraineté numérique et son impact sur l’Internet », Internet Society, 2022. Disponible en ligne : https://www.internetsociety.org/wp-content/uploads/2022/12/Digital_Sovereignty_FR.pdf (consulté le 9 mars 2025)

4.1 Initiatives techniques pour mieux protéger les données

Plusieurs solutions techniques ont émergé pour répondre aux défis que soulève la protection des droits humains au sein des systèmes blockchain. En effet, la nature immuable et décentralisée de ces registres implique de repenser les méthodes de stockage et de traitement des données sensibles, afin de garantir à la fois la transparence souhaitée et le respect des principes fondamentaux du droit, comme la vie privée ou le droit à l'oubli¹⁸⁸.

D'abord, certaines organisations et associations ont opté pour des blockchains dites hybrides, qui associent une partie publique et une partie privée afin de concilier transparence et confidentialité. La partie publique, accessible à tous, contient les éléments essentiels pour vérifier l'intégrité et l'authenticité des transactions ou des enregistrements, tandis que la partie privée, réservée à des utilisateurs autorisés, stocke les informations sensibles telles que des données médicales, financières ou identitaires¹⁸⁹. Cette approche assure une traçabilité globale, car n'importe qui peut vérifier l'existence et la validité d'une transaction, tout en maintenant un strict contrôle d'accès aux détails les plus confidentiels. Ainsi, l'information critique reste à l'abri des regards indiscrets, tout en permettant à la communauté d'auditer la validité du registre. En fin de compte, cette combinaison réduit les risques de violation de la vie privée, sans pour autant sacrifier la transparence nécessaire au bon fonctionnement d'un réseau décentralisé¹⁹⁰.

Ensuite, de nombreuses start-up et laboratoires de recherche s'orientent vers des systèmes de chiffrement sélectif et de solutions off-chain afin de résoudre les difficultés posées par l'immutabilité de la blockchain et le droit à l'effacement. Concrètement, l'idée est de n'inscrire dans le registre que des données minimales telles que des sommes de contrôle, des "hashs" ou des identifiants, tandis que les informations sensibles sont conservées dans une base de données séparée. Ainsi, lorsqu'un individu souhaite faire valoir son droit à l'oubli ou mettre à jour certaines informations, il lui suffit de modifier ou de supprimer ces données dans l'espace externe, sans avoir

¹⁸⁸ Werbach, K., *The Blockchain and the New Architecture of Trust*, MIT Press, 2018, p. 537. En ligne : http://www.btlj.org/data/articles2018/vol33/33_2/Werbach_Web.pdf

¹⁸⁹ Finck, M., *Blockchain Regulation and Governance in Europe*, Cambridge University Press, 2019, p. 53-55

¹⁹⁰ *Idem*.

à toucher au cœur de la chaîne, qui demeure intacte et cohérente. Cette méthode garantit donc un meilleur respect de la vie privée tout en conservant la robustesse et la traçabilité inhérentes au registre distribué¹⁹¹.

Enfin, l'utilisation de preuves à divulgation nulle (Zero-Knowledge Proofs, ZKP) représente une troisième voie particulièrement prometteuse pour la blockchain. Grâce à cette technologie, il est possible de prouver qu'une information est vraie comme l'authenticité d'un document ou l'éligibilité d'une personne à bénéficier d'une aide sans pour autant divulguer les données sous-jacentes¹⁹². Imaginons par exemple un réfugié qui doit justifier son statut pour recevoir un soutien humanitaire : à l'aide d'une preuve à divulgation nulle, il pourrait confirmer son droit à cette aide sans divulguer la totalité de ses informations personnelles. De cette manière, la blockchain préserve sa transparence et sa sécurité, tout en évitant de rendre publiques des données sensibles. Dans des contextes où la protection des droits humains est prioritaire, cette approche permet d'allier vérification et confidentialité, limitant ainsi les risques d'exploitation malveillante des informations ou de discrimination¹⁹³.

