LIVRE BLANC

Assurabilité des activités liées à la blockchain et aux cryptoactifs

Mythes et réalités

LSN Assurances
Groupe DiotSiaci

BDJ
Groupe DiotSiaci

NeoTech
Groupe DiotSiaci

Sommaire

Édito

Delphine MERCELAT
Directrice Professions Réglementées et Réassurance
Groupe Diot-Siaci

Les cryptoactifs seraient un effet de mode ? Ce n'est pas notre avis.

Notre conviction est que la bulle spéculative autour des cryptomonnaies et autres jetons est l'arbre qui cache une tendance émergente, mais solide, impulsée par cette innovation de rupture qu'est la technologie blockchain.

En France, l'industrie commence à se structurer. Le nombre de prestataires de services spécialisés – les PSAN, ou prestataires de services sur actifs numériques –, approche la centaine et s'institutionnalise. Des offres de services d'infrastructure de blockchain visant à accélérer les déploiements applicatifs se profilent. Et l'adoption par le grand public progresse : près d'un Français sur dix détiendrait des cryptoactifs, soit une augmentation de 18 % par rapport à l'an passé, selon une étude récente de l'association des professionnels du Web 3 en France et en Europe (l'Adan), du cabinet de conseil KPMG et de l'institut de sondage Ipsos.

Dopée à l'innovation, cette toute jeune industrie porte néanmoins des risques élevés en elle. La blockchain reste controversée – notamment sur le plan environnemental. La régulation du marché n'est pas encore stabilisée. Et les cours des cryptoactifs continuent d'afficher une extrême volatilité.

C'est le rôle de l'assurance de financer les prises de risques de l'économie, pour autant qu'elles soient mesurables et mutualisables. C'est même l'origine de son existence : « le prêt à la grosse aventure », qui a permis de favoriser, développer et sécuriser les échanges commerciaux maritimes… Or, force est de constater que le monde de l'assurance renâcle à se lancer. Les mots blockchain, NFT, PSAN, bitcoin y sont tabous : prononcez l'un d'entre eux et le joker « interdit de souscription » est immédiatement brandi !

La blockchain, à l'instar d'Internet, promet de transformer des pans entiers de l'économie, la finance en premier lieu, mais aussi la culture, la logistique, le luxe, l'immobilier ou l'assurance, elle-même. À l'heure où l'ambition nationale[2] et européenne est d'armer nos territoires et entreprises afin qu'ils deviennent les fers de lance d'un monde numérique, propre, sécurisé et transparent, l'assurance doit être au rendez-vous de l'aventure blockchain.

[1] Web3 et Crypto en France et en Europe : Adoption par le grand public et applications par les industries
[2] Bruno Le Maire veut faire de la France "le camp de base en Europe" des cryptos et de la DeFi

Leader du marché et précurseur dans la mise en œuvre de l'innovation, le groupe Diot-Siaci s'est emparé du sujet à travers ses trois filiales, LSN Assurances, courtier spécialisé dans le notariat et les professions réglementées, BDJ, courtier historique des conseillers en gestion de patrimoine, et NeoTech Assurances, spécialiste des entreprises du secteur du numérique et courtier du programme d'assurance des membres de Numeum. Durant plusieurs semaines, nos trois entités ont réuni leurs partenaires et clients respectifs pour travailler sur les risques associés aux cryptoactifs et à la blockchain et discuter des transformations induites par ces innovations sur leurs métiers.

Nous remercions vivement les assureurs, conseillers en gestion du patrimoine, entreprises du numérique, notaires et professionnels du droit qui ont participé à ces groupes de travail et dont les échanges ont permis la composition de ce livre blanc.

Notre intention est d'apporter un éclairage sur les fondements et enjeux de la technologie afin de démêler les mythes de la réalité et faciliter l'investigation sur l'assurabilité des activités liées à la blockchain et aux cryptoactifs. Cela, à travers le prisme de trois professions aujourd'hui très concrètement concernées : les notaires, amenés à liquider des patrimoines contenant des cryptoactifs ou à réaliser des transactions en cryptomonnaies ; les conseillers en gestion de patrimoine, qui guident leurs clients dans leurs stratégies d'investissement, et les entreprises du numérique qui créent ou hébergent des cryptoactifs ou développent des solutions et services s'appuyant sur la blockchain.

Cette initiative est la première étape d'une démarche au long cours. L'économie de la blockchain et des cryptoactifs pose de nombreuses questions qui devront trouver des réponses. Nous allons continuer à jouer notre rôle d'éclaireur auprès de nos clients et de nos partenaires pour les aider à assimiler ces nouvelles technologies dans leurs activités. Et nous le ferons, en nous nourrissant de leurs réflexions et expériences partagées, dans le même esprit que la réalisation de ce livre blanc.

Comprendre la blockchain et les cryptoactifs

01

La blockchain, une infrastructure de confiance pour les échanges de pair-à-pair

En 2008, la crise financière mondiale ébranle la confiance dans le système bancaire et ses institutions.

C'est alors qu'un programmeur, qui se fait appeler Satoshi Nakamoto[3], publie un article dans lequel il décrit un système monétaire alternatif permettant le transfert d'argent par voie électronique, en direct, aussi simplement que l'on s'échange des espèces ou que l'on envoie des documents par email à travers la planète.

Pour donner vie à ce dispositif révolutionnaire, Satoshi Nakamoto fait appel à un concept encore balbutiant à l'époque, la blockchain. Il le perfectionne jusqu'à le rendre utilisable dans son innovation.

De ses travaux, nait en 2009, Bitcoin, **le premier système monétaire mondial entièrement dématérialisé et géré par du code informatique.**

Aujourd'hui, soit à peine 15 ans plus tard, le réseau Bitcoin compte environ 10 000 nœuds[4] répartis dans le monde et près de 270 millions d'utilisateurs[5].

Plus de 500 000 transactions y ont cours chaque jour[6]. Une unité de cryptomonnaie bitcoin[7], qui valait 100 dollars en 2013, s'échange actuellement à plus de 20 000 dollars[8] (après avoir culminé à 65 000 dollars en novembre 2021).

Les trois principes de la blockchain

Le fonctionnement de la blockchain repose sur trois principes fondamentaux :

#1 Un registre dans lequel sont consignés tous les échanges réalisés depuis la création de la blockchain, sous la forme de blocs reliés entre eux par des moyens cryptographiques qui rendent l'ensemble infalsifiable.

#2 La réplication de ce registre sur les ordinateurs constituant le réseau (architecture distribuée).

#3 Un mécanisme de validation des transactions par consensus.

Atouts et défis

ATOUTS

Robustesse
Infrastructure décentralisée.

Variété des usages
Transfert de valeur, espace marchand dématérialisé, registre sécurisé, applications distribuées pour la finance, la logistique, la culture, l'énergie, le métavers…

Intégrité
Immutabilité des règles inscrites dans le registre.

[3] La réelle identité de ce programmeur, qui pourrait aussi être un groupe de développeurs, demeure inconnue encore aujourd'hui.
[4] Les nœuds sont les ordinateurs sur lesquels tourne le logiciel structurant le réseau.
[5] Crypto Market Sizing Report H1 2023
[6] Valeur en septembre 2023
[7] Bitcoin en tant que système s'écrit avec un B majuscule, tandis que l'unité de compte bitcoin s'écrit avec un b minuscule.
[8] Valeur fin septembre 2023

Le fait que la première implémentation aboutie d'une blockchain ait été dans Bitcoin a intriqué les deux innovations, mais la blockchain doit être comprise comme **une technologie généraliste qui se décline sous de multiples formes** et s'utilise pour d'autres activités que la finance, même si cet usage prédomine.

Elle présente, de ce point de vue, des similitudes avec le réseau Internet dont les protocoles ont servi au déploiement d'extranets et d'intranets à travers le monde et rendu possible l'avènement d'une multitude de services applicatifs, tels que les messageries électroniques, le Web, les plateformes de partage, les réseaux sociaux, etc.

La blockchain peut ainsi se définir comme une infrastructure décentralisée dont les mécanismes permettent d'échanger de la valeur et des informations, de pair-à-pair, sans nécessiter d'intermédiaire de confiance.

de la blockchain

DÉFIS

Environnement risqué
Espace de marché hautement spéculatif et entaché par la criminalité financière et les escroqueries.

