



Les défis juridiques de la technologie blockchain : chiffrement, horodatage et quête de reconnaissance normative

Legal Challenges of Blockchain Technology: Encryption, Timestamping and the Quest for Legal Recognition

El Imlahi Chair Houda

Doctorante à la FSJES Mohamed V- Agdal

Résumé

La technologie blockchain constitue une innovation disruptive dont l'ambition originelle est d'éliminer les tiers de confiance institutionnels au profit d'un registre distribué sécurisé par la cryptographie. Elle confère à ses enregistrements des propriétés d'immutabilité, de transparence et d'intégrité sans précédent. Ces caractéristiques techniques soulèvent des interrogations juridiques majeures, notamment quant à la reconnaissance de la signature numérique blockchain et de l'horodatage distribué dans les systèmes normatifs contemporains. Le présent article analyse ces défis selon une approche de droit comparé centrée sur le droit marocain et le droit français. L'étude démontre que la reconnaissance juridique effective des mécanismes cryptographiques de la blockchain se heurte à l'absence de certification par un prestataire de services de confiance qualifié, à la pseudonymisation des utilisateurs et à l'inadaptation des cadres normatifs existants à la logique décentralisée.

Mots-clés : blockchain, cryptographie asymétrique, signature électronique, horodatage, force probante, loi 43-20, droit comparé, registre distribué, preuve numérique.

Abstract

Blockchain technology is a disruptive innovation whose original ambition is to eliminate institutional trusted third parties in favor of a distributed ledger secured by cryptography. It endows its records with unprecedented properties of immutability, transparency and integrity. These technical characteristics raise major legal questions, particularly regarding the recognition of blockchain digital signatures and distributed timestamping within contemporary normative systems. This article analyses these challenges through a comparative law approach centered on Moroccan law and French law. The study demonstrates that the effective legal recognition of blockchain's cryptographic mechanisms is impeded by the absence of certification by a qualified trust service provider, the pseudonymization of users, and the inadequacy of existing normative frameworks to the decentralized logic of blockchain.

Keywords: blockchain, asymmetric cryptography, electronic signature, timestamping, probative value, Law 43-20, comparative law, distributed ledger, digital evidence.

Introduction

La technologie blockchain est une technologie disruptive qui se donne pour ambition de supprimer les tiers de confiance⁵⁶⁴. Elle permet donc l'enregistrement et le stockage des informations sans l'intervention d'un organe central (tiers de confiance habilité), grâce à des échanges pair à pair entre les nœuds, de manière sécurisée grâce à la cryptographie et leur structuration sous forme de blocs liés les uns aux autres par un chaînage cryptographique destiné à rendre immuable le stockage des données. C'est un registre distribué, c'est-à-dire stocké sur un grand nombre d'ordinateurs (des nœuds) et transparent au sens où son contenu est accessible à tout le monde.

Plus simplement, une blockchain constitue une base de données qui contient l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création. Cette base de données est sécurisée et

⁵⁶⁴ Primavera De Filippi & Aaron Wright, *Blockchain and the Law: The Rule of Code*, Harvard University Press, 2018.



distribuée : elle est partagée par ses différents utilisateurs, sans intermédiaire, ce qui permet à chacun de vérifier la validité de la chaîne⁵⁶⁵.

Les efforts de définition de la blockchain par plusieurs auteurs s'accordent à la présenter comme une technologie de stockage et de transmission d'informations dans laquelle il y a constitution de registres et leur distribution, sans organe de contrôle, de manière sécurisée⁵⁶⁶. Le Journal Officiel de la République Française a publié un avis de commission d'enrichissement de la langue française comportant la définition de la chaîne de blocs comme étant « *Mode d'enregistrement de données produites en continu, sous forme de blocs liés les uns aux autres dans l'ordre chronologique de leur validation, chacun des blocs et leur séquence étant protégés contre toute modification* »⁵⁶⁷. En d'autres termes, il s'agit d'une structure de données qui permet de créer un livre numérique de données (registre) et de le partager dans un réseau⁵⁶⁸. Ce réseau est constitué d'ordinateurs appelés des nœuds, qui vont alimenter le registre et valider les informations communiquées en les rendant immuables et en leur donnant date certaine, contre une rémunération.

Cette innovation technologique soulève des questions juridiques fondamentales, notamment concernant la valeur probante des enregistrements blockchain et la reconnaissance juridique des mécanismes cryptographiques qui en assurent la sécurité. Le chiffrement asymétrique et l'horodatage distribué, piliers techniques de la blockchain, interpellent directement les catégories classiques du droit de la preuve et du droit des obligations.

Le présent article se propose d'analyser ces défis selon un plan en deux parties. Dans une première partie, nous examinerons les fondements technico-juridiques de la blockchain, en explorant sa genèse philosophique et son architecture cryptographique. Dans une seconde partie, nous analyserons les défis juridiques spécifiques que posent le chiffrement et l'horodatage blockchain, notamment au regard du droit marocain et du droit comparé français.

PARTIE I : Les fondements technico-juridiques de la blockchain

A. Genèse philosophique et idéologique : du mouvement cypherpunk au libertarianisme numérique

Afin de comprendre un phénomène de société, il convient de se référer à la philosophie qui le fonde. La blockchain est la manifestation d'une philosophie libertarienne dont l'idéologie sous-jacente est une société libre et sans contrainte où le rôle de l'État est réduit au minimum.

Les prémices d'une *open source* ont vu le jour grâce au programmeur Richard Stallman qui pensa la notion de logiciel libre et ses possibilités pour les utilisateurs d'utiliser, d'étudier, d'améliorer, de modifier et de redistribuer un code informatique⁵⁶⁹.

Porté par cet esprit libertarien, un nouveau mouvement appelé *cypherpunks* voit le jour au début des années 90⁵⁷⁰. Ce mouvement est nourri par l'envie de préserver la vie privée (*privacy*) et l'anonymat à travers la cryptographie. Ils perçoivent l'anonymat comme un outil de protection des libertés individuelles⁵⁷¹. Ils sont favorables à l'usage de la cryptographie pour limiter les intrusions de l'État et des sociétés dans la vie privée des individus⁵⁷². Ce mouvement a mis en place deux manifestes pour défendre son idéologie, « *A Cypherpunk's Manifesto* »⁵⁷³ et « *The Crypto Anarchist Manifesto* ».

⁵⁶⁵ Ministère de l'Économie et des Finances (France), « La blockchain », disponible sur economie.gouv.fr.