En somme, ces différentes approches blockchains hybrides, stockage hors chaîne et preuves à divulgation nulle, démontrent qu'il est possible de concilier l'immutabilité et la transparence d'un registre distribué avec la protection des droits humains. Elles offrent des outils concrets pour préserver la confidentialité, éviter la divulgation inutile de données sensibles et respecter des cadres juridiques comme le RGPD, en ne consignnant dans la chaîne que les informations strictement nécessaires à la validation collective. Dans le même temps, la possibilité de corriger ou de supprimer, hors chaîne, des données sensibles demeure ouverte, afin d'empêcher toute atteinte excessive à la vie privée. Toutefois, pour que ces innovations soient pleinement efficaces, elles doivent être intégrées à des cadres juridiques adaptés et placées sous la supervision d'autorités

¹⁹¹ Start in Blockchain, « Comment concilier blockchain et droit à l'oubli », Start in Blockchain. Disponible en ligne : <https://start-in-blockchain.fr/comment-concilier-blockchain-et-droit-a-loubli/> (consulté le 10 mars 2025)

¹⁹² Volet, « Preuves à Zéro Connaissance : Améliorer la Confidentialité de la Blockchain », Volet Blog, 3 septembre 2024. Disponible en ligne : <https://volet.com/fr/blog/post/preuves-a-zero-connaissance-ameliorer-la-confidentialite-de-la-blockchain-01j7ng5htxtyskdecyb9k39a7> (consulté le 10 mars 2025)

¹⁹³ *Idem*.

expérimentées. Une telle synergie entre technologie et réglementation est indispensable pour assurer la défense des droits fondamentaux tout en profitant des atouts de la blockchain.

4.2 Projets humanitaires et sociaux s'appuyant sur la blockchain

Les organisations humanitaires et sociales explorent de plus en plus la technologie blockchain pour mieux distribuer l'aide aux populations vulnérables, renforcer la traçabilité des ressources et protéger l'identité des bénéficiaires. Comme évoqué à la section 1.6, des initiatives telles que Building Blocks du Programme Alimentaire Mondial ou les projets d'identité numérique du Haut-Commissariat des Nations unies pour les réfugiés (HCR) illustrent déjà ce potentiel. D'autres projets, présentés ci-dessous, montrent que cette dynamique s'étend bien au-delà du seul secteur de l'identité et de l'aide alimentaire, pour toucher la santé, l'environnement et le financement caritatif.

Sur le plan financier, certaines organisations mondiales et partenariats public-privé utilisent la blockchain pour garantir la transparence des dons et suivre la destination exacte des sommes versées¹⁹⁴. Par exemple, en Ukraine, le HCR a récemment expérimenté la distribution de fonds par stablecoins, directement transférés sur des portefeuilles numériques sécurisés. Les bénéficiaires peuvent ainsi retirer de l'argent en espèces ou payer des commerçants locaux, sans dépendre de structures bancaires potentiellement défaillantes en zone de conflit. Cette approche accélère l'acheminement de l'aide financière et limite les risques de corruption, chaque transaction étant tracée de bout en bout¹⁹⁵.

Au-delà de la distribution de fonds, la blockchain s'avère aussi cruciale pour lutter contre la contrefaçon et assurer la traçabilité de l'aide logistique, notamment dans le secteur médical. Selon l'Organisation Mondiale de la Santé (OMS), entre 10 et 30 % des médicaments qui circulent dans les pays en développement sont des faux, affectant en priorité les communautés les plus

¹⁹⁴ UNHCR, « UNHCR launches pilot Cash-Based Intervention Using Blockchain Technology for Humanitarian Payments », UNHCR Ukraine, 15 décembre 2022. Disponible en ligne : <https://www.unhcr.org/ua/en/news/unhcr-launches-pilot-cash-based-intervention-using-blockchain-technology-humanitarian-payments> (consulté le 10 mars 2025)

¹⁹⁵ *Idem*.