Empreinte carbone élevée
Protocole de validation des transactions énergivore.

Passage à l'échelle difficile
Ralentissement des validations avec l'expansion des réseaux et des usages.

Le mécanisme de validation des transactions

Dans une blockchain, les transactions en attente de validation sont regroupées par blocs sur chacun des noeuds du réseau. L'enregistrement d'un bloc validé consiste à l'horodater et à lui attribuer une empreinte numérique calculée par cryptographie et contenant des données relatives au bloc précédent. C'est ce lien d'ordonnancement cryptographique entre les blocs qui rend le registre de la blockchain quasiment infalsifiable.

L'innovation majeure de Satoshi Nakamoto avec Bitcoin a été de créer un protocole de validation garantissant qu'une transaction ne peut être enregistrée deux fois (autrement dit que les cryptomonnaies engagées dans la transaction ne sont pas dépensées deux fois).

La méthode consiste à demander aux valideurs de résoudre un problème de cryptographie complexe requérant des ressources en calcul élevées (pour dissuader les fraudeurs), et à récompenser le valideur qui, le premier, aura résolu le problème, en le rétribuant avec des bitcoins.

Le protocole est appelé *Proof of Work*, car la résolution du problème revient à apporter la preuve du travail effectué (le calcul pour résoudre le problème). Le processus de résolution de ce problème cryptographique est appelé le minage, et les participants qui effectuent cette tâche, les mineurs.

L'enregistrement du bloc est finalement effectué par le vainqueur après confirmation consensuelle de la validité de la transaction par le réseau de valideurs. Cette opération consiste essentiellement à consulter le registre pour authentifier les émetteurs des transferts de cryptoactifs et vérifier qu'ils possèdent effectivement les montants à transférer.

Proof of Work est utilisé par d'autres blockchains que Bitcoin, mais il existe aussi d'autres protocoles qui fonctionnent selon des règles différentes. Ainsi, *Proof of Stake* (preuve d'enjeu), mis en œuvre par les blockchains Ethereum et Tezos, repose sur la quantité de cryptomonnaies détenue et non la puissance de calcul mobilisée.

Une technologie aux multiples formes

De nombreuses déclinaisons de blockchains publiques

Il existe plusieurs dizaines de variétés de blockchains. Les plus connues sont publiques. Ce qui signifie que **quiconque peut y accéder et consulter leur registre** en ouvrant un compte. Elles sont, par ailleurs, codées en open source afin de rendre leur fonctionnement transparent.

La blockchain historique, Bitcoin, reste la plus populaire. Sa cryptomonnaie, le bitcoin, représente encore 45 % de la capitalisation du marché des cryptoactifs. D'autres blockchains concurrentes sont apparues depuis, souvent avec la promesse de résoudre une de ses faiblesses comme, par exemple, celle de réduire le temps de traitement des transactions. Ces alternatives, telles que Cardano, Dogecoin, Ethereum, Litecoin, Solana, Tezos, etc., font appel aux mêmes principes que Bitcoin. Elles appliquent, cependant, des protocoles de validation et des modes de gouvernance différents et émettent leur propre cryptomonnaie.

Dans les faits, très peu ont atteint la masse critique leur permettant de rivaliser avec Bitcoin. Ethereum fait partie de celles-là.

Créée en 2015, cette blockchain a percé grâce à une proposition de valeur qui dépasse celle de Bitcoin : elle a été conçue avec l'ambition d'en faire un système d'exploitation distribué mondial. **Ethereum se distingue ainsi de Bitcoin par sa capacité à héberger des applications informatiques** et exécuter des petits programmes natifs appelés *smart contracts*. En résumé, si Bitcoin a instauré le transfert de valeur par Internet de pair-à-pair, Ethereum a ouvert le champ à de nouveaux usages[9].

Les smart contracts

Les *smart contracts* ne sont pas des contrats au sens juridique du terme. Ce sont des petits programmes informatiques qui s'exécutent dans certaines blockchains telles qu'Ethereum. Ils se déclenchent automatiquement dès lors que des conditions définies préalablement sont réunies. Inscrits dans la blockchain, ils sont infalsifiables.

Ils se trouvent au cœur des applications distribuées sur les blockchains. On les utilise, par exemple, pour automatiser l'exécution de chaînes d'opérations impliquant plusieurs acteurs ou organisations.

Les notions de compte et de clés privée et publique

Un compte est matérialisé par une adresse dans la blockchain que l'on pourrait assimiler à un IBAN. On le crée à l'aide d'une application informatique appelée portefeuille (ou *wallet)* qui permettra ensuite d'accéder aux informations relatives aux comptes (soldes, etc.) et de réaliser des transactions.

À un compte est associée une paire de clés. La première est publique et n'est autre que l'adresse du compte dans la blockchain. Elle permet de recevoir des cryptomonnaies ou d'identifier un destinataire. La deuxième est la clé privée. Elle sert à accéder au compte et à signer les transactions. Elle doit donc absolument rester secrète et être conservée de manière sécurisée. Sans ces deux clés, l'accès à un compte et aux cryptomonnaies qu'il contient est définitivement perdu.

La clé privée se présente souvent comme une suite de 12 ou 24 mots, appelée « phrase secrète » (*seed phrase*). Idéalement, il faudrait pouvoir la retenir et ne l'enregistrer nulle part. Dans la pratique, certains utilisateurs l'écrivent sur un morceau de papier, d'autres la conservent dans le portefeuille utilisé pour créer le compte et générer les clés (lire l'encadré Une variété de types de portefeuilles). D'autres encore créent leur compte via une plateforme d'échange, ce qui rend transparente la gestion de leurs clés.

[9] Les évolutions récentes de Bitcoin ainsi que le développement de couches logicielles additives visent, néanmoins, à étendre ses possibilités.

La blockchain privée, pour faciliter les interactions entre organisations

En parallèle du développement des blockchains publiques, ont émergé des formes privatives de blockchains dont l'accès est réservé aux entités ou personnes autorisées, et des systèmes hybrides qui mêlent les modèles publics et privés.

Une blockchain privée déployée chez un industriel lui permet, par exemple, de mieux contrôler ses chaînes d'approvisionnement en fédérant ses fournisseurs sur un réseau de partage d'informations infalsifiable.

Des blockchains dites « de consortium » se sont aussi développées à l'initiative de groupes d'organisations qui veulent faciliter leur coopération dans un domaine donné, en automatisant les échanges et les chaînes de traitement, ou qui souhaitaient conjuguer leurs efforts autour d'une cause commune. On peut citer la blockchain Aura, créée par LVMH, Mercedes-Benz, OTB, Prada Group et Richemont pour garantir la traçabilité et l'authenticité des produits de luxe, le réseau Vakt, qui facilite la coopération dans le monde du trading pétrolier, et Canton Network, qui réunit Goldman Sachs, BNP Paribas, Deutsche Börse Group, Microsoft et Deloitte pour décloisonner et rendre interopérables les systèmes bancaires et améliorer la rapidité et la sécurité des échanges entre les banques.

Ces réseaux privés utilisent certains mécanismes de la blockchain publique, notamment la consignation des événements et opérations dans un registre décentralisé réputé inviolable.

La garantie de l'intégrité des données du registre permet d'instaurer la confiance entre les partenaires. En revanche, ces blockchains sont moins décentralisées et comme elles sont gérées par un nombre restreint d'acteurs approuvés, elles n'ont pas besoin d'une cryptomonnaie et de protocoles de validation des transactions aussi complexes que leurs homologues publiques pour fonctionner. Les blockchains de consortium requièrent néanmoins de s'accorder sur les règles de fonctionnement (quels processus de validation, d'authentification, d'enrôlement des nouveaux membres, etc.) et de mettre en place une gouvernance.

La décentralisation, au cœur de la philosophie

Robutesse du réseau

La décentralisation est une propriété fondamentale de la blockchain qui intervient sur plusieurs plans.