⁵⁶⁶ Voir notamment : Gérard Haas & Clément Thibault, « Blockchain : définitions et enjeux », *Revue Banque*, n° 810, 2017 ; Dominique Legeais, *Blockchain et actifs numériques*, LexisNexis, 2019.

⁵⁶⁷ Journal Officiel de la République Française, Vocabulaire de l'informatique et de l'internet, avis du 23 mai 2017, JORF n°0121 du 23 mai 2017.

⁵⁶⁸ Don Tapscott & Alex Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, Penguin, 2016.

⁵⁶⁹ Richard Stallman, « The GNU Manifesto », 1985, disponible sur gnu.org.

⁵⁷⁰ Eric Hughes, « A Cypherpunk's Manifesto », 1993.

⁵⁷¹ Timothy C. May, « The Crypto Anarchist Manifesto », 1988.

⁵⁷² Steven Levy, *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age*, Viking, 2001.

⁵⁷³ Eric Hughes, « A Cypherpunk's Manifesto », 1993.



»574. La création de ce mouvement sera suivie par la déclaration d'indépendance du cyberspace « *Libertaria in Cyberspace* »575 en 1996, écrit par John Perry Barlow en réponse à l'adoption de la Loi sur les télécommunications de 1996576. Cette déclaration soutient l'idée qu'aucun gouvernement (ou qu'aucune autre forme de pouvoir) ne peut s'imposer et s'approprier Internet.

Sous l'influence de ces mouvements, plusieurs tentatives de monnaie numérique fondée sur le chiffrement et le hachage ont vu le jour mais ont été vouées à l'échec. L'objectif de ces technologies est de rendre inutile l'intervention d'un tiers de confiance. Parmi ces tentatives, on peut citer *B-money* de Wei Dai en 1998577, *Bit Gold* de Nick Szabo en 1998578, *Hashcash* d'Adam Back en 1997579, et *RPOW* (Reusable Proofs of Work) d'Hal Finney en 2004580.

C'est dans ce contexte idéologique et technique que Satoshi Nakamoto publie en 2008 le *white paper* intitulé « *Bitcoin: A Peer-to-Peer Electronic Cash System* »581, proposant une solution technique permettant de réaliser l'ambition cypherpunk d'un système monétaire décentralisé. Le Bitcoin, première application concrète de la technologie blockchain, incarne cette vision d'un système d'échange affranchi du contrôle étatique et des intermédiaires financiers traditionnels582.

Cette genèse philosophique éclaire les choix architecturaux de la blockchain : la décentralisation, la transparence cryptographique, l'immutabilité des enregistrements et l'autonomie des utilisateurs constituent autant de traductions techniques d'une idéologie libertarienne. Comprendre cette dimension idéologique est essentiel pour appréhender les tensions que la blockchain génère avec les systèmes juridiques fondés sur la centralisation de l'autorité et la médiation institutionnelle583.

B. Architecture cryptographique de la blockchain : chiffrement asymétrique, hachage et clés

La sécurité et la fiabilité de la blockchain reposent sur plusieurs mécanismes cryptographiques sophistiqués qui méritent une analyse détaillée, tant pour leur dimension technique que pour leurs implications juridiques.

1. Le chiffrement asymétrique et le système de clés publique/privée

Le chiffrement asymétrique, également appelé cryptographie à clé publique, constitue le fondement de l'identification et de l'authentification dans la blockchain584. Ce système repose sur l'utilisation de deux clés mathématiquement liées mais distinctes : une clé publique et une clé privée585.

La clé publique, comme son nom l'indique, est accessible à tous les utilisateurs du réseau. Elle sert d'identifiant et permet de recevoir des transactions. Elle peut être comparée à un numéro de compte bancaire que l'on peut communiquer librement586. La clé privée, en revanche, doit rester strictement confidentielle. Elle permet à son détenteur de signer numériquement les transactions et de prouver ainsi qu'il est bien le propriétaire légitime des actifs associés à la clé publique correspondante587.

Le principe cryptographique sous-jacent repose sur des fonctions mathématiques à sens unique : il est facile de calculer la clé publique à partir de la clé privée, mais pratiquement impossible de retrouver

574 Timothy C. May, « The Crypto Anarchist Manifesto », 1988.

575 John Perry Barlow, « A Declaration of the Independence of Cyberspace », 1996.

576 Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996).

577 Wei Dai, « b-money », 1998, disponible sur weidai.com.

578 Nick Szabo, « Bit Gold », 1998 (publié en 2005).

579 Adam Back, « Hashcash - A Denial of Service Counter-Measure », 1997.

580 Hal Finney, « RPOW - Reusable Proofs of Work », 2004.

581 Satoshi Nakamoto, « Bitcoin: A Peer-to-Peer Electronic Cash System », 2008.

582 Arvind Narayanan et al., *Bitcoin and Cryptocurrency Technologies*, Princeton University Press, 2016.

583 Primavera De Filippi, « Bitcoin: A Regulatory Nightmare to a Libertarian Dream », *Internet Policy Review*, vol. 3, n° 2, 2014.

584 Whitfield Diffie & Martin Hellman, « New Directions in Cryptography », *IEEE Transactions on Information Theory*, vol. 22, n° 6, 1976, p. 644-654.

585 Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed., Wiley, 1996.

586 Andreas M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, O'Reilly Media, 2014.

587 Idem.



la clé privée à partir de la clé publique⁵⁸⁸. Cette asymétrie garantit la sécurité du système : même si la clé publique est largement diffusée, personne ne peut usurper l'identité de l'utilisateur sans posséder sa clé privée⁵⁸⁹.

Le processus de signature numérique fonctionne de la manière suivante : lorsqu'un utilisateur souhaite effectuer une transaction, il utilise sa clé privée pour créer une signature numérique unique pour cette transaction spécifique⁵⁹⁰. Les autres participants du réseau peuvent ensuite vérifier l'authenticité de cette signature en utilisant la clé publique de l'émetteur, sans jamais avoir accès à sa clé privée⁵⁹¹.

La clé privée est créée par l'utilisateur à travers une suite aléatoire de chiffres⁵⁹². Sa perte entraîne l'impossibilité définitive d'accéder aux actifs qui lui sont associés, ce qui soulève des questions juridiques importantes en matière de succession et de recouvrement d'actifs⁵⁹³. Cette caractéristique technique illustre le principe « *not your keys, not your coins* » qui régit l'écosystème blockchain.