vulnérables. Des start-up collaborent ainsi avec des agences humanitaires pour étiqueter et enregistrer chaque lot de médicaments sur un registre distribué, ce qui permet de réduire significativement les vols et la revente illégale¹⁹⁶. En Côte d'Ivoire, la jeune entreprise Meditect illustre bien ce potentiel : « 85 % des pharmacies de Côte d'Ivoire utilisent déjà notre technologie », affirme son cofondateur, Arnaud Pourredon. Concrètement, les laboratoires transmettent à Meditect un numéro de série pour chaque boîte de médicament, dont une fraction est convertie en “hash” inscrit sur la blockchain. Lorsque médecins, pharmaciens ou patients scannent ce code, ils introduisent simultanément dans le registre des informations telles que la date, l'heure et la localisation, créant ainsi une chaîne de traçabilité fiable et pratiquement inaltérable¹⁹⁷.

Cette innovation, qui s'appuie sur l'obligation pour les laboratoires d'intégrer un datamatrix unique à chaque emballage, contribue à protéger la santé des populations en garantissant l'authenticité des produits. Plus largement, la mise en œuvre de la blockchain dans le secteur médical ouvre des perspectives variées, de la sécurisation des données patients jusqu'à l'optimisation de la chaîne logistique humanitaire, en passant par la prévention de pertes humaines liées à la circulation de faux médicaments¹⁹⁸.

La blockchain révolutionne l'aide humanitaire en garantissant transparence, efficacité et confiance dans la gestion des dons et des projets sociaux. IBM, en partenariat avec Plastic Bank, a mis en place un système innovant où les déchets plastiques recyclés dans les pays en développement sont échangés contre des jetons numériques permettant d'acheter de la nourriture, de l'eau ou des crédits téléphoniques, alliant ainsi inclusion sociale et protection de l'environnement¹⁹⁹. Au-delà de cette initiative écologique, IBM collabore avec des ONG pour optimiser la traçabilité des fonds et renforcer la confiance des donateurs. En Espagne, la société a accompagné la start-up Comgo dans la création d'une plateforme blockchain permettant aux associations de suivre précisément

¹⁹⁶ Bpifrance, « Une blockchain pour lutter contre le trafic de faux médicaments en Afrique subsaharienne », Big Media Bpifrance, 19 octobre 2021. Disponible en ligne : <https://bigmedia.bpifrance.fr/news/une-blockchain-pour-lutter-contre-le-traffic-de-faux-medicaments-en-afrique-subsaharienne> (consulté le 10 mars 2025)

¹⁹⁷ *Idem*.

¹⁹⁸ *Idem*.

¹⁹⁹ Admical, « La Blockchain au Service de l'Humanitaire », Admical. Disponible en ligne : <https://admical.org/expertise/la-blockchain-au-service-de-lhumanitaire> (consulté le 10 mars 2025)

l'utilisation des dons, répondant ainsi à la méfiance persistante du public²⁰⁰. En Suède, IBM a développé un prototype pour le Fonds suédois du cancer de l'enfant, offrant aux donateurs la possibilité de suivre en temps réel l'affectation de leurs contributions aux projets de recherche. Ces innovations démontrent que la blockchain est un outil puissant pour améliorer l'impact des initiatives caritatives, diversifier les modes de dons et sécuriser les transactions. En ouvrant de nouvelles perspectives pour l'intérêt général, cette technologie maximise l'efficacité des transferts financiers et rend les actions humanitaires plus accessibles et efficaces à l'échelle mondiale²⁰¹.

En définitive, ces différents projets humanitaires et sociaux soulignent le fort potentiel de la blockchain pour améliorer l'efficacité et la fiabilité de l'aide, tout en protégeant mieux les droits fondamentaux des personnes concernées. Néanmoins, ils mettent aussi en évidence la nécessité d'une gouvernance adaptée et d'un cadre juridique clair : les réfugiés doivent pouvoir exercer leur droit à l'oubli ou à la rectification des données, et la reconnaissance internationale de l'identité numérique demeure un enjeu majeur. Dans l'ensemble, l'introduction de la blockchain dans les interventions humanitaires constitue un pas vers une aide plus rapide, plus traçable et plus respectueuse de la dignité des bénéficiaires.