Par-delà la sécurisation des transactions (lire l'encadré Le mécanisme de validation des transactions), elle assure à l'infrastructure la robustesse nécessaire à un fonctionnement 24 heures sur 24 et 7 jours sur 7, en toute situation et malgré les empêchements – pannes techniques, bugs dans une mise à jour, cyberattaques, mais aussi mainmise ou censure par un État. Avec la condition, cependant, que les nœuds constitutifs du réseau soient en nombre suffisant, répartis dans plusieurs pays et dispersés entre plusieurs hébergeurs. Dans les faits, peu de blockchains peuvent aujourd'hui revendiquer un tel niveau de décentralisation. Même Ethereum, pourtant dotée de plusieurs milliers de nœuds sur lesquels tournent différentes variantes du logiciel, ne remplit pas toutes les conditions, car une partie importante de ses nœuds se trouvent concentrés dans les ***clouds***[10] d'une poignée d'acteurs[11].

Gouvernance par consensus

La décentralisation figure également au cœur de la philosophie de gouvernance de la technologie. **Une blockchain vit grâce à la dynamique générée par la communauté qui gravite autour d'elle** : les développeurs, qui proposent des corrections et des améliorations du logiciel, les propriétaires des nœuds du réseau qui installent les mises à jour et les valideurs qui confirment les transactions.

L'adhésion de cet écosystème à l'esprit et aux orientations de la blockchain est déterminante pour attirer les utilisateurs et assurer sa pérennité. La baisse de motivation d'une partie de l'écosystème peut entraîner la contraction de l'activité du réseau et conduire à l'abandon du projet.

Le recueil du consensus se révèle crucial lorsqu'une évolution majeure des règles de fonctionnement (pour résoudre une limitation technique ou corriger un bug, par exemple) nécessite l'installation d'une mise à jour du logiciel sur les nœuds du réseau. En cas de désaccord d'une partie de la communauté, il peut arriver que la blockchain se scinde en deux branches qui évolueront indépendamment, les partisans de la nouveauté installant la version modifiée, les autres restant sur la mouture historique. À la suite d'un tel embranchement, appelé ***hard fork***, une nouvelle cryptomonnaie liée à la chaîne dissidente voit le jour.

Bitcoin et Ethereum ont, toutes les deux, connu des évolutions de ce type au cours de leur histoire. En septembre 2022, le passage d'Ethereum du protocole ***Proof of Work*** au protocole ***Proof of Stake***, moins énergivore, est un exemple d'embranchement réussi. Il a abouti à la création de deux réseaux Ethereum qui fonctionnent en parallèle : Ethereum ***Proof of Stake*** (le nouveau), qui a emporté la plus large adhésion, et Ethereum ***Proof of Work*** (l'ancien), qui subsiste cependant.

[10] Services d'infrastructure informatique en ligne.
[11] Ethereum et Solana dans le cloud – La blockchain à l'épreuve de la centralisation

Les principaux cas d'usage

L'échange dématérialisé d'actifs

La fonction première de la blockchain est d'assurer le transfert d'actifs sur Internet. L'opération peut s'effectuer soit directement entre deux adresses (pour envoyer des fonds à l'international ou effectuer un paiement, par exemple), soit par l'intermédiaire d'une plateforme d'échange comme Binance, Coinbase, Crypto.com ou Kraken.

Simples à utiliser, ces places de marché ont contribué à démocratiser l'accès à l'investissement dans les cryptoactifs. Malgré les soubresauts de 2021 et 2022 (le marché a perdu 60 % de sa valeur pendant cette période[12]), elles continuent d'attirer un nombre croissant d'investisseurs motivés par la perspective de rendements élevés. Le nombre de détenteurs de cryptoactifs a ainsi progressé de 21 % par rapport à décembre 2022 pour atteindre 516 millions en juin 2023[13]. La capitalisation reste néanmoins modeste en comparaison des bourses traditionnelles (800 milliards de dollars de capitalisation en juin 2022 contre 25 000 milliards pour la seule bourse de New York[14]).

Les cryptomonnaies natives des blockchains ne sont pas les seules classes d'actifs à y circuler. Sur les blockchains autorisant les ***smart contracts***, on trouve, en particulier, des ***stablecoins***. Ces produits sont arrimés à un autre actif, en général une monnaie qui a cours légal comme le dollar américain, dans le but de réduire leur exposition à la volatilité. Les ***stablecoins*** sont, à ce titre, privilégiés par les investisseurs non experts.

Les ***smart contracts*** permettent également la création de jetons (ou ***tokens***). Les jetons remplissent diverses fonctions, parmi lesquelles celle de représenter des actifs de la vie « réelle » sur la blockchain.

NFT, tendance 2022 du marché crypto

Les CryptoPunks ont été les premiers NFT (*Non-Fungible Token*). Cette collection de petites images numériques pixélisées, créée en 2017 par la société Larva Labs, est devenue emblématique de l'art numérique. Mais c'est la vente aux enchères chez Christie's, le 11 mars 2021, de l'œuvre *Everyday: the First 5 000 days* de l'artiste Beeple (alias Mike Winkelmann), pour 70 millions de dollars, qui a définitivement consacré le NFT comme un actif hautement valorisable. Dans les mois qui ont suivi, le marché des NFT a explosé. Il a atteint plusieurs dizaines de milliards de dollars pour se contracter à nouveau en 2022, perdant 30 % de sa valeur.

Les NFT sont souvent des œuvres d'art numérique, car ils sont une façon simple pour des artistes de diffuser leurs œuvres et de bénéficier de redevances automatiques lors des ventes successives (les conditions devront néanmoins être codées dans le *smart contract* du NFT). Mais un NFT peut tout aussi bien être un objet en édition limitée, un accessoire de jeu vidéo, un billet pour un événement, un territoire dans le métavers, etc.

L'achat d'un NFT présente plusieurs risques notamment celui de contrevenir à la propriété intellectuelle du sous-jacent ou tout simplement d'être trompé sur la marchandise si le smart contract ne correspond pas dans les faits à ce qui a été prétendument vendu.

Notons, par ailleurs, qu'il persiste un flou dans les législations française et européenne sur le sujet des régimes fiscaux et juridiques d'appartenance des NFT.

[12] Bloc-notes Éco publie des articles pédagogiques qui présentent la recherche, les études et l'expertise économique de la Banque de France
[13] Crypto Market Sizing Report H1 2023
[14] Enjeux et risques des crypto-actifs Trésor-Eco

Grâce aux eux, il devient possible d'utiliser le réseau pour vendre et acheter toutes sortes de biens tangibles ou intangibles – des services, des droits, des actifs financiers, des biens numériques, ainsi que des objets physiques. Ce phénomène de tokenisation permet de profiter de la grande liquidité qu'offre cet espace marchand.

Il existe plusieurs classes de jetons. Certains sont qualifiés d'utilitaires (***utility tokens***), car ils servent à accorder des droits spécifiques à leur détenteur. Ils sont souvent émis lors des ICO (*Initial Coin Offering*), qui sont des levées de fond de projets créés sur des blockchains. Lors d'une ICO, l'investisseur acquiert des droits liés au projet (souvent une facilité d'usage du futur produit) qu'il pourra exercer une fois celui-ci concrétisé.

On trouve également des jetons financiers, qui correspondent à des actions ou des titres émis par les sociétés sur une blockchain. Ces jetons, appelés ***security tokens***, sont considérés comme des instruments financiers et relèvent des réglementations nationales et européennes afférentes.

Les jetons utilitaires et financiers sont fongibles, à l'instar des cryptomonnaies. En 2017, apparaît **la notion de jetons non fongibles pour répondre aux besoins de valoriser des actifs que l'on peut individualiser**, et de garantir les droits de propriété associés. Un jeton non fongible ou NFT (*Non-Fungible Token*) possède une identité propre. Il n'est donc ni remplaçable ni interchangeable par un autre jeton. Un sous-jacent tangible ou intangible y est par ailleurs attaché. Posséder un NFT permet de revendiquer ou de transférer la propriété du sous-jacent.

Le jeton agit ainsi comme une sorte de certificat de propriété et comme un certificat d'authenticité du bien sous-jacent. L'utilisation d'une blockchain permet d'assurer la traçabilité des opérations (montant et date des transactions, adresse des acheteurs et des vendeurs, etc.) et de rendre ces dernières immuables.

NFT Comment cela marche ?

La création d'un NFT consiste à produire un *smart contract* dont le format est standardisé (norme ERC 721 ou ERC 1155), puis à l'enregistrer (les spécialistes emploient le verbe « *minter* ») dans une blockchain appropriée (souvent Ethereum). L'enregistrement du *smart contract* dans la blockchain entraîne la création du NFT sous la forme d'un identifiant unique directement lié à l'adresse du créateur du *smart contract*.