Du point de vue juridique, ce mécanisme de signature par clé privée présente des similitudes avec la signature manuscrite traditionnelle : il permet d'identifier l'auteur d'un acte et de manifester son consentement⁵⁹⁴. Toutefois, sa nature purement numérique et décentralisée pose des défis spécifiques quant à sa reconnaissance par les systèmes juridiques nationaux, comme nous le verrons dans la seconde partie⁵⁹⁵.

2. Le hachage cryptographique et l'intégrité des données

Le hachage cryptographique constitue le second pilier technique de la blockchain. Une fonction de hachage est un algorithme mathématique qui transforme n'importe quelle donnée d'entrée (texte, fichier, transaction) en une empreinte numérique de taille fixe, appelée *hash* ou condensat⁵⁹⁶.

Les fonctions de hachage utilisées dans la blockchain (notamment SHA-256 pour Bitcoin) présentent plusieurs propriétés essentielles. Premièrement, elles sont déterministes : une même donnée produira toujours le même *hash*⁵⁹⁷. À partir de chaque document ou fichier numérique, on obtient un *hash* unique, matérialisé par une suite alphanumérique de caractères, et le moindre changement (une virgule d'un texte, un pixel d'une image) suffit à produire un *hash* entièrement différent⁵⁹⁸.

Deuxièmement, elles sont à sens unique : il est impossible de retrouver la donnée originale à partir de son *hash*⁵⁹⁹. Troisièmement, elles présentent l'effet avalanche : la moindre modification de la donnée d'entrée produit un *hash* complètement différent. Enfin, elles sont résistantes aux collisions : il est pratiquement impossible de trouver deux données différentes produisant le même *hash*.

Dans la blockchain, chaque bloc contient le *hash* du bloc précédent, créant ainsi une chaîne cryptographique. Cette architecture garantit l'immuabilité des enregistrements : toute tentative de modification d'un bloc ancien invaliderait automatiquement tous les blocs suivants, rendant la fraude détectable par l'ensemble du réseau. Le hachage assure ainsi l'intégrité historique de la chaîne et permet à chaque participant de vérifier que les données n'ont pas été altérées.

⁵⁸⁸ Jonathan Katz & Yehuda Lindell, *Introduction to Modern Cryptography*, 2nd ed., CRC Press, 2014. https://eclass.uniwa.gr/modules/document/file.php/CSCYB105/Reading%20Material/%5BJonathan_Katz%2C_Yehuda_Lindell%5D_Introduction_to_Modern%20Cryptography.pdf

⁵⁸⁹ Idem.

⁵⁹⁰ Idem.

⁵⁹¹ « LES ENJEUX TECHNOLOGIQUES DES BLOCKCHAINS (CHAÎNES DE BLOCS) », Rapport de l'Office parlementaire d'évaluation des choix scientifiques et technologiques (France), n° 584, 2018, p. 17.

⁵⁹² Dominique Legeais « Blockchain et actifs numériques », LexisNexis, deuxième édition 2019, p. 21.

⁵⁹³ Idem.

⁵⁹⁴ Laurent Assaya & Vincent Baudouin, « La signature électronique par cryptographie à clé publique », *La Semaine Juridique Entreprise et Affaires*, n° 4, 23 janvier 2003, 146.

⁵⁹⁵ JurisClasseur Droit bancaire et financier, Fasc. 179 : Blockchain.

⁵⁹⁶ « LES ENJEUX TECHNOLOGIQUES DES BLOCKCHAINS (CHAÎNES DE BLOCS) », op. cit., p. 17.

⁵⁹⁷ Claire LEVENEUR « LES SMART CONTRACTS ÉTUDE DE DROIT DES CONTRATS À L'AUNE DE LA BLOCKCHAIN » Thèse de doctorat en droit soutenue le 2 décembre 2022 ; Université Paris-Panthéon-Assas ; p. 60.

⁵⁹⁸ « Blockchain et actifs numériques », op. cit., p. 22

⁵⁹⁹ Idem.



Cette propriété d'immutabilité présente un intérêt juridique majeur pour la constitution de preuves et l'établissement de dates certaines, comme nous l'analyserons dans la seconde partie de cette étude.

C. Réseau pair-à-pair et mécanismes de consensus distribué

Au-delà de la cryptographie, l'architecture de la blockchain repose sur deux autres composantes essentielles : le réseau pair-à-pair et les mécanismes de consensus.

1. Le réseau pair-à-pair (P2P)

Un réseau pair-à-pair (*peer-to-peer* ou P2P) est une architecture de réseau informatique dans laquelle chaque ordinateur (appelé nœud) peut agir simultanément comme client et comme serveur⁶⁰⁰. Contrairement aux architectures client-serveur traditionnelles où un serveur central contrôle et distribue les informations, dans un réseau P2P, tous les nœuds sont égaux et peuvent échanger directement entre eux⁶⁰¹.

Dans le contexte de la blockchain, cette architecture P2P signifie que chaque nœud du réseau possède une copie complète du registre et participe à la validation des transactions⁶⁰². Lorsqu'une nouvelle transaction est émise, elle est diffusée à l'ensemble des nœuds du réseau qui vont la vérifier et la valider collectivement⁶⁰³. Cette décentralisation élimine le besoin d'un tiers de confiance central et rend le système résilient : la défaillance ou la compromission d'un nœud n'affecte pas le fonctionnement global du réseau.

Le processus de validation d'une transaction dans un réseau blockchain P2P suit généralement les étapes suivantes⁶⁰⁴ : d'abord, un utilisateur initie une transaction en la signant avec sa clé privée ; ensuite, cette transaction est diffusée à l'ensemble des nœuds du réseau ; puis, les nœuds vérifient la validité de la transaction (signature, disponibilité des fonds, respect des règles du protocole) ; enfin, les transactions validées sont regroupées dans un nouveau bloc qui sera ajouté à la chaîne selon le mécanisme de consensus en vigueur.

2. Les mécanismes de consensus

Le consensus est le processus par lequel les nœuds du réseau se mettent d'accord sur l'état actuel du registre et sur les transactions à inclure dans le prochain bloc⁶⁰⁵. Ce mécanisme est crucial car il permet de résoudre le problème de la double dépense sans recourir à une autorité centrale.

Plusieurs mécanismes de consensus existent, chacun présentant des avantages et des inconvénients spécifiques⁶⁰⁶.

Le *Proof of Work* (PoW), utilisé notamment par Bitcoin, repose sur la résolution de problèmes cryptographiques complexes. Les nœuds appelés « mineurs » entrent en compétition pour résoudre ces problèmes, et le premier qui y parvient obtient le droit d'ajouter le nouveau bloc à la chaîne et reçoit une récompense. Ce mécanisme garantit une sécurité élevée mais consomme énormément d'énergie.