4.3 Partenariats public-privé utilisant la blockchain dans l'aide humanitaire

Les partenariats entre le secteur public et le secteur privé représentent une autre approche efficace pour maximiser l'impact de la blockchain dans les contextes humanitaires et sociaux. Ces collaborations permettent d'allier les capacités technologiques avancées des entreprises privées à l'expertise opérationnelle des organisations publiques et des ONG. IBM, par exemple, en collaboration avec Plastic Bank, a mis en place un programme innovant où les déchets plastiques collectés dans les pays en développement sont échangés contre des jetons numériques basés sur la blockchain. Ces jetons permettent ensuite aux participants d'accéder à des ressources essentielles telles que la nourriture, l'eau potable ou encore des crédits téléphoniques. Cette initiative, en plus

²⁰⁰ *Idem.*

²⁰¹ *Idem.*

de résoudre des enjeux environnementaux, favorise l'inclusion économique des populations vulnérables grâce à la technologie blockchain²⁰².

En outre, IBM a également collaboré avec des organismes humanitaires afin de renforcer la transparence des dons et de rassurer les donateurs sur l'utilisation effective de leurs contributions. En Espagne, par exemple, la société technologique a soutenu la start-up Comgo dans la création d'une plateforme blockchain permettant un suivi précis des dons destinés aux associations caritatives. Ce dispositif répond à un besoin réel de transparence exprimé par les donateurs, qui souhaitent avoir la certitude que leurs fonds sont utilisés conformément à leurs intentions initiales²⁰³.

Par ailleurs, en Suède, IBM a développé un prototype pour le Fonds suédois du cancer de l'enfant, permettant aux donateurs de suivre précisément et en temps réel l'affectation de leurs dons aux différents projets de recherche médicale. Cette innovation accroît considérablement la confiance du public envers les institutions caritatives et humanitaires, en garantissant une utilisation transparente et traçable des ressources financières²⁰⁴.

Ces exemples montrent clairement que les partenariats public-privé basés sur la blockchain peuvent contribuer efficacement à renforcer la confiance et à optimiser la gestion des ressources humanitaires. Toutefois, le succès de ces initiatives dépend d'une régulation claire, d'une gouvernance transparente et d'un cadre juridique précis pour éviter tout conflit d'intérêts ou toute utilisation abusive des données personnelles des bénéficiaires.

²⁰² Tifenn André, « La Blockchain au service de l'humanitaire », Admical. Disponible en ligne : <https://admical.org/expertise/la-blockchain-au-service-de-lhumanitaire> (consulté le 22 mars 2025)

²⁰³ *Idem.*

²⁰⁴ *Idem.*

CONCLUSION

La présente recherche a étudié comment la technologie blockchain, grâce à sa décentralisation et à son caractère immuable, peut à la fois offrir d'importants avantages (sécurité des données, transactions transparentes, identité numérique pour des populations vulnérables) et soulever d'importants défis juridiques. Tout au long de ce travail, nous avons constaté que, même si la blockchain peut réellement aider à protéger les droits humains, son intégration dans les lois en vigueur demande de nombreux ajustements.

D'abord, la blockchain se heurte à la question du droit à l'oubli et de la protection des données personnelles, qui sont des règles essentielles en droit européen (RGPD) et dans bien d'autres systèmes. Le fait que la chaîne soit infalsifiable et permanente complique l'effacement ou la modification de données. Nous avons vu que certaines méthodes, comme le chiffrement sélectif, le stockage hors chaîne et les preuves à divulgation nulle, permettent de préserver la confidentialité tout en maintenant l'intégrité du registre. Néanmoins, il reste nécessaire d'adapter les textes législatifs pour concilier l'immutabilité de la blockchain avec le droit à la rectification et à la suppression des informations.

Ensuite, la responsabilité juridique dans un environnement décentralisé soulève des questions inédites : qui doit assumer la responsabilité en cas de violation des droits humains ou d'utilisation abusive de la blockchain ? Sans autorité centrale, il est difficile de déterminer qui peut être poursuivi en justice. Les propositions pour mettre en place une responsabilité partagée ou adaptée montrent qu'on peut réviser le droit classique de la responsabilité (contractuelle et délictuelle) si l'on définit clairement le rôle de chaque acteur (développeurs, plateformes, mineurs, utilisateurs). Sans cette clarification, la confiance dans la blockchain pourrait faiblir si les victimes n'obtiennent pas réparation lorsqu'un dommage survient.