Le *smart contract* contient quelques éléments supplémentaires, notamment, une sorte d'URL qui dirige vers un fichier listant des informations caractérisant le bien sous-jacent (une description sommaire, des propriétés, une date de création, le nom de l'auteur, etc.) et l'URL du serveur où le fichier numérique représentant le bien sous-jacent se trouve stocké. Le fichier numérique est, en effet, usuellement stocké en dehors de la blockchain (éventuellement sur un système distribué comme IPFS – *Interplanetary File System* – plus sûr qu'un serveur ordinaire).

Dans le cadre d'une opération de vente-achat, le *smart contract* exécute l'opération de transfert d'adresses dès lors que la transaction en cryptomonnaie (à laquelle s'ajoutent les frais perçus par la plateforme d'échange) a été réalisée.

L'enregistrement inaltérable d'informations

La blockchain peut aussi être utilisée dans sa fonction de base de registre réputée inviolable, pour stocker et rendre publiquement accessibles des documents certifiés tels qu'un diplôme ou un titre de propriété (c'est dans cette optique que le Ghana a implémenté son cadastre dans une blockchain en vue de remettre de la transparence dans son régime foncier et fiabiliser les transactions). On peut aussi y consigner des informations inaliénables qui seront, là aussi, publiquement accessibles (à des fins de traçage réglementaire, par exemple).

Il est, cependant, important de noter d'une part, que **la blockchain garantit l'intégrité de l'enregistrement, mais pas nécessairement la véracité des informations enregistrées**; et d'autre part, qu'un enregistrement dans une blockchain ne constitue pas une preuve légale.

L'exécution d'applications distribuées

Le troisième cas d'usage est celui qui concentre le plus d'innovations. Il consiste à s'appuyer sur les blockchains programmables, publiques ou privées, pour mettre en œuvre des applications entièrement distribuées qui vont au-delà de la fonction de base de transfert de valeur. Plus résilientes que leurs homologues centralisées, ces applications sont aussi intègres par nature : reposant sur des ***smart contracts***, elles s'exécutent automatiquement selon des règles immuables, inscrites dans la blockchain. Elles sont le fer de lance du Web 3[15], cette nouvelle vague de services Internet qui vise à supplanter les services 2.0 actuels, interactifs, mais centralisés.

La finance est l'un des secteurs les plus dynamiques dans ce domaine, avec l'émergence d'infrastructures financières décentralisées, regroupées sous le nom de DeFi (***Decentralized Finance***), qui mettent en œuvre des protocoles dédiés à des fonctions spécifiques, à l'instar du protocole de prêt et emprunt AAVE.
Des écosystèmes applicatifs s'organisent autour de ces protocoles en vue de fournir des services financiers plus accessibles, transparents et robustes que la finance traditionnelle. La DeFi représenterait d'ores et déjà plus de 30 % du volume des transactions de cryptoactifs en Europe de l'Ouest[16].

La logistique et la supply chain sont deux autres secteurs qui ont très tôt manifesté leur intérêt pour la blockchain, souvent dans sa forme privée. Les ***smart contracts*** permettent d'automatiser des chaînes d'opérations ou d'événements impliquant plusieurs acteurs et de tracer les événements sans risques de falsification des informations sur les mouvements de produits ou de matériels. Par-delà les avantages opérationnels, l'utilisation d'une blockchain a aussi le mérite de responsabiliser les acteurs de la chaîne.

Autre exemple : les métavers décentralisés des sociétés Decentraland et Sandbox. Dans ces univers immersifs, investis par les grandes marques, les utilisateurs évoluent par le biais d'avatars et acquièrent des territoires et autres biens numériques sous la forme de NFT.

Enfin, la blockchain se prête bien à la gestion transactionnelle de systèmes distribués impliquant des interactions entre individus qui ne se connaissent pas tels que les ***smartgrids***, le ***crowdfunding*** ou les réseaux de l'économie collaborative.

[15] Qu'est-ce que le Web3, cette version décentralisée d'Internet ?
[16] The Chainalysis 2022 Geography of Cryptocurrency Report

Trois défis majeurs à relever

Malgré ses potentialités, la blockchain souffre d'une image négative – en partie justifiée – qui entrave sa généralisation. Son développement responsable passe par la résolution de trois défis majeurs.

Sécuriser le marché par la régulation

La criminalité financière est une réalité sur la blockchain. La technologie offre une facilité pour effectuer des transferts d'argent transnationaux sous une identité dissimulée[17] dont profitent les malfaiteurs. Les escroqueries y sont également monnaie courante[18] sous la forme de fausses ICO, de piratage de plateformes d'échange ou d'extorsion de clés privées, par exemple.

Selon le cabinet spécialisé américain Chainanalysis, le montant des transactions illicites en cryptoactifs dans le monde, toutes catégories confondues, a dépassé 20,6 milliards de dollars en 2022, en hausse de 14 % par rapport à 2021[19]. Cela équivaut à 0,24 % de l'ensemble des échanges de cryptoactifs sur la même période (à titre de comparaison, le taux de fraude à la carte bancaire en France en 2022 a représenté 0,053 % des paiements réalisés avec ce moyen[20]). Cette proportion tend, cependant, à diminuer avec le temps.

Les autorités financières nationales – américaines notamment – parviennent à juguler le fléau en durcissant les sanctions infligées et en utilisant des dispositifs de pistage de plus en plus efficaces[21].

En Europe, une nouvelle loi, entrée en vigueur le 30 juin dernier, vise à mettre un terme définitif aux comportements frauduleux à l'intérieur de l'UE.

Son intention est de lutter contre le blanchiment d'argent illicite, sécuriser le marché et protéger les investisseurs à travers deux règlements.

Le premier concerne la criminalité financière : il étend l'application de la règle de transfert de fonds (TFR, ***Transfer of Funds Regulation***), qui a cours dans la finance traditionnelle, au monde des cryptoactifs.

Définitions officielles de l'actif numérique et du cryptoactif

Dans le code monétaire et financier français, les cryptoactifs sont appelés « actifs numériques ». Selon la règle L54-10-1, ils comprennent :

- les jetons (tout bien incorporel représentant, sous forme numérique, un ou plusieurs droits pouvant être émis, inscrits, conservés ou transférés au moyen d'un dispositif d'enregistrement électronique partagé permettant d'identifier, directement ou indirectement, le propriétaire dudit bien), à l'exclusion de ceux remplissant les caractéristiques des instruments financiers,

- toute représentation numérique d'une valeur qui n'est pas émise ou garantie par une banque centrale ou par une autorité publique, qui n'est pas nécessairement attachée à une monnaie ayant cours légal et qui ne possède pas le statut juridique d'une monnaie, mais qui est acceptée par des personnes physiques ou morales comme un moyen d'échange et qui peut être transférée, stockée ou échangée électroniquement.

La définition dans le règlement MiCA diffère légèrement : selon l'article 3, un cryptoactif est une représentation numérique d'une valeur, ou de droits, pouvant être transférée ou stockée sous forme électronique au moyen de la technologie des registres distribuée ou d'une technologie similaire.

[17] Contrairement à ce que l'on entend souvent, la plupart des blockchains (dont Bitcoin) ne préservent pas l'anonymat des utilisateurs, car ces derniers sont enregistrés via une adresse identifiable, assimilable à un pseudonyme. Quelques-unes, cependant, garantissent l'anonymat complet, à l'instar de Monero (d'ailleurs menacée d'interdiction par la Commission européenne).
[18] SEC Chair Gary Gensler Says Crypto Is a Highly Speculative Field 'Rife With Fraud'
[19] The Chainalysis 2023 Crypto Crime Report
[20] Banque de France - communiqué de presse : Après une baisse globale de la fraude aux moyens de paiement
[21] D'autant que le traçage des transactions est relativement aisé du fait de la transparence des registres.

L'objectif de la ***travel rule***, comme elle est souvent dénommée, est de garantir le traçage des transactions et le blocage des opérations suspectes[22]. Elle consiste à demander aux plateformes d'échange de collecter des renseignements concernant les sources et les bénéficiaires d'une transaction (donc de lever toute forme d'anonymat) et de les attacher à cette dernière.