Le *Proof of Stake* (PoS) sélectionne le validateur du prochain bloc en fonction de la quantité de cryptomonnaie qu'il détient et qu'il accepte de « mettre en jeu » (*stake*). Ce mécanisme est beaucoup moins énergivore que le PoW mais soulève des questions quant à la centralisation potentielle du pouvoir entre les mains des détenteurs les plus importants.

D'autres mécanismes existent, tels que le *Delegated Proof of Stake* (DPoS), le *Proof of Authority* (PoA), ou encore le *Practical Byzantine Fault Tolerance* (PBFT), chacun adapté à des contextes d'usage spécifiques (blockchains publiques, privées ou consortiales).

Du point de vue juridique, le choix du mécanisme de consensus n'est pas neutre. Il détermine le degré de décentralisation effective du réseau, la répartition du pouvoir de validation, et par conséquent la

⁶⁰⁰ <https://www.spiceworks.com/tech/networking/articles/what-is-peer-to-peer/>

⁶⁰¹ <https://www.geeksforgeeks.org/computer-networks/what-is-p2p-peer-to-peer-process/>

⁶⁰² <https://brave.com/fr/glossary/peer-to-peer/>

⁶⁰³ Idem.

⁶⁰⁴ Ces éléments de déroulement sont tirés de l'ouvrage : « Blockchain et actifs numériques », op. cit.

⁶⁰⁵ « LES ENJEUX TECHNOLOGIQUES DES BLOCKCHAINS (CHAÎNES DE BLOCS) », op. cit., p. 27.

⁶⁰⁶ Dominique Legeais, *Blockchain et actifs numériques*, op. cit., p. 20.



question de la responsabilité en cas de dysfonctionnement ou de litige. Dans une blockchain publique utilisant le PoW, il est pratiquement impossible d'identifier un responsable unique, ce qui pose des défis considérables pour l'application des règles de responsabilité civile traditionnelles⁶⁰⁷.

PARTIE II : Les défis juridiques du chiffrement et de l'horodatage blockchain

A. La valeur juridique de la signature électronique blockchain

La signature numérique par clé privée, mécanisme central de la blockchain, soulève la question fondamentale de sa reconnaissance juridique en tant que signature électronique au sens des législations nationales. Cette reconnaissance conditionne la validité juridique des transactions et des contrats conclus via la blockchain.

1. Le cadre juridique marocain : la loi 43-20 relative aux services de confiance pour les transactions électroniques

Le législateur marocain a adopté la loi n° 43-20 relative aux services de confiance pour les transactions électroniques, qui transpose en droit marocain les standards internationaux en matière de signature électronique. Cette loi s'inscrit dans la continuité du Dahir des Obligations et Contrats (DOC) qui, dans ses articles 418 et 419, reconnaît la validité de l'écrit électronique et de la signature électronique⁶⁰⁸⁶⁰⁹.

L'article 2 de la loi 43-20 définit la signature électronique comme « *une donnée sous forme électronique, qui est jointe ou associée logiquement à d'autres données électroniques et qui sert de méthode d'authentification* »⁶¹⁰. Cette définition large permet, en principe, d'englober la signature par clé privée utilisée dans la blockchain.

Pour qu'une signature électronique ait la même valeur juridique qu'une signature manuscrite, la loi 43-20 pose plusieurs conditions cumulatives. L'article 45 de la loi 43-20 dispose que la signature électronique doit permettre d'identifier le signataire et de garantir son lien avec l'acte auquel elle s'attache⁶¹¹. Plus précisément, selon l'article 7 de la loi 43-20, la signature électronique doit remplir les conditions suivantes : être propre au signataire, être créée par des moyens que le signataire puisse garder sous son contrôle exclusif, et garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable⁶¹².

La signature blockchain par clé privée répond formellement à ces exigences. La clé privée est propre à son détenteur et demeure sous son contrôle exclusif. Le mécanisme de hachage garantit qu'aucune modification de la transaction signée ne peut passer inaperçue. Enfin, la signature permet d'identifier le signataire par sa clé publique associée.

Toutefois, la loi 43-20 introduit une distinction entre signature électronique simple et signature électronique qualifiée. L'article 5 de la loi 43-20 définit la signature électronique qualifiée comme une signature électronique avancée créée par un dispositif de création de signature électronique qualifié et fondée sur un certificat qualifié⁶¹³. Seule cette signature qualifiée bénéficie d'une présomption de fiabilité et d'une équivalence totale avec la signature manuscrite.

Or, la signature blockchain ne repose généralement pas sur un certificat qualifié délivré par un prestataire de services de confiance agréé, comme l'exige la loi marocaine. Au Maroc, Barid Al-Maghrib propose un service de signature électronique qualifiée (*BaridiSign*)⁶¹⁴, mais ce service n'est pas intégré nativement aux protocoles blockchain. Cette absence de certification qualifiée fragilise la reconnaissance juridique de la signature blockchain en droit marocain, même si elle répond aux exigences techniques de sécurité et d'authentification.

⁶⁰⁷ Dominique Legeais, *Blockchain et actifs numériques*, op. cit., p. 24.

⁶⁰⁸ Article 418 du Dahir des Obligations et Contrats (DOC) marocain.

⁶⁰⁹ Article 419 du DOC.

⁶¹⁰ Article 2 de la loi 43-20.

⁶¹¹ Article 45 de la loi 43-20 relative aux services de confiance pour les transactions électroniques.

⁶¹² Article 7 de la loi 43-20.

⁶¹³ Article 5 de la loi 43-20.

⁶¹⁴ <https://www.baridesign.ma/wps/portal/barideSign>



2. Le droit comparé français et l'évolution législative

Le droit français présente une évolution intéressante quant à la reconnaissance de la blockchain. L'ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse a introduit dans le droit français la notion de « dispositif d'enregistrement électronique partagé », première reconnaissance législative de la technologie blockchain⁶¹⁵.

Plus significativement, l'ordonnance n° 2017-1674 du 8 décembre 2017 a modifié le Code monétaire et financier pour permettre la représentation et la transmission de certains titres financiers au moyen d'un dispositif d'enregistrement électronique partagé. Les articles L.211-3 et suivants du Code monétaire et financier reconnaissent désormais explicitement la blockchain comme support juridique valide pour certains instruments financiers⁶¹⁷.