Par ailleurs, la souveraineté numérique et la régulation internationale sont aussi des enjeux clés. Du fait de sa portée mondiale, la blockchain échappe en grande partie aux limites géographiques des États, ce qui rend plus complexe l'application uniforme de règles fondées sur la territorialité. Cette difficulté souligne l'importance d'une meilleure coopération entre pays et organismes

internationaux, afin d'harmoniser les approches législatives. C'est dans cet esprit que s'inscrivent des initiatives comme le règlement MiCA en Europe ou les « bacs à sable » réglementaires au Canada et aux États-Unis, qui cherchent à rassurer tant les investisseurs que les innovateurs, tout en préservant les droits fondamentaux.

D'un point de vue pratique, la blockchain se révèle particulièrement avantageuse dans les actions humanitaires. Les exemples du Programme Alimentaire Mondial (PAM) ou du Haut-Commissariat pour les Réfugiés (HCR) montrent clairement comment elle facilite la distribution d'aide alimentaire, financière ou médicale de manière plus efficace et plus transparente, tout en réduisant la fraude. Les contrats intelligents (smart contracts) et les partenariats public-privé prouvent également qu'il est possible de déclencher automatiquement des versements selon des conditions prédéfinies, d'assurer la traçabilité de l'aide et de respecter la dignité des bénéficiaires.

Toutefois, ces exemples démontrent aussi la nécessité d'une gouvernance adaptée. La technologie seule ne peut pas résoudre tous les problèmes de fond (fracture numérique, manque de reconnaissance légale, etc.). Les blockchains hybrides ou les solutions off-chain indiquent l'importance d'un dispositif à la fois éthique, juridique et technique, garantissant un usage responsable de la technologie. Sans un tel équilibre, les populations déjà fragiles risquent de subir de nouvelles discriminations, par exemple si elles ne peuvent accéder à l'infrastructure numérique requise.

Cette étude, même si elle est complète sur certains points, comporte inévitablement des limites. La vitesse d'évolution des technologies blockchain et la variété des lois nationales rendent toute conclusion définitive difficile. Des recherches plus poussées seraient utiles pour mesurer l'impact réel de la blockchain sur la réduction des coûts administratifs, la gestion des crises humanitaires ou la lutte contre la désinformation²⁰⁵. Elles pourraient aussi explorer comment l'intelligence artificielle, en complément de la blockchain, influence encore davantage la gouvernance numérique.

²⁰⁵ Maréchal, N. et Hanson, L., Blockchain Technology for Media: The Good, the Bad, and the Ugly, Centre for International Governance Innovation, 2020, p. 14

Enfin, il serait intéressant de s'interroger sur la place future des organisations autonomes décentralisées (DAO) et sur leur intégration possible dans le droit international.²⁰⁶ Si elles sont majoritairement régies par des règles auto-exécutées, il faudra s'assurer qu'elles respectent les principes fondamentaux du droit et puissent être soumises à un contrôle judiciaire. Malgré tout, l'expérience montre déjà que la blockchain, avec sa robustesse et sa transparence, peut devenir un soutien solide pour protéger et renforcer les droits humains, à condition d'être utilisée de manière prudente et encadrée par un droit flexible et moderne.

Il convient enfin de noter que la blockchain ne représente qu'une parmi plusieurs technologies émergentes qui transforment aujourd'hui la manière dont les droits humains sont protégés, ou menacés, dans l'environnement numérique. L'intelligence artificielle, notamment, soulève des questions de gouvernance et de responsabilité qui recoupent largement celles examinées dans ce travail : qui est responsable lorsqu'un système automatisé porte atteinte à un droit fondamental, et comment les cadres juridiques existants peuvent-ils s'adapter à des technologies qui évoluent plus vite que la régulation? La Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle, signée par le Canada en février 2025, témoigne de cette prise de conscience internationale, par analogie avec les réflexions menées pour la blockchain dans le cadre de ce mémoire²⁰⁷. Une recherche future pourrait ainsi approfondir les zones de convergence entre ces deux technologies sur le plan de la protection des droits humains.