Pour les opérations depuis des portefeuilles autohébergés (principalement détenus par des utilisateurs privés), cette obligation ne concerne que les transferts dépassant 1 000 euros. Les transferts directs (qui ne passent pas par des plateformes d'échange) ne sont pas concernés par la règle.

Le deuxième texte est le règlement *Markets in Crypto-Assets* (MiCA). Il vise à encadrer les activités des plateformes d'échange dans l'UE (hors jetons financiers) et harmoniser les règlements locaux. Il introduit le statut de ***Crypto-Asset Service Provider*** (CASP) largement inspiré de celui de PSAN (prestataires de services sur actifs numériques) défini par la loi Pacte (lire l'encadré La France, pionnière avec la loi Pacte). Le règlement MiCA s'avère cependant plus exigeant que cette dernière, car il impose l'obtention d'un agrément pour exercer dans l'UE pour un large ensemble d'activités :

- conservation et gestion de cryptoactifs pour le compte de tiers,
- exploitation d'une plateforme de négociation de cryptoactifs,
- achat ou vente de cryptoactifs en monnaie ayant cours légal ou contre d'autres cryptoactifs,
- exécution d'ordres sur cryptoactifs pour le compte de tiers,
- placement de cryptoactifs,
- services de transfert sur des cryptoactifs pour le compte de tiers,
- réception et transmission d'ordres sur cryptoactifs pour le compte de tiers,
- conseil portant sur les cryptoactifs, gestion de portefeuille de cryptoactifs.

Parmi les exigences liées au statut de CASP : la nécessité de disposer de fonds propres suffisants ou, dans le cas contraire, de disposer d'une police d'assurance spécifique à cette activité, et de faire la preuve d'un système informatique résilient et sécurisé. Les CASP seront, en effet, tenus responsables en cas de pertes résultant de cyberattaques ou d'erreurs internes concernant les cryptoactifs de leurs clients.

La perte de clés, un des risques les plus élevés pour l'individu

L'un des principaux risques pour l'individu réside dans la perte de sa clé privée (soit volée, soit effectivement perdue). Une clé peut être volée parce que le portefeuille qui la contient est piraté ou parce que le possesseur est victime d'hameçonnage. Une clé privée, une fois volée, est en général immédiatement utilisée pour vider le compte auquel elle est rattachée.

Une clé privée perdue dépossède à jamais son détenteur de ses actifs. Dans les deux cas, aucun recours technique n'est possible (il n'existe pas de *back office* à contacter ou de lien pour récupérer son mot de passe sur la blockchain).

La blockchain offre une grande liberté à son usager puisqu'elle lui permet de se passer d'intermédiaire, mais cette liberté a un prix : celle de le rendre seul responsable de ses actes.

[22] Cryptocurrencies in the EU: deal struck between Parliament and Council

La France pionnière avec la loi Pacte

La France a fait figure de pionnière en matière de régulation des cryptoactifs. Dès 2016, la loi française reconnaît la blockchain comme un registre légal pour les instruments financiers du financement participatif (les minibons). En 2017, elle admet que les titres financiers peuvent aussi y être inscrits et échangés.

En 2019, l'instauration de la loi Pacte constitue une première avancée dans l'encadrement du marché français des cryptoactifs, avec la création du statut de prestataire de services sur actifs numériques, ou PSAN. Il se définit par 10 activités dont 4 doivent faire l'objet d'un enregistrement obligatoire auprès de l'AMF pour avoir l'autorisation d'exercer sur le territoire national : la conservation d'actifs numériques ; l'achat ou la vente d'actifs numériques en monnaie ayant cours légal ; l'échange d'actifs numériques contre d'autres actifs numériques ; l'exploitation d'une plateforme de négociation d'actifs numériques. L'obtention d'un agrément, plus contraignant et qui requiert une assurance professionnelle ou de fonds propres suffisants, n'est pas obligatoire (à ce jour, un seul PSAN a obtenu l'agrément : la Société Générale, via sa filiale Forge). La loi décrit également les régimes fiscaux et juridiques des jetons utilitaires de type ICO (les jetons financiers, assimilés à des instruments financiers, sont assujettis à la réglementation européenne afférente). En revanche, le statut des NFT n'est pas précisé laissant les éditeurs et acquéreurs dans le flou quant aux régimes d'appartenance de ces cryptoactifs.

En réaction à la faillite de la plateforme FTX fin 2022 et de ses agissements frauduleux (plus de 3,4 milliards de dollars), le législateur a renforcé les obligations des PSAN le 1er juillet 2023. Ils doivent, en particulier, garantir la ségrégation des actifs de leurs clients. À compter du 1er janvier 2025, la loi Pacte sera remplacée par le règlement MiCA. Les PSAN devront donc avoir obtenu un agrément MiCA pour exercer en Europe y compris en France. Ceux bénéficiant aujourd'hui d'un enregistrement ou d'un agrément pourront néanmoins continuer à offrir leurs services en France quelques mois supplémentaires sans agrément MiCA.

Notons qu'à ce stade, le règlement exclut la finance décentralisée (DeFi) et ne prend pas en compte les NFT en tant que tels. Il reste donc une incertitude sur ces deux sujets, mais la démarche témoigne de la volonté du législateur d'avancer à pas comptés pour préserver l'innovation dans ces domaines encore émergents. En ce qui concerne les NFT, la Commission européenne étudie la mise en place d'un régime spécifique. En attendant, c'est la finalité du jeton qui déterminera son appartenance à tel ou tel régime fiscal ou juridique.

Les acteurs de l'écosystème, par le biais de l'Adan, l'association des professionnels du Web 3 en France et en Europe, ont accueilli favorablement le règlement. *« Dans un contexte où le secteur des cryptoactifs traverse une période de défiance liée à l'actualité d'acteurs frauduleux, les règlements MiCA et TFR sont de nature à rassurer sur l'activité des opérateurs interagissant avec ces marchés »*, souligne l'association dans un communiqué[23] qui insiste cependant sur la nécessité de bien considérer les spécificités de ce domaine, notamment celles de la DeFi, afin de ne pas brider l'innovation alors que la France et l'Europe sont à l'avant-garde.

MiCA et TFR entreront en application en janvier 2025, à l'issue d'une période transitoire de mise en conformité de 18 mois[24]. Ils supplanteront alors les règlements nationaux, dont la loi Pacte (lire l'encadré ci-contre).

Il reste qu'investir dans des cryptoactifs ou dans un projet sur la blockchain demeure risqué. Le marché subit de grandes variabilités et n'importe quel soubresaut provoque des effets sur l'ensemble de l'écosystème. Ainsi, la chute de la plateforme FTX[25] fin 2022 a fait plonger les cours de toutes les cryptomonnaies, entraînant l'effondrement de plusieurs projets.

[23] MiCA et TFR — Les députés européens adoptent un cadre qui place l'Europe à la pointe sur les marchés mondiaux de crypto-actifs
[24] Marchés de crypto-actifs : publication du règlement européen MiCA
[25] Rappelons que la faillite de la plateforme FTX (localisée aux Bahamas) en novembre 2022 est le résultat d'une fraude massive similaire à celle de Bernard Madoff dans laquelle la technologie de blockchain n'est pas impliquée.

Le règlement MiCA n'empêchera pas les fraudes à l'égard des individus et les portefeuilles autohébergés resteront les cibles d'attaques en vue de piller les comptes et de dérober les clés.
De même, un ***smart contract*** mal codé peut présenter des vulnérabilités. Une grande vigilance s'impose donc dans les outils que l'on choisit et dans les plateformes que l'on fréquente.

Réduire son empreinte environnementale

Un autre reproche de plus en plus appuyé à l'endroit de la technologie concerne son empreinte environnementale. **Certains protocoles de validation des transactions requièrent des capacités de calcul très importantes.** Ils nécessitent des ordinateurs spécialisés de plus en plus puissants et difficilement recyclables et engendrent des coûts énergétiques élevés.

C'est le cas de ***Proof of Work***, mis en œuvre par Bitcoin, dont la consommation annuelle en 2023 devrait avoisiner 142 TWh selon le Cambridge Bitcoin Electricity Consumption Index[26]. Le montant équivaut déjà à 0,64 % de la consommation d'électricité mondiale[27]. Le développement prévisible des usages fait craindre une explosion de la facture énergétique.