Concernant la signature électronique, le droit français, harmonisé avec le règlement européen eIDAS (règlement UE n° 910/2014), distingue également entre signature électronique simple, avancée et qualifiée. La signature blockchain, bien que techniquement robuste, ne bénéficie pas automatiquement du statut de signature qualifiée faute de certification par un prestataire de services de confiance qualifié.

Néanmoins, la jurisprudence française tend à reconnaître la validité de signatures électroniques non qualifiées dès lors qu'elles remplissent les conditions fonctionnelles d'identification du signataire et d'intégrité du document⁶¹⁸. Cette approche pragmatique pourrait ouvrir la voie à une reconnaissance judiciaire de la signature blockchain, même en l'absence de certification formelle.

3. Les défis de l'intégration juridique

Plusieurs obstacles demeurent à l'intégration pleine et entière de la signature blockchain dans les systèmes juridiques nationaux.

Premièrement, la question de l'identification du signataire pose problème. Dans la blockchain publique, les utilisateurs sont identifiés par leurs clés publiques, qui sont des suites alphanumériques pseudonymes. Cette pseudonymisation, héritée de l'idéologie cypherpunk, entre en tension avec les exigences juridiques d'identification nominative des parties à un acte juridique⁶¹⁹.

Deuxièmement, l'absence d'infrastructure de certification qualifiée intégrée à la blockchain limite la reconnaissance juridique des signatures. Pour qu'une signature blockchain soit qualifiée au sens de la loi 43-20 ou du règlement eIDAS, il faudrait développer des ponts entre les prestataires de services de confiance agréés et les protocoles blockchain, ce qui soulève des défis techniques et organisationnels considérables⁶²⁰.

Troisièmement, la question de la révocation des certificats et de la gestion des clés compromises reste problématique. Dans les systèmes de signature électronique traditionnels, un certificat peut être révoqué par l'autorité de certification en cas de compromission. Dans la blockchain, la perte ou le vol d'une clé privée ne peut être « annulé » : les transactions signées avec cette clé restent valides sur la chaîne⁶²¹.

Enfin, la dimension transfrontalière de la blockchain pose des questions de droit international privé. Quelle loi nationale s'applique à une transaction blockchain impliquant des parties situées dans différents pays ? Quel tribunal est compétent en cas de litige ? Ces questions, classiques en droit du

⁶¹⁵ Ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse.

⁶¹⁶ Patrick barban, *l'écrit électronique et la blockchain : formalisme et preuve du consentement* in *Structures et usages de la blockchain*, Lefebvre Dalloz, 2024, p : 85 et suiv.

⁶¹⁷ Article L.211-3 du Code monétaire et financier français.

⁶¹⁸ Alice Barbet-Massin. *Le droit de la preuve à l'aune de la blockchain*. Droit. Université de Lille, 2020, p. 80.

⁶¹⁹ Voir à cet égard : Corine Namont Dauchez & Lucie Cluzel-Métayer, « Registres publics vs blockchain publique », in *L'État et le notariat face à la révolution blockchain*, *Revue du droit public et de la science politique en France et à l'étranger*, 2022, n° 1, p. 101. Et Mustapha Mekki, « Le juge et la blockchain : l'art de faire du nouveau vin dans de vieilles outres », p. 18

⁶²⁰ Idem.

⁶²¹ Cité in : « Blockchain et actifs numériques », op. cit., p. 79.



commerce international, prennent une acuité particulière dans un système décentralisé et sans ancrage territorial clair⁶²².

Malgré ces défis, des évolutions sont possibles. Certains auteurs proposent de développer des « oracles juridiques » qui feraient le lien entre les identités blockchain et les identités juridiques réelles, permettant ainsi de concilier pseudonymisation technique et identification juridique⁶²³. D'autres suggèrent de créer des blockchains privées ou consortiales dans lesquelles l'identification des participants serait assurée en amont, facilitant ainsi la reconnaissance juridique des signatures⁶²⁴.

B. La force probante de l'horodatage distribué

Au-delà de la signature électronique, la blockchain présente un intérêt majeur pour l'horodatage, c'est-à-dire l'attribution d'une date certaine à un événement ou à un document. Cette fonction d'horodatage, inhérente au mécanisme de chaînage des blocs, soulève des questions juridiques spécifiques quant à sa reconnaissance comme mode de preuve.

1. Les fondements techniques de l'horodatage blockchain

L'horodatage dans la blockchain repose sur le mécanisme de consensus et le chaînage cryptographique des blocs. Lorsqu'une transaction est incluse dans un bloc validé, elle reçoit un horodatage correspondant au moment de la validation de ce bloc⁶²⁵. Cet horodatage présente plusieurs caractéristiques remarquables.

Premièrement, il est décentralisé : aucune autorité centrale ne délivre l'horodatage, celui-ci résulte du consensus entre les nœuds du réseau. Deuxièmement, il est immuable : une fois qu'un bloc est ajouté à la chaîne, il devient pratiquement impossible de modifier rétroactivement son horodatage sans invalider tous les blocs suivants. Troisièmement, il est vérifiable : n'importe quel participant peut vérifier l'horodatage d'une transaction en consultant la blockchain publique.

Cette architecture confère à l'horodatage blockchain une robustesse technique supérieure à celle des systèmes d'horodatage centralisés traditionnels, qui reposent sur la confiance accordée à un tiers horodateur⁶²⁶. Dans la blockchain, la confiance est distribuée et repose sur des mécanismes cryptographiques et mathématiques plutôt que sur une autorité institutionnelle.

2. Le cadre juridique de l'horodatage au Maroc

Le droit marocain reconnaît l'importance de la date certaine dans de nombreux domaines juridiques. L'article 424 du DOC dispose que « *les actes sous seing privé n'ont de date certaine contre les tiers que du jour où ils ont été enregistrés, du jour de la mort de l'une des parties ou de celui où leur substance est constatée dans des actes dressés par des officiers publics* »⁶²⁷. Cette disposition illustre le principe selon lequel la date d'un acte sous seing privé n'est opposable aux tiers que si elle est établie par un moyen fiable et vérifiable.

La loi 43-20 relative aux services de confiance pour les transactions électroniques consacre un chapitre entier aux services d'horodatage électronique. L'article 23 de la loi 43-20 définit l'horodatage électronique comme « *une donnée sous forme électronique qui lie d'autres données sous forme électronique à un instant particulier et qui établit la preuve que ces dernières données existaient à cet instant* »⁶²⁸.