²⁰⁶ De Filippi, P. et Wright, A., *Blockchain and the Law: The Rule of Code*, Harvard University Press, 2018, chap. 9.

²⁰⁷ Conseil de l'Europe, *Convention-cadre du Conseil de l'Europe sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit*, STCE n° 225, ouverte à la signature le 5 septembre 2024, signée par le Canada le 11 février 2025. Déjà citée, supra note 158.

BIBLIOGRAPHIE

Instruments juridiques internationaux et nationaux

Charte canadienne des droits et libertés, partie I de la Loi constitutionnelle de 1982, constituant l'annexe B de la Loi de 1982 sur le Canada (R-U), 1982, c 11.

Conseil de l'Europe, Convention-cadre sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'État de droit, STCE n° 225, ouverte à la signature le 5 septembre 2024, signée par le Canada le 11 février 2025.

Déclaration universelle des droits de l'homme, Rés AG 217 A (III), Doc off AG NU, 3^e sess, supp n° 13, Doc NU A/810 (1948).

Directive (UE) 2018/843 du Parlement européen et du Conseil du 30 mai 2018 sur la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme (5AMLD).

Pacte international relatif aux droits civils et politiques, 16 décembre 1966, 999 RTNU 171 (entré en vigueur le 23 mars 1976).

Pacte international relatif aux droits économiques, sociaux et culturels, 16 décembre 1966, 993 RTNU 3 (entré en vigueur le 3 janvier 1976).

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD), JO L 119, 4 mai 2016.

Règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés de crypto-actifs (MiCA), JO L 150, 9 juin 2023.

Ouvrages et monographies

Bonomi, A., Lehmann, M. et Lalani, S. (dir.). (2023). *Blockchain and Private International Law*. Leiden : Brill/Nijhoff.

De Filippi, P. et Wright, A. (2018). *Blockchain and the Law: The Rule of Code*. Harvard University Press.

Finck, M. (2019). *Blockchain Regulation and Governance in Europe*. Cambridge : Cambridge University Press.

Grinhaus, A. (2022). *A Practical Guide to Smart Contracts and Blockchain Law* (2^e éd.). Toronto : LexisNexis Canada.

Lehmann, M. (2025). *Crypto Economy and International Law: Determining the Regulatory and Private Law Rules Governing the Blockchain*. Leiden : Brill/Nijhoff.

- Lessig, L. (1999). *Code and Other Laws of Cyberspace*. Basic Books.
- Magnuson, W. J. (2020). *Blockchain Democracy: Technology, Law and the Rule of the Crowd*. Cambridge : Cambridge University Press.
- Martineau, J. et Durand Folco, J. (2023). *Le capital algorithmique : accumulation, pouvoir et résistance à l'ère de l'intelligence artificielle*. Montréal : Écosociété.
- Schmitt, M. N. (dir.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2^e éd.). Cambridge : Cambridge University Press.
- Szostek, D. (2019). *Blockchain and the Law* (1^{re} éd.). Baden-Baden : Nomos.
- Tapscott, D. et Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. Penguin.
- Werbach, K. (2018). *The Blockchain and the New Architecture of Trust*. MIT Press.