Les communautés de développeurs s'efforcent de résoudre cette question de différentes manières. Ils travaillent, notamment, au développement de couches logicielles permettant de limiter l'exécution du protocole. Une autre voie consiste à privilégier l'emploi de protocoles moins énergivores comme ***Proof of Stake***[28] adopté par Ethereum et utilisé également par Tezos (qui revendique une consommation 300 000 fois inférieure à Bitcoin[29]).

Notons que le règlement européen MiCA prévoit d'imposer aux plateformes d'échange l'obligation d'informer leurs clients sur l'empreinte environnementale des cryptoactifs exposés.

Améliorer sa capacité à monter en charge

La technologie présente un autre inconvénient majeur : l'acroissement du délai de validation des transactions au fur et à mesure de l'expansion du réseau. Ce défaut, qui entrave son adoption à large échelle, est intrinsèque à la technologie. Il découle de sa nature décentralisée et du protocole de sécurisation des enregistrements par consensus : **plus le réseau est étendu, plus il devient sûr, mais plus les délais de confirmation des transactions s'allongent.**

Bitcoin est particulièrement touchée par ce problème de montée en charge – également appelé « scalabilité[30] » – en raison de son succès et des limitations techniques de son protocole qui restreignent le volume de transactions par seconde. D'autres réseaux sont également affectés. La blockchain Solana, par exemple, pourtant annoncée comme « ***scalable*** » a connu plusieurs interruptions de service en 2022.

Pour contourner cette faiblesse, les développeurs ajoutent, au-dessus de l'infrastructure, des couches applicatives destinées à absorber une partie des transactions[31].

[26] Cambridge Bitcoin Electricity Consumption Index
[27] Il est d'usage désormais de comparer la consommation du réseau Bitcoin à celle des pays. Cet article fait la part des choses.
[28] Le protocole Proof of Stake repose sur la quantité de cryptomonnaies détenue et non la puissance de calcul mobilisée.
[29] Blockchain : consolider nos atouts.
[30] La scalabilité est la capacité d'un système informatique à changer d'échelle d'utilisation sans impact notable sur ses fonctionnalités, sa sécurité ou sa disponibilité.
[31] Lightning Network pour Bitcoin, par exemple

L'écosystème de la blockchain

Les PSAN

Les prestataires de services sur actifs numériques ou CASP (Crypto-Asset Service Providers) gèrent des places de marché où s'échangent les cryptoactifs (Binance, Coinbase, Coinhouse, etc.). Les activités de ces entreprises sont encadrées par la réglementation française Pacte et le seront par le règlement européen MiCA, lors de sa mise en application en 2025. À l'écriture du document, on compte plus de 90 PSAN enregistrés en France et 1 seul agréé (Société Générale, par le biais de sa filiale Forge). Certains PSAN, comme OpenSea, Rarible ou AtomicHub sont spécialisés dans l'achat et la vente de NFT.

Les éditeurs de portefeuilles

Ces fournisseurs proposent des solutions logicielles ou matérielles de gestion de comptes sur les blockchains, qu'on appelle portefeuilles ou ***wallets***. L'acteur français Ledger figure parmi les leaders dans ce domaine avec un portefeuille matériel sécurisé.

Les éditeurs de NFT

Cette catégorie regroupe les éditeurs de collections (***collectibles***) et toute entreprise ou tout individu (des artistes en particulier) qui enregistrent (ou « ***mintent*** ») des NFT pour valoriser un bien matériel ou immatériel sur la blockchain (une création artistique, un ouvrage, un objet physique, etc.). La licorne française Sorare, qui s'est fait connaître grâce à son jeu de football en ligne, édite ses cartes de joueurs sous la forme de NFT qui s'échangent à prix d'or.

Les sociétés du numérique

Ce sont les entreprises de conseil, d'édition de logiciels, de développement informatique ou d'hébergement dont les activités participent au développement et à la mise en œuvre d'applications et de composants numériques tournant sur une blockchain (applications de traçage, développement de ***smart contracts***, outils de création de NFT, applications distribuées, etc.).

Une variété de types de portefeuilles

Le portefeuille (ou *wallet*) permet d'accéder aux informations relatives à un ou plusieurs comptes (soldes, etc.) et de recevoir ou émettre des cryptoactifs. Les portefeuilles ne sont pas nécessairement compatibles avec toutes les blockchains. Ils ne proposent pas non plus tous les mêmes services (comme de gérer des NFT).

Les plateformes d'échange proposent souvent d'héberger les portefeuilles de leurs clients. Dans ce cas, elles détiennent les clés privées associées aux comptes. La solution rend la gestion des clés transparente pour l'utilisateur et elle facilite les transactions. Elle présente néanmoins un risque puisque cela revient, pour l'utilisateur, à confier l'entièreté de ses fonds à un tiers.

Avec les portefeuilles autohébergés, la clé privée est au contraire détenue par le possesseur du compte. Ces outils peuvent se présenter comme des applications pour mobiles ou pour ordinateurs, comme des applications en ligne ou des extensions de navigateurs. Ils peuvent aussi être des dispositifs matériels non connectés et donc plus sûrs.

Il existe également des portefeuilles dits multisignatures. Leur principe : le portefeuille génère plusieurs clés privées avec l'obligation, pour valider une transaction, de réunir une partie d'entre elles, ce qui renforce la sécurité. En cas de perte d'une des clés (par exemple, celle stockée dans un mobile), il suffit d'utiliser les autres pour régénérer la clé perdue. Une des clés peut être conservée par un tiers de confiance.

Exemples de classe de risques

Malveillance

- Cyberattaque du réseau et détournement massif de fonds.
- Cyberattaque d'une plateforme d'échange et détournement de fonds*.
- Cyberattaque ou escroquerie sur un portefeuille individuel autohébergé et vol des fonds.
- Toute forme d'attaque (vol, vol avec violence, escroquerie, chantage, abus de confiance) visant à déposséder une personne de sa clé privée.

Erreurs

- Panne technique du réseau.
- Bug dans des portefeuilles ou des composants d'applications.
- Bug dans des ***smart contracts.***

Conformité (LCBFT)

- Provenance illégale ou suspecte de tout ou partie des fonds d'un patrimoine**.

Légal, contractuel

- Achat d'un NFT qui ne donne pas les droits escomptés.
- Achat d'un NFT dont le sous-jacent est un plagiat.

Fiscal

- Non-déclaration ou déclaration partielle d'un patrimoine de cryptoactifs.
- Valorisation erronée d'un patrimoine (due à la volatilité).

** La réglementation MiCA porte la responsabilité sur les CASP (ou PSAN)*

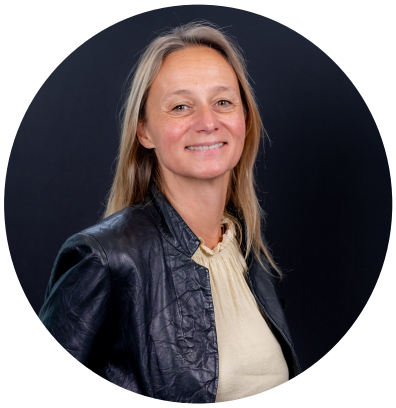
*** Si les fonds proviennent de transactions faisant intervenir des CASP (ou PSAN), c'est à ces derniers de fournir les éléments permettant de vérifier l'origine des fonds, conformément à la réglementation TFR. Dans le cas de transferts de pair-à-pair, tout soupçon sur l'origine des fonds doit être porté à la connaissance du service de renseignement sur les circuits financiers clandestins Tracfin.*

Les enjeux pour trois professions emblématiques

*Pour trois professions, la blockchain et les cryptoactifs sont une réalité qui transforme leurs activités : **les notaires**, qui commencent à traiter des opérations impliquant des cryptoactifs ; **les conseillers en gestion de patrimoine**, de plus en plus sollicités par leurs clients sur ces nouveaux produits ; **les entreprises du numérique** qui œuvrent à la construction et l'hébergement des outils et technologies.*

02

L'enjeu pour le notaire



Delphine Mercelat
Présidente LSN Assurances

« *Le notariat, profession traditionnelle, s'avère d'une très grande modernité dans l'univers numérique et technologique. Elle a, depuis quelques années, identifié les difficultés liées aux actifs numériques. L'enjeu pour le notariat, au-delà de l'assurabilité même du cryptoactif et de la blockchain, relève surtout de la formation et de la prévention. Le notaire 3.0 doit maîtriser ces technologies pour son activité de demain.* »

Amenés de plus en plus fréquemment à devoir réaliser des opérations impliquant des cryptoactifs, les notaires se posent des questions très concrètes sur la manière de procéder et sur leur couverture par rapport aux risques encourus.