L'article 25 de la loi 43-20 précise les conditions de validité de l'horodatage électronique qualifié : il doit lier la date et l'heure aux données de manière à exclure raisonnablement la possibilité d'une modification indétectable des données ; il doit être fondé sur une source de temps liée au temps

⁶²² <https://www.assemblee-nationale.fr/14/amendements/3785/AN/227.asp>

⁶²³ Yang, X., et al., « Enhancing the Regulatory Framework around Electronic Signatures through the Integration of Blockchain Technology », 2023, DOI: 10.1145/3651655.3651661.

⁶²⁴ Voir infra.

⁶²⁵ Ces éléments de déroulement sont tirés de l'ouvrage : « Blockchain et actifs numériques », op. cit.

⁶²⁶ « LES ENJEUX TECHNOLOGIQUES DES BLOCKCHAINS (CHAÎNES DE BLOCS) », op. cit., p. 27.

⁶²⁷ Article 424 du DOC.

⁶²⁸ Article 23 de la loi 43-20.



universel coordonné ; et il doit être signé au moyen d'une signature électronique avancée ou scellé au moyen d'un cachet électronique avancé du prestataire de services de confiance qualifié⁶²⁹.

La question se pose donc de savoir si l'horodatage blockchain répond à ces exigences légales. Sur le plan technique, l'horodatage blockchain exclut effectivement toute modification indétectable des données grâce au mécanisme de hachage et de chaînage cryptographique. En revanche, deux difficultés apparaissent.

D'une part, l'horodatage blockchain n'est pas nécessairement lié au temps universel coordonné de manière certifiée. Les horloges des nœuds du réseau peuvent présenter des décalages, et l'horodatage d'un bloc correspond au moment où le consensus est atteint, qui peut différer légèrement du moment réel de la transaction⁶³⁰.

D'autre part, l'horodatage blockchain n'est pas signé par un prestataire de services de confiance qualifié au sens de la loi 43-20. Il résulte d'un processus décentralisé impliquant une multitude de nœuds anonymes ou pseudonymes. Cette absence de tiers certificateur agréé constitue un obstacle majeur à la reconnaissance de l'horodatage blockchain comme horodatage qualifié en droit marocain⁶³¹.

3. Perspectives d'évolution et solutions hybrides

Face à ces difficultés, plusieurs pistes d'évolution peuvent être envisagées. Une première approche consiste à développer des services d'horodatage hybrides, combinant la robustesse technique de la blockchain avec la certification juridique d'un prestataire de services de confiance agréé. Dans ce modèle, un prestataire qualifié pourrait ancrer périodiquement des *hashs* de documents dans une blockchain publique, créant ainsi un pont entre le système décentralisé et le cadre juridique existant⁶³².

Une deuxième approche consisterait à faire évoluer la législation pour reconnaître explicitement l'horodatage blockchain comme mode de preuve valide, à l'instar de ce que le législateur français a commencé à faire pour certains instruments financiers. Cette reconnaissance législative pourrait s'accompagner de conditions spécifiques (par exemple, exiger que la blockchain utilisée soit publique et suffisamment décentralisée pour garantir la fiabilité de l'horodatage)⁶³³.

Une troisième approche, plus pragmatique, repose sur l'appréciation judiciaire au cas par cas. Même en l'absence de reconnaissance législative explicite, les juges pourraient admettre l'horodatage blockchain comme élément de preuve dans le cadre du principe de liberté de la preuve qui prévaut en matière commerciale. Cette approche nécessiterait toutefois une expertise technique des magistrats et une évolution des pratiques judiciaires⁶³⁴.

C. L'admissibilité des enregistrements blockchain comme preuve en justice

Au-delà des questions spécifiques de signature et d'horodatage, se pose la question plus générale de l'admissibilité des enregistrements blockchain comme mode de preuve devant les juridictions marocaines et françaises.

1. Le principe de liberté de la preuve et ses limites

En droit marocain, comme en droit français, le régime de la preuve varie selon la nature de l'acte juridique. En matière civile, pour les actes juridiques d'une valeur supérieure à un certain seuil, la preuve par écrit est en principe exigée (article 443 du DOC marocain). En matière commerciale, en revanche, le principe de liberté de la preuve prévaut : tous les modes de preuve sont admissibles, y compris les présomptions, les témoignages et les écrits sous seing privé⁶³⁵.

⁶²⁹ Article 25 de la loi 43-20.

⁶³⁰ Alice Barbet-Massin, *Le droit de la preuve à l'aune de la blockchain*, op. cit., p. 187.

⁶³¹ Idem.

⁶³² Idem.

⁶³³ Idem, p. 189.

⁶³⁴ Emmanuel Netter, *Numérique et grandes notions de droit privé*, Cepsisca, collection Essais, 2017, p. 59.

⁶³⁵ « Blockchain et actifs numériques », op. cit., p. 73.



Cette distinction est fondamentale pour l'admissibilité des enregistrements blockchain. Dans les relations commerciales, un enregistrement blockchain pourrait être produit comme élément de preuve sans difficulté majeure, sous réserve que le juge l'estime suffisamment fiable et pertinent. Dans les relations civiles, en revanche, l'exigence d'un écrit signé pourrait constituer un obstacle, sauf si la signature blockchain est reconnue comme équivalente à une signature manuscrite⁶³⁶.

2. La question de la fiabilité et de l'authenticité

Pour qu'un enregistrement blockchain soit admis comme preuve, le juge doit être convaincu de sa fiabilité et de son authenticité. Plusieurs éléments plaident en faveur de cette fiabilité.

Premièrement, l'immutabilité technique de la blockchain garantit que les données enregistrées n'ont pas été modifiées a posteriori. Le mécanisme de hachage et de chaînage cryptographique rend toute altération détectable⁶³⁷.

Deuxièmement, la décentralisation du réseau rend pratiquement impossible une falsification coordonnée. Pour modifier rétroactivement un enregistrement dans une blockchain publique comme Bitcoin ou Ethereum, il faudrait contrôler plus de 50 % de la puissance de calcul du réseau, ce qui représente un coût prohibitif⁶³⁸.

Troisièmement, la transparence de la blockchain permet à toute partie intéressée de vérifier l'existence et le contenu d'un enregistrement. Cette vérifiabilité publique renforce la crédibilité de la preuve⁶³⁹. Néanmoins, plusieurs limites doivent être soulignées. D'abord, la fiabilité de l'enregistrement blockchain dépend de la fiabilité des données initiales. Si une information erronée ou frauduleuse est enregistrée dans la blockchain, celle-ci conservera fidèlement cette erreur ou cette fraude. La blockchain garantit l'intégrité de l'enregistrement, mais pas la véracité du contenu enregistré⁶⁴⁰.