Articles scientifiques et juridiques

- Barraud, B. (2018). Les blockchains et le droit. *Revue Lamy Droit de l'immatériel*, (147), 1.
- Belen-Saglam, R. et al. (2022). A Systematic Literature Review of the Tension between the GDPR and Public Blockchain Systems. *arXiv preprint arXiv:2210.04541*.
- Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A. et Felten, E. W. (2015). Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. Dans *Proceedings of the IEEE Symposium on Security and Privacy* (p. 104-121).
- De Filippi, P. et Hassan, S. (2018). Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code. *First Monday*, 23(12).
- Finck, M. (2019). Blockchain and the General Data Protection Regulation: Can Distributed Ledgers be Squared with European Data Protection Law? *Journal of Data Protection & Privacy*, 2(1), 1-18.
- Godbout, A.-S. (2020). *Le droit à l'ère numérique : entre la régulation technique et la régulation juridique des actifs numériques au Canada*.
- G'ssell, F. et Martin-Bariteau, F. (2022). *L'impact des blockchains sur les droits de l'homme, la démocratie et l'État de droit*. Conseil de l'Europe. <https://ssrn.com/abstract=4170327>
- Kadji Ngassam, M. T., Babei, J. et Biloa, S. G. (2023). *Handbook of Research on Blockchain Technology and the Digitalization of the Supply Chain*.
- La difficile appréhension des blockchains par le droit. (2018). *Revue internationale de droit économique*, 2018/4, 453.

- Labbé, T. (2021). *Le droit face aux technologies disruptives : le cas de la blockchain* [Thèse de doctorat, Université de Strasbourg].
- Maréchal, N. et Hanson, L. (2020). *Blockchain Technology for Media: The Good, the Bad, and the Ugly*. Centre for International Governance Innovation.
- Mornet, A. (2021). *Y a-t-il un pilote dans la blockchain ? Réflexions sur l'identification d'un responsable de traitement dans le cadre de la blockchain*.
- Pastor Sempere, C. (2025). *The Legal Framework for New Digital Assets, Identities, and Data Spaces*.
- Poullet, Y. et Delforge, A. (2020). *Les blockchains : un défi et/ou un outil pour le RGPD ?*
- Poullet, Y. et Jacquemin, H. (2018). *Blockchain : une révolution pour le droit ?*
- Raskin, M. (2017). The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, 1, 304-307.
- Reidenberg, J. R. (1998). Lex Informatica: The Formulation of Information Policy Rules through Technology. *Texas Law Review*.
- Reijers, W. et Coeckelbergh, M. (2018). The Blockchain as a Narrative Technology: Investigating the Social Ontology and Normative Configurations of Cryptocurrencies. *Philosophy & Technology*.
- Savelyev, A. (2016). Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law. *Higher School of Economics Research Paper* No. WP BRP 71/LAW/2016.
- Sedlmeir, J., Buhl, H. U., Fridgen, G. et Keller, R. (2020). The Energy Consumption of Blockchain Technology: Beyond Myth. *Business & Information Systems Engineering*, 62(6), 599-608.
- Wright, A. et De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. *SSRN Electronic Journal*.
- Zwitter, A. et Boisse-Despiaux, M. (2018). Blockchain for Humanitarian Action and Development. *Journal of International Humanitarian Action*, 3(16), 1-7.
- Zyskind, G., Nathan, O. et Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. Dans *IEEE Security and Privacy Workshops* (p. 180-184). <https://homepage.cs.uiowa.edu/~ghosh/blockchain.pdf>