Comment valoriser un NFT ? Ce point est d'ailleurs un des premiers obstacles auquel se heurtent les assureurs européens pour envisager une éventuelle couverture. ***Comment vérifier l'origine de fonds en cryptoactifs ? Comment constituer un séquestre si la transaction implique des cryptoactifs ? Comment sécuriser une transmission comportant des cryptoactifs ? Quelle couverture attendre si l'on est amené à conserver des clés secrètes pour autrui ? Quels conseils prodiguer dans le cadre d'une anticipation successorale ?***

Les risques liés aux cryptoactifs sont d'autant plus importants que le domaine manque de maturité. Obligation de conseil, obligation de vérifier l'origine des fonds, risque fiscal sont autant de domaines dans lesquels les pratiques vont évoluer avec l'expérience, la réglementation et la technologie.

Les activités des notaires sur l'ensemble de ces sujets sont couvertes par leurs assurances de responsabilité civile dès lors qu'elles ne portent pas sur des opérations interdites. Il leur est néanmoins recommandé de procéder avec prudence compte tenu, notamment, du manque d'antériorité des pratiques dans ce domaine, de la jeunesse des solutions, de la volatilité des actifs et du caractère encore mouvant de la législation dans le domaine.

Ainsi, dans le cadre de leur obligation de déclarer à Tracfin leurs soupçons sur l'origine des fonds impliqués dans les opérations qu'ils réalisent, les notaires sont invités à redoubler de vigilance si des cryptoactifs sont en jeu. Cela, notamment s'ils ne proviennent pas de plateformes d'échange enregistrées ou s'ils ont été acquis avant la mise en place de la loi Pacte.

Une déclaration ou une valorisation de NFT demanderont également un examen minutieux de la finalité des jetons puisqu'un NFT peut relever de régimes fiscaux différents selon les cas (lire le paragraphe Sécuriser le marché par la régulation)...

Une donation ou une transmission successorale nécessitera probablement la prise en compte de la volatilité des actifs, notamment s'il est prévu une réserve d'usufruit.

La constitution d'un séquestre de cryptoactifs, dans le cadre d'une transaction immobilière par exemple, impliquera là aussi de sélectionner avec précaution le PSAN qui conservera les actifs. Il est recommandé de s'orienter vers des prestataires officiellement enregistrés, voire de choisir un institut bancaire enregistré comme PSAN pour la conservation d'actifs. Cela, dans l'attente de l'émergence de solutions proposées par la Banque des territoires. Il faudra également veiller au choix du type de portefeuille (privilégier les technologies froides moins sujettes aux cyberattaques).

Là aussi il est important de noter que la liste des PSAN agréés est limitée du fait des difficultés pour répondre à l'obligation d'assurance nécessaire à l'obtention de l'agrément.

Dans le cadre d'une anticipation successorale, le notaire pourra encourager son client à lui fournir l'inventaire de ses comptes de cryptoactifs et l'aider à organiser les modalités de leur transmission. Il devra aussi l'inviter à consigner de manière sécurisée les moyens d'y accéder. Des dispositifs répondant à ce besoin commencent à émerger, comme la plateforme patrimoniale du Lab notarial, le coffre-fort électronique notarial de Solar Tech ou encore les portefeuilles multisignatures.

Les sujets de questionnement sont donc légion et les instances travaillent sur ces sujets d'un point de vue technique (quelles sont les clauses à intégrer dans le cadre d'une vente immobilière en bitcoins), d'un point de vue pratique et technologique (comment organiser un séquestre en cryptoactifs, comment s'assurer de la conservation d'une clé). Dès 2021 et le 117e congrès de notaires, les sujets techniques étaient posés. L'arsenal de formation, information, colloque et par conséquent de prévention est déployé afin d'accompagner les études dans l'appréhension tant de ces nouvelles problématiques, mais également de ces nouvelles technologies. Une fois encore, le notariat montre sa capacité d'adaptation rapide et son agilité pour prendre ce nouveau virage.

L'enjeu pour le conseiller en gestion de patrimoine

Emmanuel du Ranquet
Directeur général BDJ

« En recherche permanente de traçabilité, de temps réel et de transparence dans un environnement ultra normalisé, les infrastructures de marché sont à l'aube d'un changement technologique. Sans cristalliser sur le support d'investissement bitcoin, j'ai la conviction que la blockchain est une vraie technologie de rupture pour l'industrie bancaire et d'investissement. Je ne serai pas surpris de voir la tokenisation d'actions d'entreprise se développer de manière importante dans les mois à venir. Pour les conseillers en gestion de patrimoine, l'enjeu de compréhension et de formation est très important pour ne pas être pris de vitesse dans un environnement où la demande est de plus en plus insistante. »

L'émergence fulgurante des cryptoactifs dans la finance bouscule le monde du conseil en gestion de patrimoine. L'engouement pour ces produits, qui ont gagné en crédibilité et en popularité auprès des investisseurs, particuliers et entreprises, oblige les conseillers en gestion de patrimoine (CGP) à s'adapter pour répondre aux nouvelles attentes de leurs clients.

Les cryptoactifs partagent des similitudes avec les investissements atypiques tels que les œuvres d'art, les métaux précieux et les investissements immobiliers non traditionnels. Ils offrent souvent une faible corrélation avec les marchés financiers traditionnels, ce qui peut contribuer à une diversification efficace des portefeuilles. Cependant, ils présentent également des risques élevés en raison de leur volatilité.

Les CGP ont le devoir d'informer leurs clients sur les avantages et désavantages de ces actifs émergents et sur les risques associés. Pour accomplir de manière responsable cette obligation, ils doivent tout à la fois acquérir une compréhension approfondie de la technologie blockchain et des cryptoactifs, maîtriser les mécanismes de marché, connaître la fiscalité et suivre l'évolution de la réglementation.

Un vrai défi si l'on considère la rapidité d'évolution de la technologie, l'effervescence du marché et le caractère encore mouvant de la régulation.

Moyennant cet effort de formation, **le CGP qui informe correctement son client et fait appel à un PSAN enregistré ou agréé n'a aucune raison de voir son conseil remis en question** (le risque est transféré au PSAN à l'instar d'une société de gestion).

Pour le conseiller en investissements financiers (CIF), la question se pose différemment. En l'état actuel de la réglementation, le service de conseil aux souscripteurs d'actifs numériques ne nécessite pas d'enregistrement ou d'agrément obligatoire en tant que PSAN auprès de l'Autorité des marchés financiers (AMF). Un CIF est donc autorisé à prodiguer, à titre accessoire, des conseils sur des actifs numériques (cryptomonnaies ou jetons numériques), sans avoir à solliciter le statut de PSAN[34].

Cela est vrai pour autant que l'exclusion des biens divers ne figure pas dans son contrat d'assurance RC. Ce qui peut être le cas des contrats dits « packagés » que l'on peut souscrire en ligne, en général à bas prix, mais à garanties limitées.

Un point de vigilance est donc à observer sur ce sujet. Il en sera autrement, à partir de 2025, avec l'avènement du règlement MiCA : la fourniture de conseil sur cryptoactifs fait partie des services pour lesquels l'obtention d'un agrément sera obligatoire (lire le paragraphe Sécuriser le marché par la régulation).

Le conseiller en investissements financiers (CIF) effectue les activités suivantes :

- **Réalisation d'opérations de banque sur instruments financiers**
- **Réalisation d'opérations de banque ou d'opérations connexes**
- **Fourniture de services d'investissement ou de services connexes**
- **Réalisation d'opérations sur biens divers**

Son statut a été créé en France par la loi de sécurité financière n° 2003-706 du 1er août 2003 pour les personnes qualifiées qui exercent une activité de conseil sur les domaines définis par l'article L.541-1 du Code monétaire et financier.

[34] Services sur cryptoactifs par un CIF : est-ce possible sans être PSAN ?