Ensuite, la pseudonymisation des utilisateurs complique l'établissement d'un lien entre un enregistrement blockchain et une personne physique ou morale identifiée. Pour qu'un enregistrement blockchain serve de preuve dans un litige, il faut pouvoir démontrer que la clé publique associée à la transaction appartient bien à la partie concernée, ce qui peut nécessiter des éléments de preuve complémentaires⁶⁴¹.

Enfin, la complexité technique de la blockchain peut constituer un obstacle à son acceptation par les juridictions. Les juges et les avocats ne sont pas nécessairement familiers avec les concepts cryptographiques et les mécanismes de consensus. L'admission d'un enregistrement blockchain comme preuve pourrait nécessiter le recours à des expertises techniques, alourdissant ainsi la procédure et augmentant les coûts⁶⁴².

3. Les premières applications jurisprudentielles et législatives

Bien que la jurisprudence marocaine en la matière soit encore embryonnaire, certaines juridictions étrangères ont commencé à se prononcer sur l'admissibilité des enregistrements blockchain comme preuve. Aux États-Unis, plusieurs États ont adopté des lois reconnaissant explicitement la valeur probante des enregistrements blockchain. L'état du Vermont, par exemple, a modifié ses règles de preuve pour créer une présomption d'authenticité pour les enregistrements blockchain, sous certaines conditions⁶⁴³.

⁶³⁶ Alice Barbet-Massin, *Le droit de la preuve à l'aune de la blockchain*, op.cit.

⁶³⁷ Gilles Kolifraith & Mélanie Goupy, « Blockchain : les enjeux en droit français », *Revue Internationale des services financiers*, 2017/4, p. 20.

⁶³⁸ Alice Barbet-Massin, *Le droit de la preuve à l'aune de la blockchain*, op. cit.

⁶³⁹ Mehdi Kettani, « Confiance numérique », disponible sur <https://www.lexisma.com/doctrine/maroc/325>

⁶⁴⁰ Rahajaritsimba Franckie Mahery, « L'authenticité et l'intégrité de la signature électronique », *Journal of Integrated Studies in Economics, Law, Technical Sciences & Communication*, vol. 1, n° 1, 2022, p. 12.

⁶⁴¹ Dominique Legeais (dir.), *Blockchain et actifs numériques*, op. cit., p. 80.

⁶⁴² Alice Barbet-Massin, *Le droit de la preuve à l'aune de la blockchain*, op. cit., p. 252.

⁶⁴³ Idem.



En France, comme mentionné précédemment, le législateur a reconnu la blockchain comme support juridique valide pour certains instruments financiers, ce qui implique nécessairement la reconnaissance de la valeur probante des enregistrements blockchain dans ce domaine spécifique⁶⁴⁴. Au Maroc, l'absence de reconnaissance législative explicite de la blockchain (hormis les dispositions générales sur la signature et l'horodatage électroniques de la loi 43-20) laisse aux juges une marge d'appréciation importante.

Pour faciliter cette reconnaissance judiciaire, il serait souhaitable que le législateur marocain adopte des dispositions spécifiques sur la blockchain, à l'instar de ce qui a été fait en France. Ces dispositions pourraient préciser les conditions dans lesquelles un enregistrement blockchain peut être admis comme preuve, les exigences en matière d'identification des parties, et les modalités de vérification technique de l'intégrité des enregistrements⁶⁴⁵.

Conclusion

L'analyse des défis juridiques posés par la blockchain révèle une tension fondamentale entre innovation technologique et cadres normatifs existants. La blockchain, issue d'une philosophie libertarienne et cypherpunk visant à éliminer les tiers de confiance, se heurte à des systèmes juridiques fondés sur la centralisation de l'autorité et la médiation institutionnelle.

Sur le plan technique, la blockchain présente des mécanismes cryptographiques robustes — chiffrement asymétrique, hachage, consensus distribué — qui répondent formellement aux exigences fonctionnelles de la signature électronique et de l'horodatage. La signature par clé privée permet d'identifier le signataire et de garantir l'intégrité du document signé. L'horodatage distribué offre une date certaine immuable et vérifiable. Les enregistrements blockchain bénéficient d'une intégrité technique inégalée grâce au chaînage cryptographique.

Toutefois, la reconnaissance juridique de ces mécanismes demeure incomplète et conditionnée. En droit marocain, la loi 43-20 relative aux services de confiance pour les transactions électroniques pose des exigences strictes pour la signature électronique qualifiée et l'horodatage qualifié, notamment la certification par un prestataire de services de confiance agréé. Or, la blockchain, par sa nature décentralisée, ne s'intègre pas naturellement dans ce modèle de certification centralisée.

Le droit comparé français, bien qu'ayant commencé à reconnaître explicitement la blockchain dans certains domaines (instruments financiers), n'a pas encore pleinement résolu ces tensions. La pseudonymisation des utilisateurs, l'absence d'infrastructure de certification qualifiée intégrée, et les questions de droit international privé constituent autant d'obstacles à l'intégration juridique complète de la blockchain.

Plusieurs pistes d'évolution peuvent être envisagées. Sur le plan législatif, une reconnaissance explicite de la blockchain comme mode de preuve valide, assortie de conditions spécifiques adaptées à sa nature décentralisée, faciliterait son acceptation par les juridictions. Sur le plan technique, le développement de solutions hybrides combinant la robustesse de la blockchain avec la certification par des prestataires agréés pourrait constituer un pont entre innovation et conformité juridique. Sur le plan judiciaire, une formation des magistrats aux enjeux techniques de la blockchain et une approche pragmatique fondée sur l'appréciation au cas par cas de la fiabilité des enregistrements pourraient permettre une reconnaissance progressive.

Au-delà de ces aspects techniques et juridiques, la blockchain interroge plus fondamentalement le rôle du droit et de l'État dans la régulation des échanges économiques et sociaux. Faut-il adapter le droit à la technologie, ou exiger que la technologie se conforme aux cadres juridiques existants ? Cette question, qui dépasse le seul cas de la blockchain, reflète les tensions contemporaines entre innovation technologique, souveraineté étatique et protection des droits individuels.

⁶⁴⁴ Jean-benoît Hubin, *la preuve par la blockchain*, in « les blockchain et les smart contract à l'épreuve du droit », édition LARCIER, p. 203.

⁶⁴⁵ Sophie Coutor, Christine Hennebert & Mourad Faher, *Blockchain et identification numérique*, 2021, p. 87.