Articles en ligne et presse spécialisée

- André, T. (s.d.). *La blockchain au service de l'humanitaire*. Admical. <https://admical.org/expertise/la-blockchain-au-service-de-lhumanitaire>
- August Debouzy. (2021). *Les brevets blockchain : état des lieux et perspectives*. <https://www.august-debouzy.com/fr/blog/1249-les-brevets-blockchain-etat-des-lieux-et-perspectives>
- Biometric Update. (2024). *UNHCR embraces blockchain, zero-knowledge proofs to improve aid systems*. <https://www.biometricupdate.com/202401/unhcr-embraces-blockchain-zero-knowledge-proofs-to-improve-aid-systems>
- Blockchain and Higher Education Diplomas. (s.d.). <https://pmc.ncbi.nlm.nih.gov/articles/PMC8314335/>
- Bpifrance. (2021). *Une blockchain pour lutter contre le trafic de faux médicaments en Afrique subsaharienne*. Big Media Bpifrance.
- Cardano Foundation. (2023). *How Blockchain Can Help in the Refugee Crisis*. <https://www.cardanofoundation.org/blog/how-blockchain-can-help-in-the-refugee-crisis>
- CNIL. (s.d.). *Blockchain*. <https://www.cnil.fr/fr/definition/blockchain>
- Coin Center. (s.d.). *Principles for Crypto Legislation*. <https://www.coincenter.org/principles-legislation/>
- Commission européenne. (2023). *La Commission lance un bac à sable réglementaire européen pour la blockchain*. <https://digital-strategy.ec.europa.eu>
- Conseil constitutionnel. (2025). *Les dimensions internationales de la souveraineté numérique. Nouveaux Cahiers du Conseil constitutionnel*. <https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/les-dimensions-internationales-de-la-souverainete-numerique>
- Deffains, B. (s.d.). *Blockchain et justice décentralisée : un nouveau défi (Partie 2)*. LexTech Institute.
- Deloitte Avocats. (2022). *Blockchain, crypto-actifs et régulation : le point sur la situation en France en 2022*.
- El País. (s.d.). *Trump approuve deux décrets pour impulser les cryptomonnaies et l'intelligence artificielle*.
- IBM. (s.d.). *Qu'est-ce que la blockchain ?*. <https://www.ibm.com/fr-fr/topics/blockchain>
- Internet Society. (2022). *Explorer la souveraineté numérique et son impact sur l'Internet*. <https://www.internetsociety.org>

- Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique (France). (2025). *Blockchain : définition, avantages et applications*. <https://www.economie.gouv.fr>
- Start in Blockchain. (2025). *Comment concilier blockchain et droit à l'oubli*. <https://start-in-blockchain.fr/comment-concilier-blockchain-et-droit-a-loubli>
- Switzerland for UNHCR. (2022). *Blockchain for Refugees*. <https://unrefugees.ch/fr/blockchain-refugees>
- Technology Review. (2018). *Inside the Jordan refugee camp that runs on blockchain*. MIT Technology Review.
- The Blockchain Land. (2018). *Identités numériques : la blockchain au secours des réfugiés*. <https://theblockchainland.com/fr/2018/12/07/identites-numeriques-blockchain-refugies>
- Village de la Justice. (2019). *La blockchain face au droit : quels défis juridiques ?*
- Village de la Justice. (2024). *Résolution décentralisée des litiges : arbitrage, blockchain et smart contracts*.
- Volet. (2024). *Preuves à zéro connaissance : améliorer la confidentialité de la blockchain*. <https://volet.com/fr/blog/post/preuves-a-zero-connaissance>

Rapports et documents officiels

- Autorité des marchés financiers (AMF). (s.d.). *Le règlement européen Markets in Crypto-Assets (MiCA)*.
- Banque du Canada. (2017). *Les implications des technologies de la blockchain pour le système financier canadien*. Rapport sur la stabilité financière.
- CNIL. (2018). *Blockchain et RGPD : quelles solutions pour un usage responsable en présence de données personnelles*. Commission Nationale de l'Informatique et des Libertés.
- Gouvernement du Canada. (2024). *Règlement sur les actifs numériques et la blockchain*. Gazette du Canada, Partie I, vol. 158, n° 27.
- Office des Nations Unies contre la drogue et le crime (ONUDC). (s.d.). *Le crime international organisé et les cryptomonnaies*. Vienne : ONUDC.
- Organisation de coopération et de développement économiques (OCDE). (2026). *Crime organisé et corruption : perspectives de l'OCDE sur l'intégrité et la lutte contre la corruption 2026*. Paris : OCDE.
- Organisation des Nations Unies. (s.d.). *Blockchain Technology and Humanitarian Aid*.
- Programme Alimentaire Mondial (PAM). (2020). *Building Blocks: Harnessing Blockchain to Improve Humanitarian Assistance*. <https://innovation.wfp.org/project/building-blocks>

Skadden. (2025). *Crypto Regulation: Who Will Protect Consumers Against Fraud ?*

UNHCR. (2022). *UNHCR launches pilot Cash-Based Intervention Using Blockchain Technology for Humanitarian Payments.*