L'enjeu pour les entreprises du numérique

Nicolas Hélénon
Co-gérant Neotech Assurances

« *L'avènement des technologies telles que les NFT, les smart contracts, la blockchain et les cryptoactifs a ouvert de nouvelles perspectives dans le monde financier, industriel, artistique... Cependant, derrière les promesses de révolution se cache un facteur fondamental qui unit ces innovations : le risque informatique.*
En effet, ces technologies novatrices reposent sur des systèmes informatiques avancés, ce qui les expose à des vulnérabilités similaires à celles rencontrées par les entreprises de services du numérique (ESN), les hébergeurs et les éditeurs de logiciel ou de contenus. Connaître les risques informatiques nous permet de comprendre les risques des NFT, de la blockchain et des cryptoactifs ainsi que de leur assurabilité. »

Bon nombre d'entreprises œuvrant dans le domaine des blockchains mènent des activités relevant du domaine informatique classique.

C'est le cas :

- des entreprises du numérique qui, en tant que prestataires, conseillent, développent ou hébergent des technologies ou des programmes (***smart contracts***, applications) relatifs à la blockchain privée,
- des entreprises du numérique qui, en tant que prestataires, conseillent ou développent des applications, des composants d'applications ou ***des smart contracts*** (des applications de traçage ou de certification ou encore des ***smart contracts*** pour NFT, par exemple), s'appuyant sur une blockchain publique sans exercer les activités de PSAN,
- des éditeurs de portefeuilles autohébergés.

Elles devraient, à ce titre, pouvoir bénéficier, pour lesdites activités, de la protection d'une responsabilité civile usuelle les couvrant, en tant que prestataire et éditeurs, des conséquences pécuniaires des fautes professionnelles suivantes :

- erreurs ou omission de programmation,
- bugs,
- défauts de conseil,
- indisponibilités des données ou des systèmes,
- retards,
- failles ou incident de sécurité informatique,
- ou même agissements en contrefaçon de droit d'auteur ou de logiciel.

Les positions des compagnies d'assurances diffèrent à ce sujet. Certaines refusent catégoriquement de couvrir toutes activités en lien avec les NFT, les ***smart contracts***, la blockchain et les cryptoactifs. D'autres compagnies limitent leurs interdits de souscription à certains domaines de ces technologies, tels que les cryptomonnaies,ou à l'édition ou l'exploitation de NFT.

Pour ces ESN, hébergeurs et éditeurs évoluant dans le secteur de la blockchain, la recherche de solutions d'assurance adaptées nécessitera donc l'analyse approfondie et une compréhension complète des activités spécifiques de l'entreprise que l'on envisage d'assurer.

Les éditeurs de NFT, dont le statut reste ambigu du fait de l'absence de clarté du cadre réglementaire dans lequel ce type de jetons s'inscrit, mériteront aussi un examen au cas par cas.

Les PSAN, quant à eux, relèvent d'un régime spécifique du fait de leurs obligations réglementaires. Rappelons que plus de 90 sont enregistrés auprès de l'AMF. Un seul est agréé à ce jour (Forge - Société Générale). La législation étant en pleine évolution, les acteurs assurantiels ont du mal à se positionner sur ce type d'activités et de prises de garantie. La mise en place du règlement européen MiCA nécessitera, cependant, de trouver des solutions d'assurance pour les prestataires qui ne disposeront pas des fonds propres requis par leur activité (lire le paragraphe Sécuriser le marché par la régulation).

Conclusion

La blockchain et ses applications prennent peu à peu leur place dans l'économie traditionnelle. La rapidité des évolutions technologiques, l'émergence de réglementations structurantes et les transformations induites par les multiples innovations bousculent les métiers de nos clients et partenaires. Afin de les accompagner dans leur appropriation de ces nouveaux usages, le groupe Diot-Siaci s'est engagé à poursuivre l'animation de groupes de travail sur les sujets évoqués dans ce livre blanc et à partager régulièrement les fruits des réflexions.

Remerciements

Éléments de bibliographie

Ouvrages et rapports en ligne

- La Blockchain décryptée. Les clés d'une révolution par Blockchain France (NetExplo Observatory - 2016)
- Révolutionner l'assurance avec le Métavers par Anouk Bara, Emmanuel Moyrand, Pierre Paperon, Alexandre Rispal (L'Argus de l'assurance - 2023)
- Web 3 et crypto en France et en Europe. Adoption par le grand public et applications dans les industries (Rapport de l'Adan, KPMG et Ipsos - 2023)
- Perspectives crypto 2023 (Rapport de KPMG - 2023)
- Blockchain, consolider nos atouts (Rapport de l'Institut Montaigne - 2023)
- Comprendre les blockchains : fonctionnement et enjeux de ces nouvelles technologies (Rapport du Sénat - 20 juin 2018)

Sites web experts

- Cryptoast
- Coin Academy
- Cryptonaute
- Cointribune

Podcast et webinaire

- Quel avenir pour Bitcoin ? – Alexandre Stachtchenko
- Webinaire IDEA - Les enjeux juridiques des NFT : l'exemple du marché de l'art (Université Jean Moulin Lyon 3 - 2018)

Le groupe Diot-Siaci

Diot-Siaci est un groupe généraliste de conseil et de courtage d'assurance et de réassurance leader en France et en Europe, présent à l'international notamment en Asie, au Moyen-Orient et en Afrique et à travers son réseau Diot-Siaci Global Partners partout dans le monde.

Il conçoit et imagine des solutions innovantes sur mesure pour ses clients Grandes Entreprises, ETI, PME-PMI et Professionnels aussi bien en assurances de personnes qu'en assurances de biens et de responsabilités.

Diot-Siaci dispose d'un actionnariat stable et familial qui lui permet d'accompagner ses clients dans leur développement et leur transformation. Nous répondons à leurs besoins sur toute la chaîne de valeur en IARD, Transport, Responsabilité Civile Professionnelle, Protection Sociale, Conseil et Mobilité Internationale, Assurance-crédit, Caution et Financement.

Avec près de 5000 collaborateurs et un vaste réseau international, le groupe exerce son activité dans le monde entier et totalise un chiffre d'affaires de près de 800 M€ en 2022.

LSN Assurances
Groupe DiotSiaci

www.lsngroupe.com

LSN ASSURANCES - Groupe DIOT-SIACI - Société de Courtage d'Assurance et de Réassurance.
Siège social : Season - 39, rue Mstislav Rostropovitch - 75815 Paris cedex 17 - France -
Tél. : +33 (0) 1 53 20 50 30. SAS - Capital : 3 978 810,90 € - RCS Paris 388 123 069 -
N° TVA : FR 37 388 123 069. N° ORIAS : 07 000 473 (orias.fr) - Sous le contrôle de l'ACPR -
4 place de Budapest - CS 92459 - 75436 Paris cedex 09 - France.
Réclamations : reclamations@lsngroupe.com - www.mediation-a surance.org.

BDJ
Groupe DiotSiaci

BDJ - Groupe DIOT-SIACI - Société de Courtage d'Assurance et de Réassurance.
Siège social : Season - 39, rue Mstislav Rostropovitch - 75815 Paris cedex 17 - France -
Tél. : +33 (0) 1 56 37 01 72. SAS - Capital : 2 294 800 € - RCS Paris 410 334 593 -
N° TVA : FR 71 410 334 593. N° ORIAS : 07 000 473 (orias.fr) - Sous le contrôle de l'ACPR -
4 place de Budapest - CS 92459 - 75436 Paris cedex 09 - France.
Réclamations : reclamations@lsngroupe.com - www.mediation-a surance.org.

NeoTech
Groupe DiotSiaci

www.neotech-assurances.fr

NEOTECH ASSURANCES - Groupe DIOT-SIACI - Société de Courtage d'Assurance et
de Réassurance. Siège social : Season - 39, rue Mstislav Rostropovitch - 75815 Paris cedex
17 - France - Tél. : +33 (0) 1 56 37 01 72. SAS - Capital : 38 460 € - RCS Paris 534 237 235 -
N° TVA : FR 20 534 237 235. N° ORIAS : 11 063 537 (orias.fr) - Sous le contrôle de l'ACPR -
4 place de Budapest - CS 92459 - 75436 Paris cedex 09 - France.
Réclamations : reclamations@lsngroupe.com - www.mediation-a surance.org.