La blockchain ne remplacera probablement pas les systèmes juridiques traditionnels, mais elle les complétera et les transformera. L'enjeu pour les législateurs et les praticiens du droit est de trouver un équilibre entre l'encouragement de l'innovation et la préservation des garanties juridiques fondamentales : sécurité juridique, protection des parties faibles, accès à la justice et responsabilité. C'est à cette condition que la blockchain pourra réaliser son potentiel de transformation des échanges économiques et juridiques, tout en s'inscrivant dans un cadre normatif légitime et protecteur.

Références

Bibliographie

I. Ouvrages et thèses

- ANTONOPOULOS, Andreas M., *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, O'Reilly Media, 2014.
- BARBET-MASSIN, Alice, *Le droit de la preuve à l'aune de la blockchain*, thèse de doctorat, Université de Lille, 2020.
- COUTOR, Sophie, HENNEBERT, Christine & FAHER, Mourad, *Blockchain et identification numérique*, 2021.
- DE FILIPPI, Primavera & WRIGHT, Aaron, *Blockchain and the Law: The Rule of Code*, Harvard University Press, 2018.
- HUBIN, Jean-Benoît, « La preuve par la blockchain », in *Les blockchain et les smart contracts à l'épreuve du droit*, édition Larcier.
- KATZ, Jonathan & LINDELL, Yehuda, *Introduction to Modern Cryptography*, 2e éd., CRC Press, 2014.
- LEGEAIS, Dominique, *Blockchain et actifs numériques*, LexisNexis, 2e éd., 2019.
- LEVENEUR, Claire, *Les smart contracts : étude de droit des contrats à l'aune de la blockchain*, thèse de doctorat, Université Paris-Panthéon-Assas, 2 décembre 2022.
- LEVY, Steven, *Crypto: How the Code Rebels Beat the Government — Saving Privacy in the Digital Age*, Viking, 2001.
- NARAYANAN, Arvind et al., *Bitcoin and Cryptocurrency Technologies*, Princeton University Press, 2016.
- NETTER, Emmanuel, *Numérique et grandes notions de droit privé*, Ceparisca, collection Essais, 2017.
- SCHNEIER, Bruce, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2e éd., Wiley, 1996.
- TAPSCOTT, Don & TAPSCOTT, Alex, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, Penguin, 2016.

II. Articles de revues et contributions

- ASSAYA, Laurent & BAUDOUIN, Vincent, « La signature électronique par cryptographie à clé publique », *La Semaine Juridique Entreprise et Affaires*, n° 4, 23 janvier 2003, 146.
- BARBAN, Patrick, « L'écrit électronique et la blockchain : formalisme et preuve du consentement », in *Structures et usages de la blockchain*, Lefebvre Dalloz, 2024, p. 85 et suiv.
- DE FILIPPI, Primavera, « Bitcoin: A Regulatory Nightmare to a Libertarian Dream », *Internet Policy Review*, vol. 3, n° 2, 2014.
- DIFFIE, Whitfield & HELLMAN, Martin, « New Directions in Cryptography », *IEEE Transactions on Information Theory*, vol. 22, n° 6, 1976, p. 644-654.
- HAAS, Gérard & THIBAUT, Clément, « Blockchain : définitions et enjeux », *Revue Banque*, n° 810, 2017.
- KETTANI, Mehdi, « Confiance numérique », disponible sur <https://www.lexisma.com/doctrine/maroc/325>.



- KOLIFRATH, Gilles & GOUPY, Mélanie, « Blockchain : les enjeux en droit français », *Revue Internationale des services financiers*, 2017/4, p. 20.
- MEKKI, Mustapha, « Le juge et la blockchain : l'art de faire du nouveau vin dans de vieilles outres ».
- NAMONT DAUCHEZ, Corine & CLUZEL-MÉTAYER, Lucie, « Registres publics vs blockchain publique », in *L'État et le notariat face à la révolution blockchain*, *Revue du droit public et de la science politique en France et à l'étranger*, 2022, n° 1, p. 101.
- RAHAJARITSIMBA, Franckie Mahery, « L'authenticité et l'intégrité de la signature électronique », *Journal of Integrated Studies in Economics, Law, Technical Sciences & Communication*, vol. 1, n° 1, 2022, p. 12.
- YANG, X. et al., « Enhancing the Regulatory Framework around Electronic Signatures through the Integration of Blockchain Technology », 2023. DOI : 10.1145/3651655.3651661.

III. Textes législatifs et réglementaires

Droit marocain

- Dahir des Obligations et Contrats (DOC).
- Loi n° 43-20 relative aux services de confiance pour les transactions électroniques.

Droit français

- Code monétaire et financier français.
- Ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse.

Droit américain

- *Telecommunications Act of 1996*, Pub. L. No. 104-104, 110 Stat. 56 (1996).

IV. Rapports institutionnels et encyclopédies juridiques

- JurisClasseur Droit bancaire et financier, Fasc. 179 : Blockchain.
- Ministère de l'Économie et des Finances (France), « La blockchain », disponible sur economie.gouv.fr.
- Journal Officiel de la République Française, Vocabulaire de l'informatique et de l'internet, avis du 23 mai 2017, JORF n°0121 du 23 mai 2017.
- Office parlementaire d'évaluation des choix scientifiques et technologiques (France), « Les enjeux technologiques des blockchains (chaînes de blocs) », Rapport n° 584, 2018.

V. Sources primaires et manifestes

- BACK, Adam, « Hashcash — A Denial of Service Counter-Measure », 1997.
- BARLOW, John Perry, « A Declaration of the Independence of Cyberspace », 1996.
- DAI, Wei, « b-money », 1998, disponible sur weidai.com.
- FINNEY, Hal, « RPOW — Reusable Proofs of Work », 2004.
- HUGHES, Eric, « A Cypherpunk's Manifesto », 1993.
- MAY, Timothy C., « The Crypto Anarchist Manifesto », 1988.
- NAKAMOTO, Satoshi, « Bitcoin: A Peer-to-Peer Electronic Cash System », 2008.
- STALLMAN, Richard, « The GNU Manifesto », 1985, disponible sur gnu.org.
- SZABO, Nick, « Bit Gold », 1998 (publié en 2005).

VI. Sources en ligne

- <https://www.assemblee-nationale.fr/14/amendements/3785/AN/227.asp>
- <https://brave.com/fr/glossary/peer-to-peer/>
- <https://www.baridesign.ma/wps/portal/barideSign>
- <https://www.geeksforgeeks.org/computer-networks/what-is-p2p-peer-to-peer-process/>
- <https://www.spiceworks.com/tech/networking/articles/what-is-peer-to-peer/>